NAJA FUKAMOLO SALOMON

ID: UB69796SME78930

COURSE NAME

INFORMATION SYSTEMS PROJECT MANAGEMENT.

STUDENT'S PROFILE

PROFESSIONAL PERSONNEL, LEADERSHIP AND DECISION MAKER.

ATLANTIC INTERNATIONAL UNIVERSITY

HONOLULU, HAWAII

DECEMBER 2021

TABLE OF CONTENT

1. INTRODUCTION

A collection of tools and procedures for gathering, integrating, and disseminating the outputs of project management processes. It is used to assist all phases of a project, from conception to completion, and may incorporate both human and automated technologies.

While each PMIS implementation is unique in terms of scope, architecture, and functionality, software applications are regarded a necessary component of each. The optimal use of a PMIS is highly dependent on the accessibility of essential information to all stakeholders and the degree of process automation. Many project managers have reservations about their PMIS's performance, in part due to improperly setup software and partly due to ROI issues. The goal of this research is to investigate and report on project managers' impressions of software programs that are a critical component of their PMIS installations.

Globally, organizations increasingly depend on digital programs to automate project management operations. Additionally, much focus is made on enhancing the quality of the data used to compile important performance indicators and reports. Major project management obligations, such as maintaining several registers and recording lessons learned, become much simpler to fulfill when an appropriate application is deployed. The following sections offer an overview of the EMEA region's current PMIS landscape.

A management information system (MIS) is a standardized structure and display of data that is often needed by an organization's management in order to make more informed choices. The MIS data may be obtained from numerous organizational units or from external sources. However, defining the precise structure of MIS is challenging due to the fact that the structures and objectives of various kinds of companies vary. Thus, both the data and structure of MIS are depending on the kind of organization and are often adapted to meet the management's unique requirements.

2. OBJECTIVES AND HOMEWORK

A project management information system (PMIS) is the logical structure of the data necessary for a company to effectively complete projects.

Typically, a PMIS consists of one or more software applications and a systematic methodology for gathering and using project data. These electronic solutions "assist in the planning, execution, and closure of project management objectives. PMIS systems vary in scope, design, and feature set based on the operational needs of an organization.

Tool for managing project information systems (PMIS). The Project Management Information System (PMIS), which is a component of the enterprise environmental factors, enables access to an automated tool, such as a scheduling software tool, a configuration management system, an information collection and distribution system, or web interfaces to other online automated systems that are used during the Direct and Manage Project Execution effort.

A. INFORMATION SYSTEMS CONCEPTS AND USAGES

PMIS are system tools and methods used in project management to transmit information. Through technological and manual methods, project managers use procedures and tools to gather, synthesize, and disseminate information. Upper and lower management interact through the Project Management Information System (PMIS).

The Project Management Information System (PMIS) assists in the planning, execution, and closure of project management objectives. Throughout the planning phase, project managers use PMIS to create a budget framework, which includes cost estimation. Additionally, the Project Management Information System is utilized to develop a detailed timetable and establish a scope baseline. The project management team gathers information into a single database over the course of executing the project management objectives.

The PMIS is used to compare the baseline to actual activity completion, manage materials, gather financial data, and maintain a record for reporting reasons. At the conclusion of the project, the Project Management Information System is used to assess the objectives and determine whether or not the tasks were completed. Then, it is utilized to generate a final report for the completion of the project.

To summarize, the project management information system (PMIS) is used to create schedules, budget for, and execute project management activity.

Characteristics of a PMIS Software

The methodology used to gather and arrange project data might be aligned with established standards such as Project Management Professional or PRINCE2.

A PMIS Software facilitates the management of all project-related knowledge areas, including integration management, project scope management, project time management, project cost management, project quality management, project human resource management, project communications management, project risk management, project procurement management, and project stakeholder management.

A PMIS Software application is a multi-user program that may be hosted in the cloud or on-premises.

Information system

An information system is a collection of interconnected components that enable the collection, storage, and processing of data as well as the provision of information, knowledge, and digital goods. Businesses and other organizations depend on information systems to conduct and manage operations, communicate with customers and suppliers, and compete in the marketplace. Interorganizational supply chains and electronic marketplaces are managed using information systems.

For example, firms utilize information systems to execute financial transactions, manage human resources, and promote their products and services online. Numerous large businesses are totally based on information systems.

These include eBay, a primarily auction-based marketplace; Amazon, an expanding electronic mall and cloud computing service provider; Alibaba, a business-to-business e-marketplace; and

Google, a search engine company that earns the majority of its revenue from keyword advertising on Internet searches. Governments use information technology to efficiently offer services to residents. Information systems supply digital items such as electronic books, video products, software, and online services such as gaming and social networking. Individuals rely heavily on information systems, most of which are based on the Internet, to conduct the majority of their personal lives: socializing, studying, shopping, banking, and entertainment.

Over millennia, when significant new tools for capturing and processing information were devised, new capacities emerged and humans gained empowerment. Johannes Gutenberg's development of the printing press in the mid-15th century and Blaise Pascal's invention of a mechanical calculator in the 17th century are only two examples. These technologies ushered in a sea change in our capacity to record, analyze, share, and seek information and knowledge. This resulted in even more profound changes in people's lives, commercial organizations, and human governance.

Herman Hollerith's census tabulator was the first large-scale mechanical information system. Hollerith's machine, invented in time to handle the 1890 United States census, was a significant step forward in automation and served as an inspiration for the development of computerized information systems.

The UNIVAC I, deployed at the United States Bureau of the Census in 1951 for administrative purposes and at General Electric in 1954 for commercial purposes, was one of the earliest computers used for such information processing. Personal computers began bringing some of the benefits of information systems to small enterprises and people in the late 1970s. The Internet started its spread as a worldwide network of networks early in the same decade. In 1991, Tim Berners-World Lee's Wide Web started functioning as a way of accessing the interconnected information housed on the geographically scattered computers connected by the Internet. It quickly became the network's primary service.

The Internet and the Web's worldwide penetration have increased access to information and other resources and encouraged the establishment of ties between individuals and organizations on a never-before-seen scale. Electronic commerce's advancement via the Internet has resulted in a substantial increase in digital interpersonal interactions (through e-mail and social media), product distribution (software, music, e-books, and movies), and corporate transactions (buying, selling, and advertising on the Web). With the global use of smartphones, tablets, laptops, and other computer-based mobile devices linked through wireless communication networks, information systems have been expanded to accommodate mobility as a natural human state.

Because information technologies facilitated a broader range of human activities, they had a tremendous effect on society. These technologies accelerated everyday routines, enabling individuals to form and sustain new and often more gratifying connections, altered the structure and composition of organizations, altered the types of items purchased, and altered the nature of labor. Knowledge and information have developed into critical economic resources. However, the increased reliance on information technology introduced new concerns. Continuous industrial innovation and academic research seek to provide new possibilities while containing risks.

Components of information systems

Computer hardware and software, telecommunications, databases and data warehouses, human resources, and processes are the primary components of information systems. Information technology (IT) is comprised of hardware, software, and telecommunications. IT is increasingly interwoven in the operations and administration of businesses.

- **Computer hardware**

Today, even the tiniest businesses and many homes worldwide possess or lease computers. Individuals may possess a variety of computers, including smartphones, tablets, and other wearable gadgets. Large enterprises generally use distributed computer systems, ranging from powerful parallel processing servers in data centers to widely spread personal computers and mobile devices that are connected with the organization's information systems.

Sensors are increasingly being deployed across the physical and biological environment in order to collect data and, in many situations, to operate devices known as actuators. These components, together with auxiliary equipment such as magnetic or solid-state storage disks, input-output devices, and telecommunications equipment, comprise the hardware of information systems.

Hardware costs have declined continuously and fast, while processing speed and storage capacity have improved significantly. This growth has occurred in accordance with Moore's law: the processing capability of the microprocessors at the core of computer devices has been roughly doubling every 18 to 24 months. However, designers are concerned about the hardware's energy consumption and environmental effect. Computer and storage services are increasingly being supplied through the cloud, using shared facilities accessible over telecommunications networks.

- **Computer software**

There are two major categories of computer software: system software and application software. The operating system is the primary piece of system software. It controls the computer's hardware, data and program files, and other system resources, as well as providing a mechanism for the user to operate the computer, often via a graphical user interface (GUI). Application software is a collection of applications that are intended to perform certain tasks for users. Individuals increasingly used smartphone applications to access information systems.

Other examples include general-purpose application suites containing spreadsheet and word processing tools, as well as "vertical" apps that cater to a particular industrial area, such as an application that plans, routes, and monitors package delivery for an overnight carrier. Larger businesses license and manage software programs produced and maintained by specialist software companies, adapting them to match their unique requirements, and build more applications in-house or via outsourced development.

Businesses may also employ cloud-based software-as-a-service (SaaS) solutions supplied through the Web. Proprietary software, which is only accessible from and maintained by its sellers, is being challenged by open-source software, which is freely available on the Web for use and modification under a license that ensures its continued availability.

- **Telecommunications**

Telecommunications is a term that refers to the process of connecting, or networking, computer systems, portable and wearable devices, and transmitting information. Wired or wireless media are used to establish connections. Coaxial cable and fiber optics are examples of wired technology. Mobile computing is enabled via wireless technologies, which are primarily based on the transmission of microwaves and radio waves. With the incorporation of computer devices into a wide variety of physical items, pervasive information systems have emerged.

For instance, sensors such as radio frequency identification devices (RFIDs) may be connected to items as they move through the supply chain to track their position and condition. Wireless sensor networks connected into the Internet have the potential to generate large volumes of data that may be utilized to improve productivity or monitor the environment.

Numerous computer network setups are feasible, based on an organization's requirements. Local area networks (LANs) connect computers inside a certain physical location, such as an office building or university campus. Metropolitan area networks (MANs) are the electronic backbone of "smart cities." They span a small, heavily populated region. Wide area networks (WANs) link geographically dispersed data centers, which are usually operated by distinct enterprises. Without centralized oversight, peer-to-peer networks allow widespread material exchange.

The Internet is a network of networks that connects billions of computers worldwide. Users receive access to information resources, such as big databases, and to other people, such as colleagues, clients, friends, or persons who share their professional or personal interests.

Within a company and for its exclusive use, internet-type services may be given through different intranets that are accessible via a browser; for example, an intranet may be installed as an access gateway to a shared corporate document base. To create a private and secure connection with business partners via the Internet, extranets are built as so-called virtual private networks (VPNs) by encrypting the communications.

A huge "Internet of things" has developed as a result of sensors and actuators being extensively spread across the physical world and providing data such as the acidity of a square yard of soil, the speed of a moving vehicle, or an individual's blood pressure. The availability of such information permits both immediate response in the event of an emergency and sustained decision-making based on the analysis of large amounts of gathered data.

Extensive networking infrastructure enables the rising trend toward cloud computing, in which information-system resources are shared across several firms, resulting in increased usage efficiency and flexibility in data center location. With algorithms that are sensitive to real-time needs and resource availability, software-defined networking enables flexible management of telecommunications networks.

- **Databases and data warehouses**

Numerous information systems serve largely as vehicles for the distribution of data held in databases. A database is a collection of linked material that has been arranged in such a way that individual records or groups of information may be accessed in response to certain criteria. Employee records and product catalogs are two common types of databases. Databases assist an enterprise's operations and management tasks.

Data warehouses store historical data that has been accumulated over time and may be mined for information in order to create and promote new goods, improve customer service, and reach out to prospective new consumers. Anyone who has ever made a transaction with a credit card, whether in person, by mail, or through the Internet, is included in such data sets.

Massive collecting and processing of quantitative, or structured, data, as well as textual material often acquired on the Web, has evolved into a large-scale endeavour dubbed "big data." Numerous advantages may accrue as a result of judgments based on the facts revealed by big data. Examples include evidence-based medicine, resource conservation via the elimination of waste, and personalized suggestions of new items (such as books or films) based on a user's preferences. Big data facilitates the development of novel business models.

For instance, a commercial business gathers product pricing using crowdsourcing (collection from various independent persons) via cell phones distributed across the globe. The aggregated data provides early warnings of price swings, allowing for more responsive decision-making than was previously feasible.

Automated sentiment analysis of textual data such as reviews and opinions expressed by individuals on social networks, blogs, and discussion boards is possible through the processing of textual data such as reviews and opinions expressed by individuals on social networks, blogs, and discussion boards.

Human resources and procedures

A qualified workforce is critical to the success of any information system. Development and operations managers, business analysts, systems analysts and designers, database administrators, programmers, computer security professionals, and computer operators are all examples of technical employees. Additionally, all employees within a business must be taught to maximize the potential of information technology. Through their usage of the Web, billions of individuals worldwide are learning about information systems.

The documentation of an information system includes procedures for its use, operation, and maintenance. For instance, protocols for running a payroll program must be created, including when to run it, who is permitted to execute it, and who has access to the output. Data centers are increasingly being administered autonomously as part of the autonomous computing concept, with the protocols encoded in the software that manages the centers.

Types of information systems

Organizations rely on information systems to support operations, knowledge work, and management. (The graphic depicts the general structure of organizational information systems.) Functional information systems supporting a single organizational function, such as marketing or manufacturing, have been largely overtaken by cross-functional systems supporting whole business processes, such as order processing or personnel management.

Such systems may be more successful in terms of product creation and delivery and can be assessed more carefully in terms of commercial results. The kinds of information systems discussed here may be implemented using a wide number of application packages.

Operational support and enterprise systems

Transaction processing systems assist in the design, marketing, manufacturing, and delivery of goods. In bigger businesses, transaction processing is usually performed by means of huge integrated systems referred to as enterprise systems. The information systems that support the different functional units of sales and marketing, manufacturing, finance, and human resources are linked in this example into an enterprise resource planning (ERP) system, the most common kind of business system.

ERP systems assist the value chain, which is the whole of the activities or processes through which a business adds value to its goods. For instance, a person or another firm may place a custom order over the Web, which will immediately commence just-in-time manufacturing according to the customer's requirements, a process known as mass customisation.

This entails routing client orders to the firm's warehouses and maybe to suppliers in order to ensure that input materials arrive in time for a batch bespoke manufacturing run. Financial accounts are updated as necessary, and logistics and billing are launched.

Along with assisting in the integration of a business's internal value chain, transaction processing systems may also aid in the integration of the organization's entire supply chain. This category encompasses all businesses engaged in the design, production, marketing, and delivery of products and services, from raw materials through final product delivery. A supply chain management (SCM) system coordinates the movement of goods, data, money, and information along the supply chain, beginning with raw material suppliers and ending with distributors and retailers.

For instance, buying an item at a large retailer creates more than a cash register receipt; it also immediately sends a restocking order to the relevant supplier, which may trigger orders to the supplier's suppliers. Suppliers may also use an SCM system to connect to a retailer's inventory database through the Internet in order to arrange efficient and timely deliveries in the correct amounts.

Customer relationship management (CRM) is the third kind of enterprise system. It assists businesses in marketing, sales, customer service, and new product development in engaging with their consumers. A CRM system provides a consolidated picture of a business's customers and transactions with them, allowing a constant and proactive connection. Customers may participate in the development of new goods via cocreation programs.

Numerous transaction processing technologies enable Internet-based electronic commerce. Online shopping, banking, and securities trading are just a few examples. Other systems provide on-demand access to information, education, and entertainment. Various additional methods assist the search for items with required characteristics (for example, keyword searches on search engines), price discovery (for example, through an auction), and delivery of digital products (such as software, music, movies, or greeting cards).

Social networking platforms, like as Facebook and LinkedIn, are an extremely effective tool for assisting consumer groups and people in expressing their thoughts, evolving new ideas, and being exposed to promotional messaging. On the Web, numerous businesses are offering an increasing variety of specialized services and information-based goods, as a worldwide infrastructure for electronic commerce develops.

Transaction processing systems collect the data essential for higher-level information systems in databases and data warehouses. Additionally, enterprise systems have software modules that enable many of these higher-level operations to be performed.

Support of knowledge work

In an information society, a significant portion of work is spent manipulating abstract information and knowledge (defined in this context as an organized and comprehensive structure of facts, relationships, theories, and insights), rather than directly processing, manufacturing, or delivering tangible materials. This kind of job is referred to as knowledge work. Three broad types of information systems facilitate this kind of knowledge work: professional support systems, collaboration systems, and knowledge management systems.

Professional support systems

Professional support systems provide the infrastructure necessary to undertake the duties associated with a particular profession. Automotive engineers, for example, use computer-aided engineering (CAE) software in conjunction with virtual reality systems to design and test new models as electronic prototypes for fuel economy, handling, and passenger protection prior to producing physical prototypes, and then use CAE to design and analyze physical tests. Before investing in long clinical trials, biochemists employ sophisticated three-dimensional modelling software to understand the molecular structure and likely action of novel medications. Investment bankers often use financial tools to determine the projected returns and associated risks associated with different investment strategies. Indeed, most occupations today have dedicated support systems.

Information system development

In bigger firms, information technology departments have a considerable effect on the development, usage, and application of information technology. An information system may be developed and utilized using a variety of approaches and procedures. Many developers today use an engineering methodology known as the system development life cycle (SDLC), which is a methodical process for constructing an information system in sequential phases. An organization's information system might be built in-house or outsourced. This may be performed by contracting out portions of the system or the whole system. [24] A particular example is the development team's geographical dispersal (offshoring, global information system).

According to Langefors' definition, a computer-based information system is a technologically realized medium for:

- linguistic expressions by recording, storing, and spreading them,
- as well as for deducing meaning from these statements.

Geographic information systems, land information systems, and disaster information systems are all instances of developing information systems, but they may all be regarded to be spatial information systems in their broadest sense. The evolution of a system occurs in phases, which include the following:

1. Recognize and specify problems
2. Collecting data
3. Specification of the new system's requirements
4. Design of the system
5. Constructing the system
6. Implementation of the system
7. Review and maintenance

Information systems research

The study of the consequences of information systems on the behavior of people, groups, and organizations is often multidisciplinary. Hevner et al. (2004) classified research in information systems into two scientific paradigms: behavioral science, which is concerned with developing and validating theories that explain or predict human or organizational behavior, and design science, which is concerned with expanding human and organizational capabilities through the creation of new and innovative artifacts.

Salvatore March and Gerald Smith presented a framework for investigating various facets of information technology, including the study's outcomes (research outputs) and the actions necessary to do the research (research activities). They recognized the following research outputs:

- Constructs, which are notions that comprise a domain's vocabulary. They comprise a conceptualization that is used to explain and specify domain-specific issues and their solutions.
- A model is a collection of assertions or statements elucidating the connections between constructions.
- A procedure is a collection of steps (an algorithm or guideline) used to accomplish a job. The methods are built upon a foundation of fundamental structures and a representation (model) of the solution space.
- Instantiation is the process by which an item is realized in its surroundings.

Additionally, research efforts include the following:

1. Create an artifact to do a certain activity.
2. Assess the artifact to see if any progress has been made.
3. When evaluating the performance of an artifact, it is critical to identify why and how the item performed well or poorly in its setting. As a result, develop and defend hypotheses regarding information technology artifacts.

Although Information Systems as a field has evolved over the last three decades, the fundamental emphasis or identity of IS research remains a point of contention among researchers. There are two distinct perspectives on this debate: a limited one that emphasizes the IT artifact as the central focus of IS research, and a wide one that emphasizes the interaction of social and technological components of IT imbedded in a dynamic developing environment.

A third perspective encourages information scientists to devote equal attention to the IT item and its context.

Given that information systems research is an applied discipline, industry practitioners anticipate that discoveries from information systems research will be instantly useful in practice. This is not always the case, since information systems researchers often go far further into behavioral difficulties than practitioners would assume. This may make the outcomes of information systems research difficult to comprehend, which has prompted criticism. Examine all 41 terms

B. INFORMATION SYSTEMS IN BUSINESS CONTEXT

Walmart's success is an excellent illustration of the advantages of corporate information systems. Since its beginnings, the multinational retailer has been a pioneer in implementing new information technology for commercial usage.

According to data specialist Anthony B. Smoak, Walmart "was a pioneer in barcode scanning and analyzing point of sale data stored in large data warehouses."

In the mid-1980s, Walmart established its own satellite network, which had a dramatic effect on the company's supply chain management process. Strategic systems... allowed Walmart and its suppliers to integrate and share data. Additionally, these technologies supported the idea of vendor-managed inventories," adds Smoak.

The retail behemoth is at the vanguard of an industry that benefits a wide variety of enterprises. Since the dawn of the Internet Age, the value of information in business has been incalculable. In his 2003 piece, "IT Doesn't Matter," Harvard Business Review editor Nicholas Carr compared information technology to a new, required commodity, similar to electricity. Businesses who do not invest extensively in business information technology may struggle to remain viable a decade and a half later.

In the corporate sense, information systems are complementary networks and interrelated components that collect, distribute, and otherwise make data relevant for management decision-making.

Information systems have developed throughout time, necessitating redefinitions in response to the proliferation of new technologies (Web 2.0, for example).

However, information systems are not only technical. "In addition to the hardware, software, and data components that have long been regarded the fundamental technology of information systems, one more component has been suggested: communication," notes researcher Dave Bourgeois.

An information system may exist without the capacity to communicate—the earliest personal computers were stand-alone devices that did not have internet connectivity. However, in today's hyperconnected world, a computer that is not connected to another device or network is quite unusual," Bourgeois says.

Bourgeois proposes integrating people and process to the usual hardware, software, and data components of information systems in order to integrate communication. Business executives across nearly every industry have discovered that the processes they employ, particularly the

"as-a-service" cloud analytics services, and the active participation of customers who want to customize their experiences more and more each year are inextricably linked to business information systems.

Once all of the pieces are connected, each information system serves a variety of functions for companies, each with a varied degree of significance based on the demands of the organization. On Chron.com, technology journalist Julie Davoren outlines them as follows:

Store and analyze data: Sophisticated and extensive databases, some of which are cloud-based, are used to store and analyze data on company functions, customers, transaction data, and employee and customer activities. These studies provide knowledge that may assist decision-makers in resolving current and future problems.

Assist in decision-making: Information systems may compare internal insights to external sources, such as information on the overall status of the economy or rival financial reports. These insights enable decision-makers to assess the appropriateness and quality of their strategic choices.

Assist in the development of value-added systems for business functions: Information systems are used to produce value-added systems for business functions. Through the use of information systems tailored to typical business operations such as manufacturing, supply chain management, and personnel workflows, business processes may be simplified and redundant activities eliminated.

As information systems grow increasingly ingrained in the world of business, managers and executives are required to get a full understanding of corporate information systems and their capabilities. As a result, many MBA programs now include information technology as part of their curriculum.

Management Information Systems Capabilities

Managers of business units that use information systems should be familiar with the fundamental capabilities of information technology, data analytics, and business intelligence systems. Management information systems make use of all of these capabilities in ways that are specifically designed for management and executive decision-making.

Information access: Managers need to have easy and fast access to information including customer records, sales data, market research, financial records, manufacturing and inventory data, and human resources records to make informed decisions.

Data collection: Management information systems gather and aggregate data from both external and internal sources. This data is aggregated and stored in data warehouses, which are subsequently networked for analytical purposes.

Collaboration is one of the most beneficial aspects of information systems because it enables multiple departments and distant teams to cooperate on choices while incorporating huge volumes of data from a variety of different sources, departments, and even sectors.

After a choice is taken, information systems may assist managers in comprehending the potential consequences of that action by continuously updating raw data and forecasting potential future advantages or difficulties.

The majority of information systems, particularly those aimed at managers, contain facilities for creating simple-to-understand reports for evaluation by senior managers or C-suite executives.

Managers may also use information systems that are purpose-built for certain business operations affecting their department or role. Marketing information systems, product subsystems, sales forecasts, and product design systems all create data that managers may use to make critical decisions.

Performance Monitoring Indicators

Performance indicators are quantitative measurements of a project's effects, results, outputs, and inputs that are monitored during the project's execution to determine progress toward the project's goals. They are also used to determine the success of a project later on. Indicators arrange data in a manner that explains the linkages between a project's effects, results, outputs, and inputs and assist in identifying issues that may obstruct the attainment of the project's goals along the way.

Several significant studies conducted in recent years—most notably the Portfolio Management Task Force Report and reviews conducted by the Operations Evaluation Department (OED) found that the monitoring and evaluation of Bank-financed projects did not place an adequate emphasis on the factors necessary for positive development impact. Both the task force and OED decided that performance indicators should be included into the Bank's and its borrowers' monitoring and assessment systems.

The Portfolio Management Task Force Report (a.k.a. the Wapenhans Report) examined the elements affecting the Bank's development effect. The task force examined how assessment procedures, such as the economic rate of return calculation and project rating methodology, were utilized to improve the quality of Bank-supported projects during project appraisal and supervision. The task force discovered that project ratings were not giving enough input on progress toward development effect to implementation units, borrowers, and Bank task managers for many reasons:

- Too much attention was put on the mechanics of project execution (physical and financial).
- The risks and variables that have the greatest impact on project results were inadequately recognized.
- Criteria that were objective, transparent, and—because the process was dependent on the
- Individuals' judgments were inconsistent among units.
- Ratings were often exaggeratedly hopeful.

Without adequate input, none of the stakeholders in a project's result can make suitable, informed choices about whether and how to alter the project's design or execution arrangements to accomplish the project’s stated goals more effectively. A related issue is that goals are often poorly defined or expressed, obscuring the establishment of acceptable performance monitoring indicators and complicating monitoring and assessment.

Additionally, the task group noted that the Bank's typical approach of project assessment and evaluation, calculating the economic rate of return or net present value cannot be applied to all

projects and that a meaningful cost-benefit analysis is not practicable for certain projects. Even when net present value or economic rate of return is computed for a project, the Bank's approach is to do so only a few times—during the appraisal process, at a midterm review, during any required restructuring, and at the time of the Implementation Completion Report. Throughout implementation, neither the computations nor the crucial variables that impact them are openly monitored. Additionally, the paper noted that in many circumstances, costs and benefits might be recognized and quantified more simply using performance indicators.

The task force determined that the Bank's project grading methodology and supervision reporting system should be modified to include indications of project performance monitoring derived from the development goals and execution plan of a project.

Two OED investigations examining the Bank's record of accomplishment of monitoring and evaluating programs corroborated the task force report's conclusions.

In fiscal 1994, a review of twenty years of Bank projects discovered that the Bank's monitoring and evaluation rules and instructions were not being implemented sufficiently, either during project assessment (when monitoring and evaluation are planned) or during implementation.

However, the investigation discovered indications that the situation was deteriorating. A follow-up assessment of monitoring and evaluation plans for a sample of fiscal 1995 projects indicates an improvement in the quality of such planning. The increase in the use of performance monitoring indicators is seen in the fact that the percentage of projects having at least some indicators increased from 72% in fiscal 1993 to 77% in fiscal 1995. Nonetheless, the increased use of indicators has not been matched by data collecting structures or capacity-building activities at the Bank or in borrowing nations. Only a small percentage of projects (14% of the sample examined by OED in fiscal 1995) demonstrate overall best practices in comprehensive design or monitoring and evaluation. And, although performance monitoring indicators are increasingly extensively utilized, they are often lacking in structure, lack a logical framework or typology, and data gathering is not always carried out.

To address these issues, the Bank's management has promoted the use of performance metrics. Management recommended incorporating performance monitoring indicators into the project rating system used for project monitoring (via Form 590 and the Annual Report on Portfolio Performance) in order to better monitor progress toward a project's development objectives in the Next Steps Action Plan, which was created to implement the recommendations of the Wapenhans task force.

Additionally, management realized that the Bank needed to establish sector-specific indicators to assist borrowers and Bank personnel in narrowing project goals and deriving rational metrics of project outcomes and effect to assess project success. Additionally, the Bank needs to advocate for the inclusion of indicators in the redesigned project grading system. As a result, the action plan directed sector departments within the Central Vice Presidency to prepare sets of sector-specific indicators that are most pertinent to project design and monitoring. These sector comments on indicators are covered in the second section of this handbook. Staff would then be responsible for ensuring that important sector-specific project impact indicators were established in the project assessment paperwork and that progress against these benchmarks was tracked.

Procurement Management Plan

A procurement management strategy specifies the purchasing requirements for all stages of the project's lifecycle, from document creation through contract conclusion. It is basically a road map for managing the project's procurement operations and ensuring that all deliverables are completed with the greatest possible value and efficiency.

Without further ado, let us look at what a procurement management strategy is and why it is necessary! Continue reading...

Procurement management, according to the PMBOK Guide, is an essential procedure for purchasing or acquiring items, services, or results from a project team through outsourcing. And when this process is documented on a document or piece of paper for teams to follow, it is referred to as a procurement management plan.

A procurement management strategy establishes the basis for your project's purchases. It acts as a guide for managing procurements of products, commodities, and/or services throughout the course of a project's lifecycle and is updated when procurement requirements change.

This plan defines the products that will be acquired, the contracts that will be utilized to support the project, the procedure for contract approval, and decision criteria. It is a fantastic place to start when it comes to organizing procurement procedures. When implemented properly, a procurement management strategy may assist reduce total procurement costs and facilitate corporate operations.

Furthermore, a procurement management plan defines the following:

- Procurement items with justifications and project schedules
- Contract types to be employed in the project • Procurement management risks
- Estimates costs
- Establishes contract deliverables and deadlines
- Specifies the procedures for coordinating procurement and contracts with the project's scope, budget, and timeline
- Describes any restrictions associated with the procurement of the project.
- Keeps track of procurement-related performance indicators

Managing an organization's procurement is one thing; managing it efficiently is another! A sound procurement strategy may help organizations save money and time while enhancing compliance.

Thus, in order to handle a company's procurement demands successfully, it is critical to establish a comprehensive procurement management strategy based on reliable data. Additionally, these proposals include the following:

- Compile a list of all the requirements that are anticipated to be purchased during the course of a timeframe.
- Establish a procurement timetable that details the deadlines for each phase of the procurement process, from contract award through demand fulfillment.
- Allow for the consolidation of comparable needs into a single contract or the segmentation of demand into many contract packages to achieve economies of scale.
- Include external aid or outsourcing to ensure that all procurement requirements are met.

- Allow for analysis of the procurement process in order to compare actual performance to anticipated outcomes.
- Enhances the procurement process's predictability and openness.

The project manager has a variety of tools and procedures at their disposal for monitoring and directing the procurement process. These are not self-contained and need certain inputs, which are often established during the procurement planning step. The procurement management strategy, the procurement contract, the project management plan, work performance information and performance reports, and authorized modification requests are the primary inputs for monitoring project procurement operations. Any performance reports will be compared to the project management plan's established baseline.

Only when a contract is signed can an accurate estimate of when project products and services will become accessible be made. If a component step for any item slips, the amended list of dates will be instantly updated. Because the procurement processes for works, products, and services are distinct, the PPMS employs distinct milestones for each kind. Additionally, it generates a list of procurement operations for a particular time period, giving a monthly calendar of all procurement activities necessary. This serves as a reminder of the key procurement chores that the project crew is required to do on a daily basis.

Disbursement Planning and Tracking System (DPTS)

With the recent implementation of the Loan Administration Change Initiative (LACI), project management units for World Bank-supported projects are required to submit accounting reports to the Bank in a prescribed format. The tables in these reports must include the disbursements made in each quarter as well as the prediction for the next quarter's payments.

The DPTS is a system that enables the planning of each contract's payment schedule for works, products, and services, as well as the entry of actual payment dates against this schedule. The system analyses the data automatically and generates reports in the desired format. All essential LACI reports may be generated straight from the database when used in conjunction with the Procurement Planning and Monitoring System (PPMS).

Project Performance Indicator Tracking System

The World Bank requires project managers to report to it on the status of each Performance Indicator in the project's Hierarchy of Objectives and the management measures taken to accomplish them. The report must be submitted semi-annually and in a format that has been agreed upon. This report has been created using a word processor over the last several years. Due to the fact that the report includes a column for the project manager's comments on the status of each indicator, the project manager spent substantial time producing this report.

The new Project Performance Indicator Tracking System (PPITS) stores indicators in a database format and categorizes their status into five categories: Successfully Completed, Being Achieved (on track), Experiencing Minor Problems (being addressed), Experiencing Major Problems and Target Date Rescheduling Required, and Not Yet Due. The project manager changes the state of each indicator as events occur, enters comments, and tracks management actions performed. At the conclusion of each reporting period, the needed report is generated automatically (a system function) with all current data.

Procurement Activity Tracking System (PATS)

Apart from the large contracts for the construction of new schools and the large consultancies, each project management unit also conducts a number of smaller contracts for equipping the new schools and procuring school supplies. The following stages comprise these shopping activities: Finalizing the original requirements; contacting suppliers for pricing quotes; negotiating specification changes, discounts, and delivery dates; receiving shipments or checking deliveries in terms of quantity and quality; and approving payments by the accountant.

While purchasing an individual item is straightforward, when the quantity of products needed for a given date increases, a database is necessary to monitor the progress of order placing and delivery to ensure that suppliers are paid on time. At the moment, payment authorizations are sent off-line, either the printing of a list of permitted payments or the delivery of a diskette to the accountant.

Project Planning and Scheduling System (PP&SS)

A detailed critical path based project plan and schedule was produced using MS project. A part of this plan is illustrated in Figure 3. The initial level of indenture is the WBS of the project. The schedule for the items of procurement, transferred from the PPMS, is shown on one line in the CPM chart using the rollup approach in MS Project.

The consultants devised five modules to aid the project management team in improving the quality of information utilized in management planning, control, and reporting. The quick prototyping design philosophy emphasized simplicity of use, reusing existing formats and methods, and needing little work to maintain the systems.

Implementation of the System

Three steps were used to develop and execute the system. The initial step included requirement development, basic training, and quick prototyping of a prototype system. The second step included system fine-tuning and on-the-job training. After a few months, the third phase included advanced training and support with system updates. Additionally, certain adjustments were made throughout this time period.

Information Systems Development

Organizations now place a premium on information systems (IS) that are planned and built effectively, precisely, and reliably, and that satisfy the intended requirements and expectations of stakeholders. However, cost, quality, and scheduling concerns have been commonly highlighted throughout the creation of information systems.

In the information technology area, project failure is an expensive issue, and difficult projects are not uncommon. It is difficult to accurately estimate the costs associated with establishing an information system, and despite the advent of new estimating techniques, little progress has been made.

Traditional Information Systems Development

The conventional Information Systems Development Life Cycle (ISDLC or SDLC) is a well-established concept that is commonly utilized in the development of information systems. It is

a strict procedure that ensures control over the development process by dividing it into phases, each of which must be completed before proceeding to the next, and each of which has a predefined set of tasks. It has always been a difficult, expensive, and time-consuming process, and the desire for a more flexible approach to development dates all the way back to the early 1980s.

C. FUNDAMENTALS CONCEPTS OF INFORMATION SYSTEMS

Today, an information system is critical to the operation and management of a corporation. Information technology enables the administration of critical production data, which enables the production, management, and owners of the firm to operate their business more efficiently and profitably. Operational excellence; business models; customer/supplier intimacy; enhanced decision-making; competitive advantage; and day-to-day survival are the six reasons. An information system is a method for collecting, storing, and sharing data about your organization.

\This might include financial planning, procurement, manufacture, and eventually, selling. With the use of several systems, such as SAP (System, Application, Products). The SAP system enables various business units to view and share data that is stored in a centralized location via its various components, such as material management, which is primarily used by warehouse functions associated with purchasing, and finance, which is primarily used by the finance department. According to my readings, the people component is concerned with topics such as training, managerial conduct, and work attitudes.

Additionally, I've learnt that the organization component is related to the specialization of duties performed by personnel, corporate culture, and the firm's structure. The technology component includes the computer system, data management, telecommunications, internet, and intranet of the business. Employees benefit from information system literacy when it comes to storing data and information related to their work performance. Computer literacy is necessary in order to comprehend the numerous programs used in an information system.

Internet is a service that enables you to maintain contact with the rest of the world, your customers, and investors. With a World Wide Web address that is usually available through the internet, you may sell items that your firm manufactures utilizing a single centralized warehouse, so minimizing the expenditures associated with many warehouses.

Information systems affect business careers and what information system skills and knowledge

Information systems play a critical part in employment in accounting, finance, marketing, and operations management. An information system assists each profession in a unique manner in achieving the company's shared aim of profitability. New information system technologies enable firms to increase productivity, reduce operational costs, operate more effectively, and generate the greatest profit. However, nations such as India, Japan, and China, who have developed their information systems and have a big pool of highly skilled workers at much lower labor costs, are compelling local firms to outsource some of their operations and services to those countries.

Information systems support the major business functions: sales and marketing, manufacturing and production, finance and accounting, and human resources

Sales and marking systems aid in identifying the consumer base for the items sold by your business. Demand data enables marketers to advertise items that are suitable for their specific markets. This assists in maximizing sales and profit from sales. Manufacturing and production systems are concerned with the planning, development, and manufacturing of the products manufactured by your business.

Additionally, this system assists in planning and maintaining the flow of production in order to minimize excess or under production and to consistently satisfy customer requests. Finance and accounting systems assist in the tracking of money and their usage in the manufacture and selling of items. Additionally, it assists in tracking earnings and losses. Human resource systems assist in the maintenance of employee personal and professional data, as well as the tracking of their skill levels, work performance, and any needed training to keep your personnel current on the newest technologies. This approach is also utilized to compensate employees and enhance their careers.

At the operational management level, the system is used for transaction processing, such as payroll and order processing. Middle management makes use of decision-support systems, which assist them in making choices on production, labor, and so forth. These are not very difficult or analytical exercises. Executive support systems, on the other hand, are very analytical. They are often presented to senior management in the form of graphs and charts in order for them to make executive level decisions.

The business has a plethora of applications. I'm going to define each one separately. Enterprise applications are a collection of functions that are integrated into a single software system to aid in the synchronization, efficiency, and decision-making processes. These apps are intended to facilitate the coordination of numerous corporate tasks. Supply chain management systems are beneficial for material management, resource planning, production, and distributing finished goods and services to the sales channel or, in certain situations, directly to consumers.

Customer relationship management (CRM) is a component of information technology that is used to organize and communicate company activities to customers in order to maximize revenue and customer happiness. Collaboration and communication tools are included in knowledge management systems. They assist businesses in optimizing their product development, information exchange, and distribution processes. Intranet is a term that refers to a section of a website that is restricted to internal corporate access.

Additionally, the business may have an Internet presence that is accessible to anybody with access to the World Wide Web. Oftentimes, businesses that sell directly to customers rely heavily on the Internet. Additionally, businesses have Extranets that are accessible to suppliers for purposes of material management, ordering raw materials, and so on.

Typically, the information systems function inside a firm is handled by the technology department. This division is sometimes referred to as Information Technology (IT). These teams of specialists are responsible for maintaining the company's hardware, software, data storage, and network infrastructure.

Characteristics of high quality information

Accuracy, completeness, consistency, distinctiveness, and timeliness are five qualities of high-quality information.

To be helpful and accurate, information must be of a high quality. The data entered into a data base is believed to be both flawless and accurate. The information retrieved has been determined to be credible. While database design flaws may occur, do not allow something under your control, accurate and dependable data, to be one of them. A precise and dependable database design will aid in the creation of new company ideas as well as the promotion of corporate objectives.

Another characteristic of high-quality information is its completeness. Partial information is just as likely to be incomplete information since it represents just a portion of the picture. When entering data into a database, completeness is just as critical as correctness.

When putting data into a database, consistency is critical. For instance, the typical length of a field containing a phone number input is ten digits. Once the fields are defined in the database, any value more or less than ten digits will be rejected. The same holds true for each field, regardless of whether the input demands a single number, a sequence of digits, an address, or a name. If the fields are not restricted to a specified amount of data, consistency becomes much more critical.

The fourth component of high-quality information is uniqueness. To offer value to an organization, information must be distinct and unique. Information is a critical component of every organization and, when handled appropriately, may help a business become or remain competitive.

A fifth critical characteristic of information is its timeliness. For enterprises, new and current data is more useful than old and out-of-date information. Particularly in this day of rapid technological advancement, out-of-date information might prevent a business from accomplishing its objectives or thriving in a competitive environment. The information does not have to be out of date to have an impact; it just has to be out of date. Real-time data is a component of timeliness.

- **Accuracy**

As implied by the name, this data quality attribute indicates that information is accurate. To ascertain if data is reliable, consider whether it accurately represents a real-world scenario. For instance, in the financial services industry, does a consumer really have a $1 million bank account?

Accuracy is a critical data quality attribute since erroneous information may result in serious difficulties. We'll apply the example above if a customer's bank account has an error, it might be because it was accessed without his knowledge.

- **Completeness**

Completeness" refers to the extent to which the information is complete. Consider if all of the data you want is accessible; you may require a customer's first and last names, but the middle initial may be optional.

Why is completeness important as a criterion of data quality? If data is incomplete, it may be rendered useless. Assume you're sending out a mailing. A customer's last name is required to guarantee that mail is sent to the correct address; without it, the data is incomplete.

- **Reliability**

In the context of data quality characteristics, dependability refers to the absence of inconsistencies between pieces of information from various sources or systems. We'll take the healthcare industry as an example; if a patient's birthdate is January 1, 1970 in one system but June 13, 1973 in another, the data is untrustworthy.

Reliability is a critical property of data quality. When elements of information contradict one another, the data cannot be trusted. You might make an error that costs your business money and harms your reputation.

- **Relevance**

When considering data quality criteria, relevance is critical since there must be a compelling rationale for gathering this information in the first place. You must determine if this information is really necessary or whether it is being gathered only for the purpose of obtaining it.

Why is relevance an important attribute of data quality? If you collect irrelevant data, you are wasting both time and money. Your analysis will be less useful as a result.

- **Timeliness**

As the term indicates, timeliness relates to how current information is. If the information was acquired during the last hour, it is current - unless new information has been received that makes earlier information obsolete.

The timeliness of information is a critical attribute of data quality, since out-of-date information may lead to individuals making incorrect judgments. As a result, firms incur expenses in terms of time, money, and reputational harm.

Timeliness is a critical attribute of data quality out-of-date information costs businesses time and money."

Data quality features guarantee that you get the most out of your information in today's business climate. If your data does not match these criteria, it is not useful. Precisely delivers data quality solutions that ensure your data is accurate, full, reliable, relevant, and current.

System software

System software is a sort of computer program that is used to manage the hardware and software on a computer. If we consider the computer system in terms of a layered architecture, system software serves as the interface between the hardware and user applications. The most well-known example of system software is the operating system. The operating system (OS) is responsible for the management of all other applications on a computer.

The computer's system software is used to administer it. It operates in the background, preserving the computer's fundamental functionality so that users may execute higher-level application software to do specific tasks. System software, in its simplest form, offers a foundation for application software to execute on.

Significant characteristics of system software

Typically, computer makers design system software as an integrated component of the machine. This software's principal function is to serve as a bridge between the computer hardware they build and the end user.

Generally, system software provides the following features:

- Rapid acceleration. System software must be as efficient as feasible in order to serve as an effective platform for the computer system's higher-level software.
- Difficult to manipulate. It often necessitates the use of a programming language, which is more challenging to learn than a more intuitive user interface (UI).
- It is written in a low-level programming language. System software must be written in a machine-readable computer language that can be read by the central processor unit (CPU) and other computer hardware.
- Close proximity to the system. It establishes direct contact with the hardware that allows the computer to function.
- Versatile. System software must interact with both the specialized hardware on which it operates and the higher-level application software, which is often hardware-agnostic and frequently does not have a direct link to the hardware. Additionally, system software must support the evolution and modification of other programs that rely on it.

Operating systems

The operating system of a computer is a well-known example of system software. Microsoft Windows, macOS, and Linux are all widely used operating systems. Unlike other forms of system software, the normal computer user interacts with the operating system on a regular basis through the graphical user interface (GUI) and, in certain cases, a less complicated command-line interface (CLI).

Because a graphical user interface is a program that runs on top of the operating system, it is often referred to as application software rather than system software. In other terms, the GUI is application software that enables the user to modify various components of the operating system.

The operating system performs critical functions.

The operating system's primary job is to manage a computer's software and hardware resources. It is the primary control software for the computer. The operating system (OS) is in charge of and keeps track of all other programs running on the computer, including both application and system software. The operating system (OS) establishes an environment in which all other computer programs may function and delivers services to those other programs.

Operating systems perform out functions. Five of the most critical are as follows:

Management of files and scheduling of processes. The operating system distributes resources and establishes priorities for which applications should get them and in what sequence. For instance, when a digital audio workstation program is utilized, it may demand a particular amount of computing power. The operating system determines how much CPU power a program receives and handles the impact of that allocation on other apps. If a more vital function is running on the computer, the operating system may sacrifice part of the power sought by the digital audio workstation to guarantee the other process can finish.

Management of the processor and memory. When a process requires memory, the operating system allocates it and then deals locates it when the process is complete.

Determination of errors. The operating system (OS) monitors, logs, and debugs faults in the computer's other applications.

Security. The operating system use passwords to safeguard the computer's applications and data from illegal access.

Control and administration. Compilers, assemblers, and interpreters are used by the operating system to control and manage other programs on the computer. These language processers are pieces of system software that convert the high-level languages — Java, Python, and C++ — in which many computer programs are written into low-level machine code instructions, which are essentially a series of 1s and 0s that the computer's central processing unit (CPU) can read.

Difference between system software and application software

The two primary categories of computer software are system software and application programs. In contrast to system software, application software also referred to as an application or app – provides a specific purpose for the end user. The following are some instances of application software:

- Web browsers
- Clients e-mail
- Word processors
- Spreadsheets

Application software is coded differently from system software. System software is created in system programming languages such as Executive Systems Problem Oriented Language (ESPOL) that are specifically intended to provide access to the underlying computer hardware. Application programs are developed in general-purpose languages such as Pascal, which enables the application to run on several systems using the same code. Certain languages, for example, C, are utilized for both system and application software development.

Additionally, system and application software are activated differently. In general, system software is activated when a computer or other device is switched on and stays active until the device is shut off. After the computer is switched on, the end user initiates the application program. System software is required for application software to operate, but application software may run independently of system software.

In most situations, since system software operates in the background, end users do not interact with it. In contrast, end users do engage with application software they install it, start it up, use it to complete certain tasks, shut it down, and remove it.

Telecommunications (telecom)

Telecommunications management is rapidly becoming a primary responsibility for information technology leaders. The issues of executives span from network construction and connection to using information technology for competitive advantage. These leaders seek assistance and insights in a constantly changing world. Regrettably, they may get only a limited amount of assistance from information systems research. A thorough assessment of over 9800

publications spanning eleven years of MIS research revealed that academics have not put the same focus on telecommunications management as practitioners. Additionally, the bulk of telecommunications research focuses on lower-level management challenges, such as network installation, rather than on how to use information technology for competitive advantage. Additional study in telecommunications is required to offer insight into how to manage the telecommunications function for information systems executives.

Telecommunications is the science and practice of conveying data through electromagnetic waves. Contemporary telecommunications centers focus on the difficulties inherent in delivering huge amounts of data over great distances without incurring detrimental loss due to noise and interference. A contemporary digital telecommunications system's fundamental components must be capable of transferring voice, data, radio, and television signals.

Digital transmission is used to achieve high dependability and because digital switching systems are much less expensive than analog switching systems. To employ digital transmission, however, the analog signals that comprise the majority of voice, radio, and television communication must be converted to digital signals. (This step is skipped in data transmission since the signals are already in digital form; nevertheless, the majority of television, radio, and voice communication utilize the analog system and must be digitized.) Often, the digitized signal is processed via a source encoder, which utilizes a variety of formulae to eliminate superfluous binary information.

Following source encoding, the digitized signal is processed in a channel encoder, which inserts redundant data that enables the detection and correction of mistakes. The encoded signal is made appropriate for transmission by modulating it into a carrier wave and may be multiplexed with another signal. The multiplexed signal is then sent through a multiple-access channel. Following transmission, the procedure described above is reversed at the receiving end, and the data is retrieved.

Analog-to-digital conversion

The goal of voice, audio, and video transmission is high fidelity, or the finest possible replication of the original message without deterioration caused by signal distortion and noise. The binary signal serves as the foundation for generally noise- and distortion-free transmission. The binary signal is the simplest signal of any kind that may be used to transfer messages. It has just two potential values. Binary digits, or bits, 1 and 0 are used to represent these values. Unless the noise and distortion picked up during transmission are significant enough to affect the binary signal's value, the receiver can calculate the right value for flawless reception.

If the data to be conveyed is already in binary form (as in data communication), no digital encoding of the signal is required. However, voice communications via the telephone are not binary; nor is most of the data collected for transmission from a space probe, nor are television or radio signals collected for transmission over a satellite connection. Analog signals are those that continuously fluctuate between a range of values, and in digital communications systems, analog signals must be transformed to digital form. The process of converting analog signals to digital signals is referred to as analog-to-digital (A/D) conversion.

Executive information system

An executive information system (EIS), also referred to as an executive support system (ESS),[1] is a sort of management information system that enables and supports senior executive information and decision-making requirements. It enables quick access to internal and external data that is pertinent to the organization's objectives. It is often referred to as a particular kind of decision support system.

EIS places a premium on graphical displays and intuitive user interfaces. They provide robust reporting and drill-down functionality. EIS are enterprise-wide decision support systems that assist top-level executives in analyzing, comparing, and highlighting patterns in critical variables in order to monitor performance and discover opportunities and issues. In the marketplace, EIS and data warehousing technologies are convergent.

Historically, executive information systems were comprised of mainframe-based computer applications. The objective was to bundle a business's data and deliver sales performance or market research figures to decision makers such as marketing directors and chief executive officers who were not necessarily computer savvy. The purpose was to create computer programs that emphasized essential information in order to meet the demands of top executives. Typically, an EIS contains just the data necessary to enable executive-level decisions, not the whole company's data.

Today, EIS is used not just at the top of traditional corporate hierarchies, but also at lower organizational levels. Because some client service organizations have implemented cutting-edge enterprise information systems, workers may use their own computers to access corporate data and find information pertinent to their decision-making. This system ensures that pertinent information is communicated to both top and lower business levels.

EIS components can typically be classified as:

- ✓ **Hardware**

When discussing computer hardware for an EIS environment, we should place a premium on gear that satisfies the executive's requirements. Priority must be given to the executive, and the executive's requirements must be determined before hardware can be picked. The essential hardware for a standard EIS consists of four components:

Devices for data entering. These gadgets enable the executive to rapidly input, check, and update data.

The central processing unit (CPU), which is the most critical component of the computer system since it controls the other components.

Files used to store data. This section allows the executive to preserve essential business information and also enables the executive to readily look for past business information.

Output devices offer an executive with a visible or permanent record that he or she may preserve or read. This term refers to a device that produces visual output, such as a monitor or printer.

Additionally, the introduction of local area networks (LAN) enabled the availability of various EIS solutions for networked workstations. These systems need less maintenance and are more

cost effective in terms of computer hardware. Additionally, they provide access to EIS information to additional enterprise users.

- ✓ **Software**

Selecting the suitable software is critical to the success of an EIS. [reference required] As a result, the software components and their ability to integrate data into a single system are critical. A typical EIS consists of the following four software components:

Text: the majority of software documentation are text-based.

Database: executive access to both internal and external data is facilitated by heterogeneous databases running on a variety of vendor-specific and open computer systems.

Graphic foundation: visuals enable executives to see large amounts of text and figures. Time series charts, scatter diagrams, maps, motion graphics, sequence charts, and comparison-oriented graphs are all examples of common graphic forms (i.e., bar charts)

Model foundation Routine and specialized statistical, financial, and other quantitative studies are included in EIS models.

- ✓ **User interface**

An EIS must be efficient to access essential data for decision makers, hence the user interface is quite crucial. Several kinds of interfaces may be accessible to the EIS structure, such as scheduled reports, questions/answers, menu driven, command language, natural language, and input/output.

- ✓ **Telecommunications**

As decentralizing is becoming a trend in corporations, telecommunications plays a crucial role in networked information systems. Transmitting data from one point to another has become vital for developing a trustworthy network. In addition, telecommunications inside an EIS might expedite the requirement for access to dispersed data. It may be both via scientific and commercial methods.

D. CONCEPTS AND USAGES- ESTABLISHING A MANAGEMENT INFORMATION SYSTEM

Establishing a management information system

Information is a crucial resource for businesses' operation and administration. Access to pertinent information on a timely basis is critical to the efficient execution of management responsibilities such as planning, organizing, leading, and controlling. An organization's information system is similar to the human nervous system: it is the glue that holds all of the organization's components together and enables better functioning and survival in a competitive environment. Indeed, modern enterprises are information-driven.

The word "information system" often refers to a computer-based system that is intended to assist an organization's operations, management, and decision-making responsibilities. Thus, information systems in businesses offer decision makers with information assistance. Transaction processing systems, management information systems, decision support systems, and strategic information systems are all examples of information systems.

Information is made up of processed data that are relevant to a user. A system is a collection of components that work together to accomplish a shared goal. Thus, a management information system gathers, transmits, analyses, and saves data about an organization's resources, programs, and achievements. The system enables the translation of this data into management information for use by organizational decision makers. Thus, a management information system generates data that assists an organization's management activities (Davis & Olson, 1985; Lucas, 1990; McLeod, 1995).

Information is data that has been contextualized and given to a receiver for the purpose of decision-making. The exchange and receiving of intelligence or knowledge is referred to as information. It appraises and informs, surprises and stimulates, alleviates ambiguity, provides extra possibilities or assists in the elimination of ineffective or irrelevant ones, and encourages and stimulates persons to action. When you wish to reach a friend, his or her telephone number is a piece of information; otherwise, it is simply another bit of data in the telephone directory.

Computers have simplified the processing function significantly. Computers can rapidly process large amounts of data, assisting in the conversion of data to information. The system receives raw data and transforms it into the system's output, which is information to assist managers in their decision-making.

Relevance, timeliness, correctness, cost-effectiveness, dependability, usefulness, exhaustiveness, and aggregation level are all qualities of excellent information. Relevant information is that which contributes to enhanced decision-making. Additionally, it may be significant if it reinforces a prior judgment. If it has no bearing on your issue, it is irrelevant. For instance, if you are planning a vacation to Paris in January, knowledge regarding the weather in Paris in January is relevant. Otherwise, the data is irrelevant.

The term "timeliness" relates to the currency with which people are supplied with information. The time interval between the occurrence of an event in the field and its presentation to the user is referred to as the currency of data or information (decision maker). When this period of time is very brief, the information system is referred to as a real-time system.

The accuracy of data is determined by comparing it to real occurrences. The critical nature of reliable data differs according to the sort of choice that must be taken. Payroll data must be accurate. Approximations will just not do. However, a broad estimate of staff time spent on a given task may suffice.

Because information has a significant influence on decision making, its worth is inextricably linked to the choices that follow from its utilization. Information does not have a universal absolute value. It’s worth is contingent upon who uses it, when it is utilized, and under what circumstances it is used. Information is comparable to other commodities in this regard. For instance, a drink of water has a different value for someone who has been disoriented in the Arctic glaciers than it does for a wanderer in the Sahara Desert.

Economists differentiate value from the cost or price of a commodity associated with its production or acquisition. Obviously, a product's value must exceed its cost or price in order for it to be cost effective.

Economists and statisticians established the idea of information's normative value, which is taken from decision theory. The theory's fundamental assumption is that we always have some prior information about the occurrence of events that affect our judgments. Additional information may alter our perception of the occurrence probability, hence altering our choice and the anticipated pay-out from it. Thus, the value of new knowledge is the difference in anticipated pay-out that results from less uncertainty about a future occurrence.

Choices are aided by information, actions are triggered by decisions, and actions have an effect on the organization's accomplishments or performance. If we can quantify performance differences, we can track the influence of information, given that the measurements are conducted accurately, the connections between variables are clearly defined, and the impacts of irrelevant factors are separated. The difference in performance that is assessed as a result of informative elements is referred to as the realistic value or disclosed value of information.

For the majority of information systems, especially those supporting middle and upper management, the ensuing choices often entail occurrences that are not precisely specified and contain quantifiable probability. Often, the decision-making process is opaque, and the consequences are multidimensional and incomparable. In these instances, we may either do a multiattribute analysis or generate an overall subjective value. Subjective value represents people's overall perceptions of information and their willingness to pay for individual pieces of information (Ahituv, Neumann, & Riley, 1994).

Simon (1977) defines decision making as a four-step process comprised of four stages: intelligence, design, choosing, and review. The intelligence stage is concerned with the gathering, categorization, processing, and display of data about the organization and its surroundings. This is important in order to recognize circumstances that need decision-making. The decision maker proposes potential alternatives during the decision stage, each of which entails a series of activities to be done.

The intelligence stage data is now utilized to estimate likely outcomes for each choice using statistical and other models. Additionally, each option may be evaluated for its technical, behavioral, and economic viability. At the selection step, the decision maker must choose one of the choices that will most effectively contribute to the organization's objectives. Past decisions may be reviewed throughout implementation and monitoring to ensure that the management learns from their errors. Information is critical at each of the four phases of the decision-making process.

Differences between data and information

The phrases "data" and "information" are often used synonymously. There is, however, a slight distinction between the two.

In a nutshell, data may take the form of a number, symbol, letter, phrase, code, graph, or any combination thereof. By contrast, information is data that has been contextualized. Humans make extensive use of information (such as to make decisions, forecasts etc).

A computer is a fundamental example of information. A computer converts data to information via the use of programming scripts, formulae, or software programs.

Data is interpreted differently in different areas. In its simplest form, data is a collection of various symbols and letters whose meaning becomes apparent only when they are connected to context. Data are generated by the collection and measurement of observations. Generally, machines are used to transmit, receive, and process data. The distinction between data and information often occurs as a result of the fact that information is created from data. Additionally, statistics are often understood as facts in the colloquial sense and are therefore classified as information. It is worth noting that although computers are quite adept at crunching data, they are just now learning to make sense of it in order to extract insight through Machine Learning.

The term "data" refers to a collection of unstructured facts and information such as text, observations, figures, symbols, and descriptions of objects. In other words, data does not serve any function and is meaningless on its own. Additionally, data is quantified in terms of bits and bytes which are the fundamental units of information used in computer storage and processing.

By integrating data into a context, it becomes more complicated and becomes information. Information imparts knowledge about facts or people. Example of information: When the identity of the individual to whom the date of birth belongs is unknown, the information about the date of birth has very little value. By adding more information like as a name, interconnected bits of information, and context, knowledge may be represented.

Information is data that has been processed, organized, and structured. It contextualizes facts and facilitates decision-making. For instance, a single customer's purchase at a restaurant is data; it becomes information when the firm is able to determine which meal is the most popular or least popular.

To put it simply, data is an unstructured depiction of basic facts from which information may be retrieved.

Characteristics of information

Each piece of useful knowledge has the following characteristics:

- ✓ Subjectivity:

Information's worth and utility are extremely subjective since what constitutes information for one person may not constitute information for another.

- ✓ Relevance:

Only relevant information - that is, information that is important and meaningful to the decision maker - is useful.

- ✓ Timeliness:

Information must be supplied to the appropriate person at the appropriate time and location.

- ✓ Accuracy:

Information must be error-free since incorrect information may lead to bad judgments and decrease consumers' trust.

- ✓ Correct data format:

To be valuable to the decision maker, information must be presented in the appropriate manner.

- ✓ Completeness:

Complete information is defined as that which enables the decision maker to address the situation at hand successfully.

- ✓ Accessibility:

Information is worthless if it is not easily available to decision makers in the format required at the time it is required.

Value of Information in Management Information System

The idea of information value is a rather nebulous one since information does not have a universal worth. It's worth is determined by who uses it, when he uses it, and for what purpose he uses it. Any evaluation of the value of information must thus take into account the value of the decision-making that is facilitated by the information.

Consider two individuals who are stranded in the Sahara Desert. One individual has an ample amount of drinking water (much more than he could ever need), whereas another has depleted his supply. If one approaches these two persons with knowledge about a nearby drinking water well, such information will clearly be more valuable to the one who has depleted his water supply. For the person who is thirsty, this knowledge is critical at that moment in time since it will decide whether he survives.

If the knowledge reaches this thirsty guy late and he dies of thirst, the information's value is reduced to zero. As a result, we can observe how the same piece of knowledge may have a different meaning for various individuals at different moments in time. As a result, it is reasonable to assume that information has a relative worth. Information has no absolute worth.

However, the conventional mathematical and economic explanation for the value of knowledge implies that if an event happens with a low probability of recurrence and the information about its existence is known, the information is valuable. For instance, if the reader of this text learns that an earthquake of 10.5 magnitude on the Richter scale is about to strike India, and that the epicentre of the earthquake will be exactly where he is, that information is more valuable to him than learning (say) that he must pass his BCA exam in order to enrol in the MCA course. In the first scenario, the knowledge is more useful to him since he is not anticipating it, but in the later example, he already knows the information with confidence and fully anticipates it, diminishing the value of the information. All market mechanisms are based on this information model.

This was previously discussed in the preceding chapter, and as Eq.1 indicates, the value of knowledge about an event is equal to the negative logarithm of the event's likelihood of occurrence. Thus, the more improbable the occurrence, the greater its informational worth, if presented properly. This is also reflected in our behavior, since ages of evolution have built us in such a way that we place a higher premium on improbable occurrences.

In a gaming environment, such as horse racing, if the chances of a horse winning the race are higher, the reward for that horse is lower. Similarly, if a stock is expected to beat the market, the price payback is not large; nevertheless, if a stock is expected to underperform, the price

payoff becomes quite high. Thus, we can see that the problem of information's worth is multifaceted.

Normative Value of Information

Marschak (1971) and McGuire (1972) contributed fundamental work to this area of study. This notion has been extended further in decision theory, with the essential premise being that we always know some early information about the occurrence of events relevant to our judgments. This knowledge or information is represented by an a priori probability of occurrence assignment to the event and hence a computed pay-out. The a priori probability may be objective or subjective, and when further information becomes available, the probabilities are adjusted, leading in a change in the predicted payoffs. This technique, however, is best suited for theoretical debates since its practical usefulness is limited. For such circumstances, the issue must be thoroughly organized, which is uncommon in management.

Subjective Value of Information

It is the subject-specific perspective on the information that is accessible. It is the information's subjective sense or impression. This subjective approach to value differs significantly across people. No probabilities are computed during the subjective evaluation of information. Subjective value of information refers to an individual's (receiver's) overall assessment of the information's substance.

Decision-making process

Decision making is the process of selecting decisions via the identification of a problem, the collecting of information, and the evaluation of various solutions.

By collecting pertinent information and identifying options, a step-by-step decision-making process may assist you in making more careful, considered judgments. This strategy enhances the likelihood that you will choose the most pleasing choice.

- ✓ **The first step is to ascertain the choice**.

You recognize that you must make a choice. Make a concerted effort to clarify the nature of the choice you are about to make. This first step is critical.

- ✓ **Step 2: Compile pertinent data**

Prior to making a choice, gather essential information: what information is required, the best sources of information, and how to get it. This level includes internal as well as external "labor." Certain information is internal; you'll seek it out via a self-assessment procedure. Other information is derived from other sources: it may be found online, in books, from other people, or from other sources.

- ✓ **Step 3: Identify potential substitutes**

As you gather data, you're likely to find numerous different courses of action, or options. Additionally, you may use your creativity and extra knowledge to create new possibilities. This stage will include a list of all feasible and desired choices.

- ✓ **Step 4: Weigh the evidence**

Utilize your knowledge and emotions to visualize what it would be like if you followed through on each of the possibilities. Evaluate if each option would meet or satisfy the requirement indicated in Step 1. As you go through this arduous internal process, you will develop a preference for particular alternatives: those that seem to have a greater chance of achieving your objective. Finally, prioritize the possibilities according to your personal value system.

- ✓ **Step 5: Select from a variety of choices**

After weighing all of the data, you are ready to choose the option that seems to be the greatest fit for you. You may even combine several possibilities. Your selection in Step 5 is very likely to be identical to or close to the alternative at the top of your list at the conclusion of Step 4.

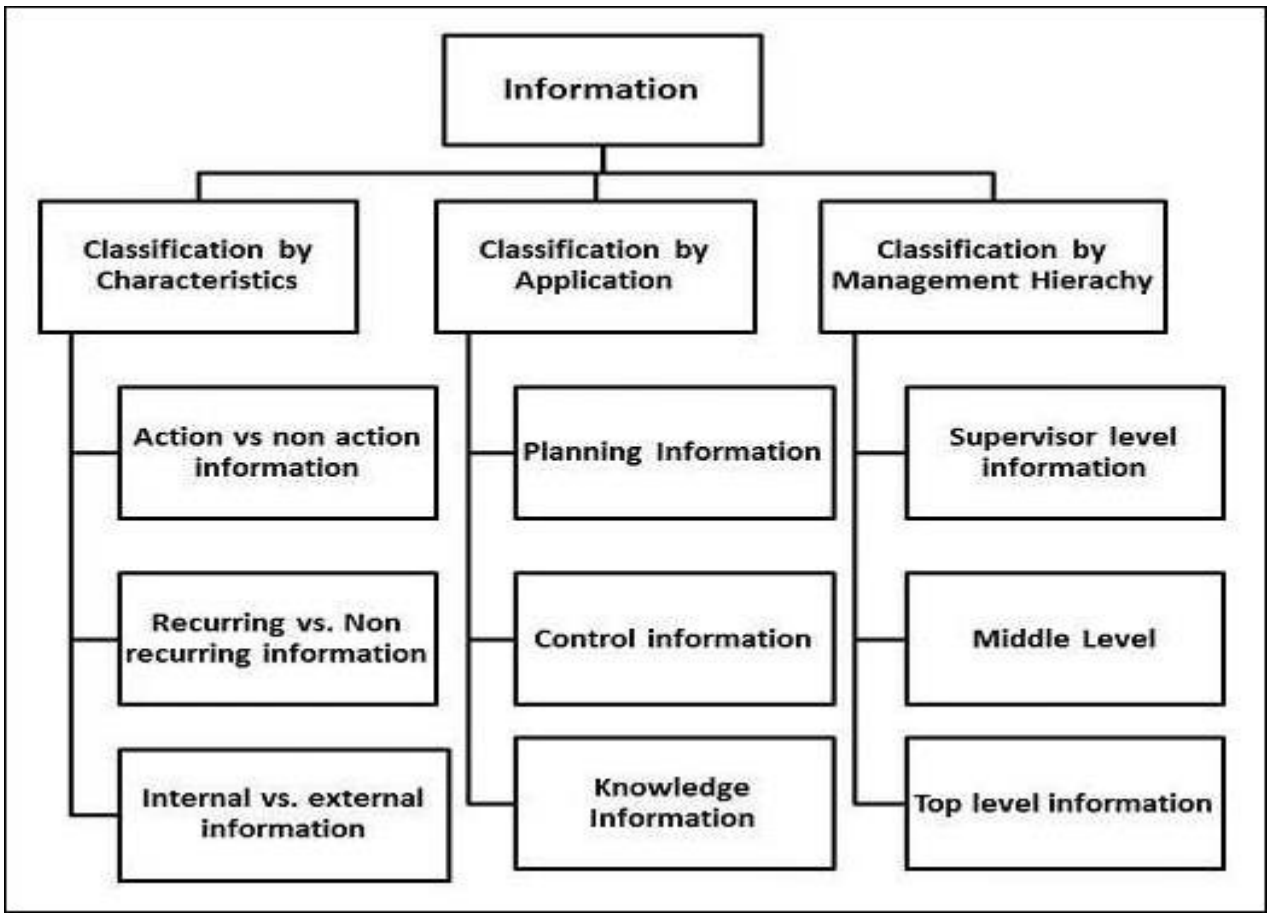
- ✓ **Step 6: Take action**

You are now prepared to take constructive action by implementing the solution you selected in Step 5.

- ✓ **Step 7: Evaluate your choice and its repercussions**

Consider the outcome of your choice and determine whether or not it satisfied the demand specified in Step 1. If the choice does not satisfy the indicated requirement, you may choose to redo some parts of the process in order to reach a different conclusion. For instance, you may want to obtain extra or somewhat different information or consider new choices.

MIS - Classification of Information



Classification by Characteristic

According to Anthony's management categorization, information utilized in business for decision-making is often classified into three types:

Strategic Information is concerned with long-term policy choices that define a business's goals and monitors how successfully those objectives are accomplished. For instance, strategic information encompasses the acquisition of a new facility, the development of a new product, and the diversification of a corporation.

Tactical Information Tactical information refers to the data required to exercise control over corporate resources, such as budgeting, quality control, service levels, inventory levels, and productivity levels.

Operational Information Operational information is concerned with information at the plant/business level and is used to guarantee that certain operational duties are completed as planned/intended. This category includes a variety of operator-specific, machine-specific, and shift-specific quality control inspections.

Application-Specific Classification

Information may be classified according to its intended use.

Planning Data These are the data required to define standard operating procedures and standards inside a company. This data is utilized to plan any activity's strategic, tactical, and operational aspects. Time standards and design standards are examples of this kind of information.

Control Data This data is required in order to create control over all company operations through a feedback system. This data is used to manage the accomplishment, type, and use of critical processes within a system. When such data indicates a divergence from set norms, the system should trigger a decision or action that results in control.

Knowledge is defined as "knowledge about information." Knowledge is obtained via experience and education, as well as through the analysis of archive material and research investigations.

Organizational Information Organizational information is concerned with the environment and culture of an organization in relation to its goals. Karl Weick's Organizational Information Theory highlights the need of an organization reducing its ambiguity or uncertainty via cautious collection, management, and use of information. This information is utilized by every member of the company; examples include employee and payroll data.

Functional/Operational Data This is data that is particular to an operation. For instance, in a manufacturing facility, daily schedules relate to the specific assignment of work to machines or operators to machines. It would be the duty roster of numerous staff in a service-oriented firm. This data is mostly used inside the company.

Database Information A database is a collection of enormous amounts of data that has a variety of uses and applications. Databases are used to store, retrieve, and manage this information. For instance, several users may access material specifications or supplier information.

Classification as per Business Function

TPS is a transaction processing system that handles transactions and generates reports. It is a term that refers to the automation of routine, fundamental tasks that support company operations. It provides no information to the user to aid in decision-making.

TPS makes use of and generates data in the manner shown in the following or as a consequence of the diagram.

TPS has previously been approached to serve as the administration's information system. Prior to the introduction of computers, data processing was carried out manually or with basic machinery. The TPS domain is positioned at the bottom of the management structure of an organization.

As an example of a management information system (MIS), MIS is a well-known information system that organizes data and transforms it into relevant information. A supervisory information system's data inputs are TPS. The information created by the information system may be utilized for operational purposes, strategic and long-range planning, and business intelligence. Short-term planning, supervision, and control, as well as other managerial issue solving, include processing in support of a broad variety of organizational activities and management processes. MIS is capable of assisting with analysis, planning, and decision-making. A company's functional areas include marketing, manufacturing, human resources, finance, and accounting.

A decision support system (DSS) is an information system that facilitates the submission of official requests to be considered for a job or to be permitted to do or have something. This helps in decision-making. DSS should be oriented on planning, examining possibilities, and conducting a trial-and-error search for a solution. A decision support system's components include a database and software. Finance, manufacturing, and marketing are just a few of DSS's primary application areas.

DSS and MIS may be separated by the manner in which information is handled. MIS transforms data into information. DSS analyses data to assist managers in making decisions.

Executive Support System (ESS): An ESS is a kind of management information system, which is a subset of DSS; an ESS is specifically designed to assist the chief executive officer of an association in making decisions. It encompasses a variety of decision-making styles, but is more focused and adult-oriented.

Office Automation Systems (OAS): The term "office automation" refers to the use of computers and communication technologies to perform administrative tasks. By offering secretarial help and enhanced communication capabilities, office automation systems are intended to increase the productivity of workers at different levels of management.

The following are the two primary classifications of office activities, namely

- ✓ Clerical staff members such as clerks, secretaries, and typists perform these functions.
- ✓ Executives' responsibilities (managers, engineers or other experienced like economist, research etc.)

The OAS's primary functional activities are as follows:

- Typing
- Mailing
- Meetings and conferences scheduling,
- Maintaining a calendar, and
- Document retrieval

The following is a list of current activities (managerial category)

- Conferencing.
- Controlling output and generating data (messages, memos, reports, and so on).

A businessperson is someone who is employed or trained for a job. Systems: These systems are a sort of knowledge-based information system that is widely used. These are modern information systems that are based on artificial intelligence. A business professional system is a strategy-based information system that acts as an expert by using its strategic knowledge of a particular, difficult application area. A professional system's primary components are as follows:

- Base de connaissances
- Engine of Interaction
- User Interface

Predictive Information System for Management

Predictive information systems allow users to make inferences and predictions that are useful in making decisions. It is feasible to gain information helpful for generating predictions or drawing conclusions if the data from the preceding instances is used in this way.

E. INFORMATION SYSTEMS IN BUSINESS CONTEXT

Project governance

In the project management world, the phrase "project and program governance" is thrown about a lot. A rising tendency is that when a project fails, project governance seems to be the core cause of the project's failure.

Project governance encompasses all of the critical components that contribute to a project's success. This is not, however, a one-size-fits-all situation. There are eight components that must be addressed when tailoring project governance to an organization's particular requirements. These elements will have an impact on how you design, execute, monitor, and regulate the governance structure for your project, program, or portfolio.

According to A Guide to the Project Management Body of Knowledge, project governance is an oversight role that is linked with the organization's governance model and includes the project life cycle." This sentence has two key parts that must be highlighted:

Alignment with the organization's governance: A thorough knowledge of the project's environment is required to guarantee that it is compatible with the existing organization's governance. When creating (1) the project governance structure, (2) roles and duties, and (3) stakeholder participation and communication, this congruence is critical. These requirements must be satisfied prior to the start of the project.

The governance plan's longevity, monitoring, and control: These three elements are realized during the project's life cycle. The project/program manager is responsible for ensuring that the governance plan is followed throughout the project, as well as monitoring and controlling its efficacy. The project manager must ensure that there are enough (4) meetings, (5) reporting, (6) risk and problem management, (7) assurance, and (8) project management control methods when monitoring and regulating the project governance framework.

There has been a gravitational drive toward robust project governance in recent years. With scandals like ENRON, Tyco International, and WorldCom, this has become much worse. The Sarbanes-Oxley Act was enacted in response to a lack of oversight in these businesses (Muller, 2009). This law is an excellent illustration of governance, and we see it in action every day as it establishes corporate norms, regulations, reporting, and supervision, all of which trickle down to the project team. This act exhibits the purest form of government.

Many project managers have battled with defining, validating, and quantifying the return on investment in creating project governance, as well as identifying how to make the project governance framework repeatable while still being responsive to the project's individual needs. How do you make project and program governance dynamic while yet being repeatable? This is a conundrum that the project management community constantly tackles.

At the start of a project, developing and implementing project governance is critical. Project governance is basically a "recipe" on how to run a project for the project manager. The eight major governance components are defined in Exhibit 1 along with how they are translated into the project management Process Groups. These eight elements are required for each project’s success, must be investigated, and examined.

Eight Governance Components and Their Applicability to the Real World

- **Models of Governance:**

The project manager must examine the level of rigor that you want to add while designing an appropriate governance model that supports the company. Stakeholders may be irritated by overzealous governance models, while a lack of project governance can lead to a lack of stakeholder involvement or false escalations.

Choosing the best governance model is a difficult issue. However, based on past experience, the organization should create a baseline of important project governance features depending on the project's scope, duration, complexity, risk, stakeholders, and relevance to the company. A basic tool that does a rapid analysis based on some of the aforementioned indications should be available to determine how aggressive your governance structure should be and which components are required.

- **Responsibilities and Accountability:**

The project manager's duties revolve on defining accountability and responsibilities. The efficacy of meetings, the change control process, risk assessment, and the communication strategy will all suffer if accountabilities and duties are not defined. The project manager must specify not just who is accountable, but also who is responsible, consulted, and informed for each of the project's deliverables when establishing accountability and duties.

- **Involvement of Stakeholders:**

Understanding the project environment is critical when laying the groundwork for your governance strategy. The first step is to make a list of all the people that are involved. This may seem to be a difficult and inane activity, yet it is crucial. If one stakeholder is left out, the project will be derailed and will have a negative effect.

Stakeholders come in many shapes and sizes. The project steering committee, PMO, sponsors, suppliers, government boards, the project team, company owners, and so on are examples of these. Stakeholders are everyone who might be affected by the project's deliverables. The project manager must first identify the stakeholders, their interests and expectations, and, most importantly, how to interact with them.

- **Communication with Stakeholders and Meetings and Reporting:**

Once all of the stakeholders have been identified and their interests and expectations have been outlined, the communication strategy must be devised. All relevant stakeholders get succinct, efficient, and timely information from a well-formulated communication strategy.

The project manager must ensure that there is a proper mix of meetings and reports after the communication strategy has been established. This must be specified so that each stakeholder is aware of the communication medium and content, as well as the frequency, owner/receiver, communication milestones, and decision gates. Furthermore, communication must be concise, accurate, and to the point.

- **Management of Risk and Issues:**

It's no secret that initiatives and programs are fraught with dangers and problems. It's impossible to predict what will happen, but a lack of planning will push the project team farther behind schedule. There must be agreement at the start of each project or program on how to identify, categorize, and prioritize risks and hazards. To be honest, how you deal with the danger or problem is more essential than the risk or issue itself.

- **Assurance:**

Project assurance guarantees that risks and concerns are properly controlled, as well as defining the metrics that support the project's/delivery program's confidence. Developing metrics that provide insight into project performance is an important part of assurance. Adherence to the business case, the efficacy of the change control and risk analysis process, the capacity to monitor variations in project scope, time, cost, and schedule, and quality evaluation and tracking correctness of the project plan are just a few of the indicators.

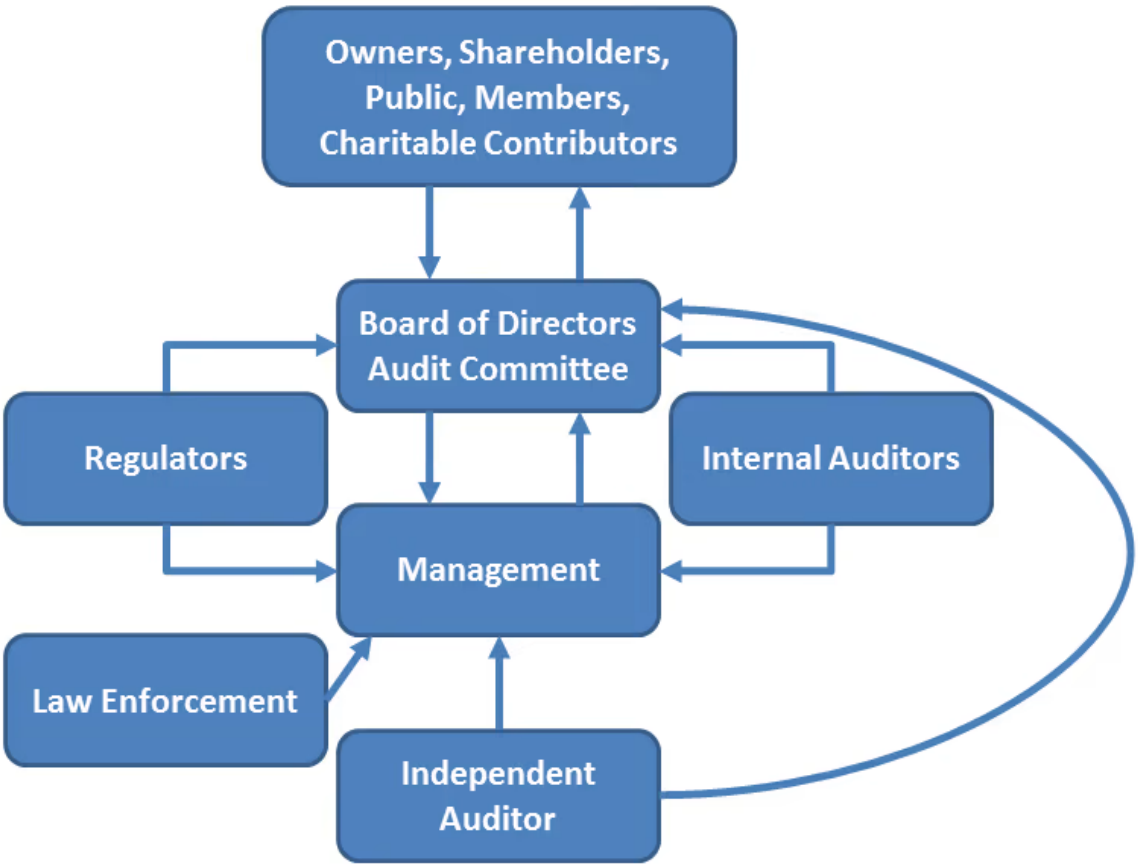
- **Control Process for Project Management:**

Because of continual checks and balances, this is the simplest component yet the most difficult to implement. All activities and metrics related with the project and programs are monitored and controlled, and performance is measured against the baseline scope, budget, time, and resources. This is not a one-time evaluation; the project/program manager must regularly monitor performance and respond to any deviations in a timely manner.

The governance processes

The methods used by representatives of the organization's stakeholders to give supervision of risk and control processes run by management are referred to as governance processes. Both

the fulfillment of organizational objectives and the maintenance of organizational value are directly influenced by the monitoring of organizational risks and the assurance that controls appropriately minimize such risks. For successful stewardship, those executing governance duties are responsible to the organization's stakeholders.



We believe that good governance entails that every human, organizational, technical, and financial resource works to support and contribute to the achievement of your mission and vision in a way that is verifiable, measurable, efficient, and effective, as well as in accordance with your principles, policy directives, and constraints.

We assist enterprises in fine-tuning their current foundation. We examine the present social, political, economic, and regulatory context in which the organization works as a first step in enhancing governance. The purpose and governance requirements of any organization will be shaped by social, political, and economic pressures.

Our strategy is based on the G20/OECD Corporate Governance Principles. It provides the foundation for a solid corporate governance structure. We tailor governance rules and regulations to the realities of the company.

Enterprise architecture (EA)

An enterprise architecture (EA) is a conceptual model of an organization's structure and functioning. The purpose of enterprise architecture is to find the most effective means by which a business may accomplish its present and future goals. Enterprise architecture is the process of evaluating, planning, developing, and ultimately implementing an enterprise's analysis.

Enterprise architecture aids enterprises undergoing digital transformation by focusing on the integration of legacy systems and processes in order to create a seamless environment. The usage of EA frameworks increased in reaction to the fast rise of business technologies throughout the 1980s, when company strategy required a mechanism for responding to rapid technological growth. Later, this method was extended to include all aspects of a corporation, not simply information technology (IT). This ensures that the rest of the company is aligned with digital transformation.

Because enterprise architectural concepts vary, it will appear differently in each company. Additionally, various segments of an organization may have varying perspectives on EA. For instance, programmers and other technical information technology workers see enterprise architectural plans in terms of the infrastructure, application, and management components they handle. Enterprise architects, on the other hand, are still responsible for conducting business structure analyses.

Enterprise architecture's critical role

Enterprise architecture enables many divisions of a corporation to comprehend the overall business model and define business issues and dangers. As a result, enterprise architecture plays a critical role in the unification and coordination of departmental activities within a company. Accessing and comprehending business capabilities should also assist people in identifying gaps in their company, allowing them to make more educated choices.

Enterprise architecture's purpose and objectives

Enterprise architecture's primary objective may be to build a map or blueprint of an organization's structure and activities. This blueprint should contain information such as a map of the organization's information technology assets and business processes.

Additionally, we have a same purpose of increasing team alignment and standards. This may be accomplished in part via the unification of work environments across teams and organizations. Typically, guidance is provided in accordance with an organization's business needs.

The process of enterprise architecture

Michael Platt, a director in Microsoft's strategic projects department, describes enterprise architecture as encompassing four perspectives: business, application, information, and technology. The business viewpoint establishes the methods and standards that govern the day-to-day operations of the firm. The application viewpoint specifies the relationships between the organization's procedures and standards. The information viewpoint identifies and categorizes the raw data (document files, databases, graphics, presentations, and spreadsheets) that an organization needs to function effectively. The technological viewpoint specifies the organization's hardware, operating systems, programming, and networking tools.

The phrase may have a variety of connotations for professionals working in a variety of fields and with a variety of different EA frameworks. For example, programmers and other technical information technology workers see enterprise architectural initiatives through the lens of the infrastructure, application, and management components over which they have authority.

When referring to the hardware and software components of a design, high-level programmers will use the term enterprise architecture. A website's infrastructure may include a web server, a database, a NoSQL database cache, API endpoints, and a content delivery network.

For technical enterprise architecture descriptions, the context of software architecture, system architecture deployment types, and other phases such as testing may be used.

Others may evaluate business architecture via the lens of quality qualities. These are mandatory characteristics of software that are unlikely to fit in a specification paper. Reliability, capacity, scalability, and security are just a few examples. Quality aspects are not functional requirements; rather, they serve as a means of determining acceptable operating conditions and the trade-offs required to achieve them.

In a business setting, enterprise architecture may require enterprises to differentiate between their enterprise architecture and the technological architecture necessary to construct and operate applications. This may be defined more precisely by working inside an enterprise architectural framework.

Enterprise architecture models and methodologies

Typically, enterprise designs are implemented as frameworks. There are several frameworks, and some will be a better match for a particular company than others. For instance, a framework that emphasizes consistency and linkages between diverse components of an overall company would be more beneficial to big firms with many moving elements than to small organizations. A framework such as the Unified Architecture Framework (UAF) may be appropriate in this instance.

Some example frameworks include:

The Zachman Framework for Enterprise Architecture which defines and standardizes IT architecture components by addressing six architectural points and six major stakeholders.

The Unified Architectural Framework (UAF) is a sophisticated yet adaptable enterprise architecture framework that is well-suited for military and government software development as well as commercial enterprises. It is implemented in the form of a UML profile.

Agile enterprise architecture which centers an organization around a malleable, extensible set of structures and procedures that may develop with the company. It has the potential to become a critical component in agile software delivery.

Federal Enterprise Architecture Framework (FEAF) which is a reference model for IT effectiveness that was launched in 1996. It was developed for the US government but may also be utilized by commercial businesses.

Several more frameworks are available, including The Open Group's Architectural Framework, the European Space Agency's Architectural Framework, the SAP Enterprise Architecture Framework, and the Ministry of Defence's Architecture Framework.

Enterprise architecture's advantages

Among the possible benefits of having an enterprise architecture are the following:

- Enhanced decision-making ability.
- Increased flexibility to shifting market circumstances or consumer needs.
- Efficiencies and redundancies in procedures are eliminated.
- Optimum use of organizational assets.
- Employee turnover is kept to a minimum.
- Sustain organizational changes with the purpose of redesigning and reorganizing.
- Facilitates the evaluation of architecture in relation to long-term aims.
- Can provide outsiders with perspectives on IT designs.
- Can aid in the harmonization of IT processes.
- Can aid in the simplification of finance teams; and
- Collaboration with project management is facilitated.
- Vendors, tools, and certifications for enterprise architecture

Numerous third-party suppliers and technologies provide enterprise architecture solutions, as well as certifications focused on certain abilities.

Orbus Software, Software AG, Planview, Avolution, and Sparx Systems are just a few examples of suppliers.

ServiceNow Project Portfolio Management is an example of an enterprise resource planning (ERP) platform that enables complete visibility. It can keep employees from many areas, from sales to IT, on the same page. It is quite simple to setup and enables users to choose a management style for each project, such as agile. It may, however, be challenging to employ for resource management.

Another example of an EA tool is Oracle Enterprise Architecture. The program assists users in building strategic roadmaps and architectures that facilitate the synchronization of business and IT. This software is motivated by commercial objectives and simplifies technical designs; nonetheless, novices may find it challenging to use.

Some example certifications include:

- Certified Technical Architect for Salesforce
- The Certified Architect of the Open Group
- AWS Solution Architect Certified
- Certification as a Professional Cloud Solutions Architect
- Training and certification for Dell EMC Cloud architects
- CISSP Certified Information Systems Security Professional

Commercial-off-the-shelf (COTS)

Instead of contracting custom-made or customized solutions, commercial off-the-shelf or commercially available off-the-shelf (COTS) items are packed or canned (ready-made) hardware or software that is modified afterwards to the buying organization's requirements.

The Federal Acquisition Regulation (FAR) defines "COTS" in the context of the United States government as a formal word for commercial things, including services, that are available in the commercial sector and may be purchased and utilized under federal contract. Microsoft, for example, is a supplier of commercial off-the-shelf software. While goods and building

materials may be considered COTS, bulk shipping is not. Services linked with commercial commodities, such as installation, training, and cloud computing, may also qualify as COTS.

COTS purchases are an alternative to bespoke software or one-off development projects – whether supported by the government or not.

Although COTS products may be utilized out of the box, they must be modified to meet business requirements and connected with existing organizational systems in practice. Extending the capabilities of commercially available goods via custom development is also a possibility, but this choice should be made carefully owing to the long-term support and maintenance consequences. Because such customized functionality is not supported by the COTS vendor, it introduces its own set of challenges during product upgrades.

Numerous government and industry initiatives have enforced the use of commercial off-the-shelf (COTS) goods, since they may result in considerable cost reductions associated with procurement, development, and maintenance.

ERP Enterprise Resources Planning systems

An Enterprise Resource Planning (ERP) system is a kind of software that is applied across a company to optimize data flow and streamline business operations. By implementing a high-quality ERP system, you can simplify your business's processes, cut expenses, boost productivity, and provide a better overall customer experience.

Your ERP system will streamline back-office operations by automating tasks like as adding, classifying, and grouping new goods, launching special offer campaigns, stock counts, and inventory replenishment, among others. Your system may be tailored to your operation's unique requirements.

With a complete retail management software system in place, you can quickly manage employee rosters, monitor work schedules, and control labor expenditures. The ERP system can compute sales commissions automatically and assist in loss prevention by identifying suspicious behaviour in your Point of Sale (POS) transactions.

An ERP system may gather consumer data, providing significant insight into your customers' purchasing behaviors. You may then utilize this data to develop customized offers based on their prior purchases. Additionally, you may create a loyalty program that rewards loyal clients.

Historically, the majority of ERPs were on-premises, meaning they were housed on retailer-owned hardware and servers. Internally, the retailer's IT staff was in charge of system updates, upgrades, maintenance, and security.

However, ERPs have migrated dramatically to the cloud in recent years. Cloud-based ERP (often referred to as SaaS ERP, with SaaS standing for "software as a service") offers various benefits over on-premises ERP:

It is updated automatically by the ERP vendor. The shop is not required to take any action as software ensures that you are always on the newest version, complete with all of its functions.

The ERP vendor is responsible for security and compliance with applicable laws.

Capital expense is minimized: no hardware or servers are required, and the cost of operating and maintaining the system is covered in the subscription fee.

It's simpler to add new features and install additional apps.

Enterprise Decision Management (EDM)

Enterprise decision management (EDM) is a business strategy that entails the use of analytical and rule-based systems to manage and deploy all operational choices, such as those involving workers, suppliers, and consumers.

By adding information-based choices based on historical behavioral data, as well as earlier judgments and their results, the computerized EDM movement revolutionized the business decision-making process.

EDM was born out of the necessity to assist large-scale corporate decision-making.

Enterprises implement EDM procedures to their business and technological infrastructures for a variety of reasons.

- To increase the rate of return on existing assets
- To raise the complexity of commercial decision-making
- To alleviate competitive stress caused by increasingly complex decision-making
- To seize a short competitive advantage chance (IT struggles to keep pace with business development)

Program in Project Management

A program is a set of initiatives that are handled together in order to obtain scale efficiencies. As with project management, program management entails the coordination of connected initiatives.

When the advantages of managing the collection surpass the benefits of managing the projects individually, they are packaged into a program. A similar notion is project portfolio management, which is a technique for managing and evaluating a large number of projects by combining them into strategic portfolios. Portfolios are then reviewed for overall efficacy, cost projections vs actual expenses, and alignment with the organization's bigger, strategic goals.

A program manager's responsibility is to coordinate all initiatives within a program in order to ensure that they correspond with the organization's strategy and long-term objectives. They supervise programs and evaluate deliverables to guarantee that each project's objectives are met.

Program managers should not be confused with project managers, who are responsible for the particular, short-term deliverables associated with specific initiatives.

A well-executed project management program may be very beneficial to a corporation. Among the advantages are the following:

Clarity: A program brings together several initiatives to accomplish a common aim. This ensures that project managers understand their specific deliverables and can organize their efforts in accordance with the program's strategic goals.

Efficiency: The program management procedure centralizes a group of initiatives. Program managers may utilize project management software to keep an eye on the status of all ongoing projects and to allocate resources appropriately.

Risk management: By allowing project managers to express pain points as they develop, it is possible to build a set of best practices for identifying comparable risks early and avoiding repeating errors.

F. INFORMATION SYSTEMS LIFE CYCLE MANAGEMENT-CASE STUDY

Information Lifecycle Management

Information is now the lifeblood of companies of all sizes. When data-driven businesses match their plans with market needs, they achieve success. They must understand and satisfy their consumers' desires and demands. Additionally, they may contact prospective clients in their target market who are interested in their goods or services, based on the precise data they gather and thoroughly analyze.

All companies deal with massive amounts of data that they acquire, create, or keep throughout the course of their existence and growth. Because information is a vital component of a business's productivity and profitability, it must be managed effectively.

A company gathers, generates, classifies, and archives data and then deletes it when it is no longer needed. As a result, information lifecycle management (ILM) is a key component of every growing and evolving firm.

ILM (a subset of data lifecycle management) is a best practice for managing corporate data at all stages of its existence. These technologies have the potential to significantly increase the performance of corporate applications while also lowering infrastructure expenses. Additionally, they may give frameworks for risk, compliance, and control of corporate data.

As a result, organizations may optimize their infrastructures via the use of ILM in conjunction with a tiered enterprise data management approach, while also providing a control framework for data governance and compliance.

Industry researchers point out that most of the data on which businesses depend is out of date. Due to the substantial decline in the value of data over time, it is necessary to implement information technology lifecycle management. It would guarantee that only current, active data consumes precious tier-one computing, processing, and storage resources and that all data is subject to compliance policies throughout its lifespan.

Information lifecycle management (ILM) is the process of monitoring and managing data (information) from creation through retirement in order to maximize its value and minimize its expenditures. Additionally, it tries to mitigate the regulatory and legal risks associated with data.

ILM enables information to be more aligned with business objectives by establishing service levels and management standards for metadata, data, and applications.

Throughout their existence, businesses must handle information and data. ILM begins with the creation or receipt of the record and continues with its use, maintenance, storage, and retrieval.

Finally, the information is disposed of, deleted, or preserved permanently in accordance with the agreed records retention schedule.

Additionally, organizations must handle all information with the utmost care and security, particularly personal and secret data. Best practices in information lifecycle management include storage optimization as well as techniques for enhancing data quality, usefulness, and security. Due to the massive amount of data that a normal business generates, data management solutions are critical for minimizing storage expenses. ILM manages data growth and expenses while enhancing application performance.

Additionally, ILM helps avoid out-of-compliance scenarios and minimizes legal risk by ensuring that data is held securely and for no longer than necessary. Data retention that is too lengthy incurs unnecessary expenditures and poses liabilities for the company. Additionally, it enforces compliance policies, avoiding audit fees.

Database archiving, test data management, data privacy/data masking, and data/application retirement are the primary tasks. However, any systematic application of rules to business data, as well as initiatives to eliminate, simplify, or enhance data security, may come within the ILM's general processes.

Information Lifecycle Management Process

The information management lifecycle begins long in advance of the establishment of a firm or organization. Prior to beginning, a business or organization performs market research, which entails amassing massive volumes of data in order to make key judgments. These include the product or service on which to concentrate your efforts (create, distribute, or manage), the client or market segment on which to concentrate your efforts, correct positioning, price, and current competition.

When the firm begins operations, it begins generating and collecting data, which it utilizes to further fine-tune its processes and procedures. It then classifies and saves the information that has been produced and handled in order to make it retrievable when needed.

As a corporation or organization grows in size and maturity, it archives older data and deletes outdated data. Additionally, it safeguards the stored data, ensuring that only authorized individuals have access to it. As a result, organizations constantly analyze and evaluate data in order to utilize it to develop strategies and decision-making processes.

The policy for information lifecycle management includes the overall data storage and information rules that govern management activities. ILM policies are dictated by business objectives and drivers, and they are typically integrated into an information lifecycle management framework that includes overall IT management and governance, change control processes, service level agreements (SLAs), and system availability and recovery times.

Information Lifecycle Management Goals

While managing data is a difficult undertaking, there are particular objectives that a firm must address. They serve as the basis for the system's uninterrupted and optimized information flow. ILM's primary aims are as follows:

- Security and Confidentiality of Data: The vast quantity of data in existence translates into an equally massive number of hazards and threats. Today, data is essentially the new money of the digital world, and its protection is critical for every person or organization. Thus, it is vital to safeguard data security, to prevent unauthorised third-party users from accessing it, and to safeguard it against virus or corruption.
- Availability: Given that data is the driving force behind the digital world, it makes sense to guarantee that information is easily accessible when required. Due to the cascade failures of operations that rely on information from prior processes, data availability is a fundamental aim of ILM.
- Integrity: Because data is utilized on a daily basis, it is susceptible to various changes and adjustments at each point of usage. Additionally, data-centric technologies such as cloud computing and the Internet of things are being implemented at a faster rate (IoT). Thus, data integrity is required to guarantee that all users have access to accurate information and that any modifications made are reflected in all instances.

Developing an ILM strategy may assist firms in determining how to handle their data, information, and storage media, as well as the appropriate level of security to use.

- Taking a Step Back: Without a backup, organizations cannot go back in time to make errors or locate and recover lost data, information, or applications. As a result, an information lifecycle protection plan is required to manage and coordinate the numerous life cycles within the framework of data and information lifecycle management.
- Considering the Future and the Past: Data is readable at various intervals or on a continuous basis. Businesses generate fresh data, metadata, copies, and copies of copies on a continuous basis. Thus, by recognizing that the basic data will stay static and unchanged in the future, organizations obtain insight into how to preserve it – for example, by periodically preserving static data.
- Concentrating on the Essentials: Businesses understand the similarities and differences in their data, information, and media storage, as well as the ILM and layered security that accompany them. As a result, businesses can create value and eliminate complexity and excessive expenses in order to continue growth. To do this, they begin by re-evaluating their information management processes, as well as their storage media, backup, and associated lifecycles.

Enterprise Content Management

Enterprise Content Management (ECM) is a methodical approach to content management that spans its whole lifespan. It provides the safe storage and distribution of unstructured data such as Word documents, PDFs, emails, and scanned photos.

From commercial supply chains to contract management, human resource management to government administration, the goal of using an ECM system is to increase corporate efficiency. Organizations may simplify and streamline work by reducing reliance on paper documents and categorizing unstructured information according to business requirements.

Through years of listening to our clients, we've identified consistent objectives for deploying ECM. Frequently, customers depend on ECM to:

- Reduce reliance on paper and simplify company operations.
- Improve client service and productivity.
- Reduce the risk to the organization.

Leading ECM systems, such as Laserfiche, achieve these objectives and more. The following are five critical components of an ECM solution:

1. Digitally capture documents

Content management starts with the collection and import of data into a secure digital repository. This may refer to any kind of document that is generated, recorded, saved, shared, or preserved, including but not limited to the following:

- Vendor invoices.
- Resumes submitted by job candidates.
- Contracts.
- Correspondence.
- Reports on research.

Several approaches for collecting these documents include the following:

- By using electronic forms, papers are converted to digital format at the moment of generation.
- Paper documents are scanned and stored in a digital repository.
- Managing digital information natively, such as Microsoft Office documents, PDFs, images, and video files.
- Organize and categorize documents from servers, shared devices, and network files automatically.

Traditional techniques of document capture are time consuming and costly. By capturing documents in a digital repository, many of the challenges associated with paper are eliminated: labour-intensive duplication, sluggish distribution, lost originals, and the difficulty associated with accessing files from offsite storage.

2. Store documents in a digital repository

Organizations may readily save any business-critical document in a digital repository using powerful ECM systems, which enables users to:

- Determine who has permission to access, modify, and create documents.
- Classify and find documents based on their metadata
- Organize your papers with a recursive folder system.

Enterprise content management's advantages extend well beyond document storage. Additionally, a content management system saves the time, expense, and complexity involved with handling documents that need retention schedules throughout their life cycle, aiding in regulatory compliance efforts. Indeed, a recent Nucleus Research found that content management systems provide a $6.12 return on investment for every dollar spent.

3. Retrieve documents, regardless of device or location

After securely storing an organization's documents, you can:

- Utilize full-text search to locate any document.
- Identify particular words or phrases included within the text, metadata, annotations, and entry names of a document.
- Utilize predefined search options to do searches on the creation date of documents, the identities of people who checked them out, and other information.

Enterprise content management software enables staff to respond rapidly to information demands from customers, citizens, and auditors, hence reducing time spent looking for information. Additionally, staff has fast access to the information necessary to make more informed choices on critical problems affecting your organization's bottom line.

4. Automate operations that are document-based

Automation enables firms to reduce manual chores such as photocopying or even dragging and dropping digital documents in order to do more with fewer resources. Certain ECM systems provide digital automation capabilities that enable the following:

- Automatically route papers to the appropriate recipients at the appropriate times.
- Staff members will be notified when papers demand their attention.
- Recognize mistakes prior to causing delays or requiring personnel to repeat work.

Every day, companies need the signing of purchase orders, the archiving of documents, and the approval or denial of employee vacation requests. Automation expedites the evaluation and approval of these key papers in the desired sequence. The ultimate result is more cost-effective, simplified, and error-free procedures.

5. Secure documents and reduce organizational risk

As compliance requirements tighten across a broad variety of sectors, firms are increasingly turning to ECM solutions to enhance records management procedures and mitigate risk. A content management system for enterprises must provide customisable security settings that enable firms to safeguard data against unwanted access or change. These settings should enable you to:

- Access to folders, documents, fields, annotations, and other granular document attributes may be restricted as necessary.
- Monitor system logins and logouts, the production and removal of documents, and password changes, among other things.
- Secure sensitive metadata by restricting access to certain files, templates, and fields.

Leading ECM solutions enable line of business departments to manage user access independently this means that sensitive human resources data remains within the human resources department, while private financial data remains within the finance department, even if the data is stored in the same repository.

While the majority of ECM systems have some of these five critical components, market leaders such as Laserfiche offer a comprehensive ECM solution that enables your firm to significantly enhance business operations. To learn more, schedule a demo.

Records Information Management

Records information management (RIM) is a business function that is responsible for the management of all company records throughout their life cycle.

A record is defined in this context as documentation of a business occurrence. Contracts, memoranda, physical and electronic files, marketing materials, reports, emails and instant messaging logs, website content, database records, and information on portable storage devices are all examples of possible documentation.

The records lifecycle is a series of distinct events that begin with the creation of a record and end with its archiving or destruction. Records management activities are defined in the ISO 15489: 2001 standard as "the generation, reception, maintenance, use, and dispose of records, as well as the procedures for collecting and keeping evidence of and information about business operations and transactions in the form of records."

Effective record management is critical for a variety of organizational functions, including enterprise information management (EIM), business intelligence/analytics (BI/BA), regulatory compliance, and disaster recovery. Records information management (RIM) are often referred to as records management (RM) and records and information management (RIM).

Managing the information lifecycle

The management of the information lifecycle entails ensuring that data is available to the people who need it and selecting how the data is preserved in accordance with the organization's current priorities. The management infrastructure must decide the optimal software, hardware, and storage media for the information at each step of its lifespan, as well as how those components change as the data progress through the lifecycle.

Stages in the information lifecycle

The information lifecycle, in general, consists of three stages:

- The data's generation and/or acquisition. The organization obtains information either via the creation of information by one or more persons or by the acquisition of information through emails, faxes, letters, and phone calls, among other methods.
- The data's publishing. Certain information must be publicized, whether in print or on an organization's intranet or public Web site.
- Data retention and/or deletion. Certain types of information must be stored for future use, while others have a defined life and may be deleted after they have fulfilled their function or are no longer useful to the organization.

G. DECISION MAKING

Managerial Decision-Making

Decision-making is a cognitive process that results in the choosing of a course of action from a variety of possible outcomes.

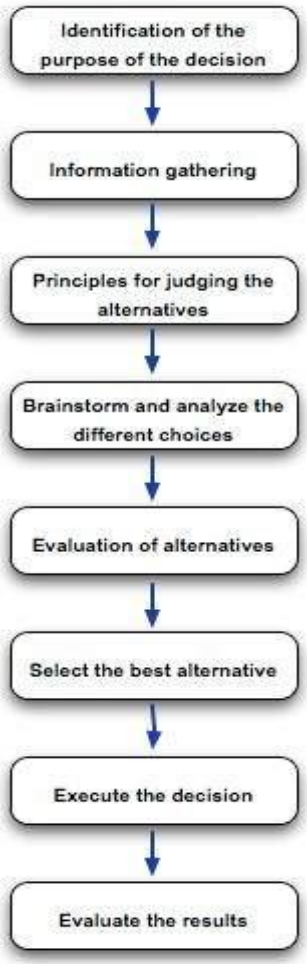
Any human being engages in daily decision-making. There are no exceptions to this rule. In corporate organizations, decision-making is both a habit and a process.

Profits arise from effective and successful choices, whereas losses follow from ineffective and failed ones. As a result, decision-making at the corporate level is the most crucial activity in every firm.

We pick one course of action from among many available possibilities throughout the decision-making process. We may use a variety of tools, tactics, and perspectives throughout the decision-making process. Additionally, we may make our own individual choices or choose a group decision.

Generally, decision-making is difficult. The majority of business choices are motivated by discontent or disagreement with another party.

Following are the major phases of the decision-making process. Each phase may be assisted by various tools and strategies.



- **Step 1: Determining the Decision's Purpose**

The issue is extensively evaluated in this stage. When it comes to determining the decision's purpose, there are a few questions to ask.

- What is the precise nature of the issue?
- Why should the issue be resolved?
- That are the parties who are impacted by the issue?

- Is there a deadline or a precise timeline for resolving the issue?

➢ **Step 2: Data Collection**

A business's challenge will include a large number of stakeholders. Additionally, there may be hundreds of variables involved and impacted by the issue.

While solving the issue, you will need to acquire as much information as possible on the elements and parties involved. Tools such as 'Check Sheets' may be utilized efficiently throughout the information collection process.

➢ **Step 3: Judging the Alternatives**

This stage establishes the baseline criteria for evaluating the options. When creating the criteria, both company objectives and business culture should be considered.

Profit, for instance, is a primary consideration in every decision-making process. Unless an extraordinary circumstance exists, businesses seldom make choices that lower profitability. Similarly, fundamental concepts pertinent to the issue at hand should be established.

➢ **Step 4: Brainstorm and Analyze Your Alternatives**

For this phase, brainstorming to generate all possible ideas is the best course of action. Prior to the idea generating stage, it is critical to identify the underlying causes of the issue and their priority.

This may be accomplished via the use of cause-and-effect diagrams and the Pareto Chart tool. The cause-and-effect diagram assists you in identifying all potential causes of the issue, while the Pareto chart assists you in prioritizing and identifying the reasons that have the greatest influence.

After that, you may proceed to generate all viable solutions (alternatives) for the current issue.

➢ **Step 5: Alternatives Evaluation**

Evaluate each possibility using your judgment principles and decision-making criteria. At this point, the judgment principles' experience and efficacy come into play. You must weigh the advantages and disadvantages of each solution.

➢ **Step 6: Decide on the Best Alternate**

Once you've completed Steps 1 through 5, this step is straightforward. Additionally, the best alternative pick is an educated choice, since you have previously followed a process to generate and choose the best alternative.

➢ **Step 7: Put the choice into action**

Convert your choice into a strategy or a series of actions. Execute your strategy either alone or with the assistance of subordinates.

➢ **Step 8: Assess the Results**

Evaluate the result of your choice. Determine if there is anything you can learn and then use to future decision-making. This is one of the most effective strategies for honing your decision-making abilities.

Process and Modelling in Decision-Making

In decision-making, there are two fundamental models:

- Models rationales
- Model normative

The rational models are predicated on cognitive judgements and aid in the selection of the most logical and reasonable choice. Various models of this kind include decision matrix analysis, Pugh matrix analysis, SWOT analysis, Pareto analysis, and decision trees, as well as selection matrix analysis.

A rational decision-making model follows the stages below:

- Defining the issue,
- Defining the critical criteria for the process and its outcome,
- Taking into account all viable options,
- Calculating the ramifications of all possible solutions and assessing their likelihood of fitting the requirements,
- Choosing the optimal choice.

The normative model of decision-making takes into account potential limitations associated with decision-making, such as time, complexity, uncertainty, and resource scarcity.

According to this approach, decision-making is defined by the following:

- Processing of restricted information - An individual can handle only a certain quantity of information.
- Judgmental heuristics - An individual may use shortcuts to facilitate decision-making.
- Satisfying - An individual may choose for a solution that is only "good enough."

Decision-Making in a Dynamic Environment

Dynamic decision-making (DDM) is synergetic decision-making involving interdependent systems in a changing environment, either as a result of the decision-prior maker's actions or as a result of circumstances outside the decision-control. maker's

These are more complicated and real-time decision-making processes.

Dynamic decision-making is watching how individuals utilized their experience to influence the dynamics of a system and recording the best judgments made as a result.

Analyses of Sensitivity

Sensitivity analysis is a method for allocating the uncertainty in the output of a mathematical model or a system to the many sources of uncertainty in the model's inputs.

From a corporate decision-making standpoint, sensitivity analysis enables analysts to discover cost drivers and other numbers necessary for making an educated conclusion. If a given number

has no influence on a choice or forecast, the associated criteria may be omitted, simplifying the decision-making process.

Additionally, sensitivity analysis is beneficial in a variety of different scenarios, like as

- Optimization of resources
- Collecting future data
- Recognize important premises
- To achieve the highest possible tolerance on produced components

Models, Both Static and Dynamic

Models that are static:

- Demonstrate the relative importance of different traits in a balanced system.
- Perform optimally in static systems.
- Make no allowance for time-related variations.
- Although it may not operate well in real-time systems, it may work effectively in a dynamic system that is in equilibrium.
- Reduce the amount of data involved.
- Are straightforward to assess.
- Produce outcomes more quickly.

Models that are dynamic

- Consider how data values vary throughout time.
- Consider the cumulative impact of system behavior.
- Calculate equations again as time passes.
- Can only be used in dynamic systems.

Techniques of Simulation

Simulating the functioning of a real-world process or system over time is a method. Simulation approaches may be used to aid management decision-making in situations when analytical methods are unavailable or impractical.

Several common business issue areas where simulation methods are used are as follows:

- Inventory management
- Issue with queues
- Production scheduling
- Techniques of Operations Research

Operational Research (OR) is a broad category of problem-solving methodologies that use a variety of sophisticated analytical models and methods. It contributes to more effective and informed decision-making.

It incorporates approaches like as simulation, mathematical optimization, queuing theory, stochastic-process models, econometric methods, data envelopment analysis, neural networks, expert systems, and decision analysis.

OR methods provide a description of a system by developing mathematical models of it.

Programming using Heuristics

Heuristic programming is an artificial intelligence subfield. It comprises of self-learning programs.

However, these programs are not ideal in nature, since they are built on experience-based problem solving strategies.

The majority of fundamental heuristic systems are built on pure 'trial-error' approaches.

Heuristics approach issue solving in a 'guess' manner, producing a 'good enough' solution rather than the 'best possible' one.

Collective Decision-Making

Group decision-making is a collaborative process in which members of a group make decisions together.

Group Decision Support System (GDSS) is a decision support system that assists a group of individuals in making decisions. It enables the free flow of ideas and information amongst group members. Decisions are taken with a greater degree of consensus and agreement, which results in a significantly increased probability of execution.

The following table summarizes the many kinds of computer-based GDSSs available.

This kind enables players to interact with one another through a network or a central database. To give assistance, application software may make use of widely shared models.

Participants congregate in a single location, referred to as the decision room. The objective of this is to improve participants' relationships and decision-making skills over a specified time period with the assistance of a facilitator.

Teleconferencing Groups are made up of geographically scattered members or subgroups; teleconferencing enables interactive communication between two or more decision rooms. This contact will include the transfer of electronic and audio-visual data.

Examples of decision-making in management

- **Decision-making in human resources**

Assume you are the CEO of a small e-commerce business. Your business is growing, and you need to employ the appropriate people to assist you in realizing your goal of becoming the world's premier online retail platform.

You'd need to recruit individuals that are knowledgeable and skilled in areas such as software development, marketing, operations, procurement, and logistics.

Because the firm is an internet start-up, you will not need to recruit personnel that will work entirely on-site. Additionally, you may hire competent location-independent individuals capable of providing online technical assistance and services.

By assuring an ideal balance of on-site and remote employees, you can quickly and cost-effectively perform the duties. Emails, chat discussions, and video exchanges may all help

maintain team spirit. This also enables you to hire people that may be dispersed across several physical places yet can collaborate digitally to generate game-changing solutions.

- **Decision-making in human resources**

Making a choice on manufacturing facilities is a common example of managerial decision-making.

As your firm develops and demand increases, you will be compelled to expand your manufacturing capacity. The next stage would be to determine the amount of capacity that needs to be installed to successfully satisfy demand. Additionally, you will need to determine the appropriate equipment and personnel to operate the manufacturing operations.

Your selection must be driven by the fact that the ultimate goal is to sustainably grow output while maintaining the ability to scale up or down without incurring a hefty expense.

- **Decision-making in marketing**

Most businesses undergo rebranding at some time throughout their travels. Typically, companies begin small, with limited local or regional reach and branding, but as they grow, the need for rebranding becomes apparent.

Frequently, logos, official mascots, and even names are altered to communicate a new identity, capabilities, and vision. Rebranding operations are excellent instances of great decision-making abilities since they consider corporate values, products, target audiences, cultural and social sensibility, and commercial objectives.

- **Decision-making in client servicing**

When a company is just starting out, the objective is to acquire as many projects and customers as possible. The conventional wisdom is that the more labor you do, the more money you earn. However, as shown by several decision-making skills instances, this strategy is not optimal in the long term.

For example, you may realize that you are devoting an inordinate amount of time and resources to an old customer who is not earning enough income to support such a high level of resource allocation. That customer may have been one of your very first clients and may have played a critical role in your business's early development. However, it is critical to adapt to changing times. Once you reach a certain size, the customer or project that succeeded initially may become unfeasible. As a result, difficult judgments must sometimes be made.

Economic feasibility

Economic analysis is a subset of cost-benefit analysis. It is the most often utilized approach for determining a new system's efficacy. Economic analysis is the process of determining the predicted advantages and savings from a proposed system and comparing them to the associated expenses. If the advantages exceed the costs, the decision to develop and deploy the system is taken. Before taking action, an entrepreneur must carefully balance the costs and advantages.

Economic study may raise the following questions:

- ✓ Is the system cost effective?

- ✓ Do the advantages exceed the costs?
- ✓ The expense of doing a comprehensive system analysis
- ✓ The cost of an employee's time in a firm
- ✓ Hardware cost estimate
- ✓ Estimated cost of software/development of software
- ✓ Is the proposal feasible in light of resource constraints?
- ✓ What savings are anticipated as a consequence of the system?
- ✓ Cost of workers' study time
- ✓ Cost of packaged software/development of software
- ✓ Alternative finance methods (rent/lease/purchase)

Before committing to a comprehensive system study, the concerned firm must understand the worth of the investment. If the short-term expenses are not outweighed by the long-term benefits or do not result in an immediate decrease in operating costs, the system is not economically viable and the project should be abandoned. If the anticipated benefits equal or surpass the expenses, the system is considered economically viable. Economic analysis is done to determine the proposed system's efficacy.

Economic feasibility will examine the anticipated expenses to see if they are within the predicted budget or whether the project will provide an acceptable return on investment. At this stage, the estimated expenses are merely a ballpark figure. Costs in detail are not necessary to assess economic viability. It is only necessary to ascertain if the project's expenditures can be kept within the intended budget or return on investment. A preliminary estimate of the project timeline is necessary to establish if the systems project can be completed within the specified period. The organization would need to establish the requisite timeline.

Types of Feasibility

Today, before you obtain any order to commence a project, you need an executive order, particularly if such a project might cost millions of dollars. For such executive order to be approved, there has to be a feasibility assessment on the specified project.

A feasibility study helps to establish whether a certain project will succeed or not. It is frequently undertaken before the real project starts, including the planning phase. A feasibility study is a crucial aspect to assess whether a project can go ahead.

The analyst evaluates three distinct forms of viability throughout the feasibility analysis process: technical, economic, and operational, which are all interconnected.

Technical Feasibility: During this analysis, the analyst examines the department's current computer systems (hardware and software) and decides if they are adequate for the proposed system. If they are insufficient, the analyst makes recommendations for the configuration of the needed computer systems. Generally, the analyst will seek two or three distinct configurations that each meet the critical technical criteria but have a distinct cost. Financial resources and budget are also addressed during a technological feasibility assessment. Technical feasibility is primarily concerned with determining if a project is technically possible, assuming that it is economically feasible.

Economic Feasibility: This is the most critical research since it establishes the proposed system's cost and benefits and compares them to the allocated budget. The budget should not

be exceeded by the cost of the project. The project's cost is comprised of the hardware, software, development, and implementation phases.

Cost/benefit analysis is a widely used technique for determining the predicted advantages of a proposed system and comparing them to the estimated costs associated with its development. If the analyst determines that the advantages outweigh the costs, they choose to continue developing the proposed system; otherwise, the analyst determines that the proposed system is economically unfeasible. The feasibility study shows both concrete (e.g., greater productivity, reduced operating costs, etc.) and intangible (e.g., enhanced organizational planning, increased asset utilization, etc.) advantages in a formal manner. In a following subsection, we will explore the cost/benefit analysis.

Operational Feasibility: Once economic and technical feasibility have been established, the project's operational feasibility must be determined. It is established during the operational feasibility study if the system will work in the manner desired by the user. Operational viability is contingent upon the availability of human resources for the system's development and deployment. It is determined if the system's development and execution need skilled and experienced staff. Participation of users is more necessary for assessing operational viability.

Social Feasibility: The social feasibility of a given project is determined by determining whether or not the public would accept it. This judgment often considers the likelihood that the proposed system change will be approved by the group immediately impacted by it.

Management feasibility is the process of determining if a given project is manageable. If management rejects a proposal or provides only rudimentary assistance, the analyst is likely to perceive the initiative as unfeasible.

Legal feasibility is the process of determining if a proposed project violates any existing Acts, Statutes, or forthcoming legislation. While the project may seem to be solid at first glance, a deeper examination may reveal that it violates various legal provisions.

Time feasibility is a word that refers to determining if a given project can be completed within a certain time period. A project that takes an unreasonable amount of time is almost certain to be rejected.

Following completion of the feasibility study, a document titled 'Feasibility Study Report' is created. Additionally to this report, the analyst presents the feasibility study to management through oral presentation.

Operational Feasibility Study

Operational feasibility is contingent upon the availability of human resources for the project and entails forecasting whether the system will be utilized after development and implementation.

Operational feasibility is a criterion that indicates how successfully a proposed system solves issues, exploits opportunities found during scope definition, and meets criteria defined during the requirements analysis phase of system development.

Cost-cutting programs that do not compromise the product's quality are an example of operational viability. Studies are conducted to ensure that programs may be implemented in

the existing manufacturing plant without requiring additional equipment or personnel. If more space, equipment, or employees are required, the system must enhance the way the product is viewed by customers. This provides for the additional manufacturing cost associated with the projected rise in sales and revenue.

Economic viability is a subset of operational viability. Everyone engaged with the manufacture and usage of the system, product, or program must understand it and be able to utilize it properly. Not only are feasibility studies conducted in the commercial sector, but also by all governmental institutions. If end customers do not understand the modifications made to a product or service, they are not deemed practical.

Operational feasibility assesses the organization's willingness to support the proposed system. This is perhaps the most challenging of the feasibilities to assess. It is critical to assess the management commitment to the proposed project in order to establish its viability. If management started the request, there is a good chance that the system will be adopted and utilized. However, it is critical that the employee base accepts the change.

The following are the critical questions that aid in determining a system's operational feasibility:

- Is the existing mode of operation suitable in terms of throughput and reaction time?
- Is the present mode capable of delivering timely, topical, accurate, and helpful structured information to end users and managers?
- Is the existing style of operation providing the firm with cost-effective information services?
- Could there be a cost savings and/or an increase in benefits?
- Is the existing method of operation effective in terms of safeguarding against fraud and ensuring the correctness and security of data and information?
- Is the existing style of operation making the best possible use of available resources, such as personnel, time, and the flow of forms?
- Is the existing mode of operation capable of providing dependable services?
- Are the services adaptable and scalable?
- Are present work practices and policies sufficient to support the new system?
- Will the system be implemented if it is developed?
- Personnel issues
- Labour objections
- Managerial resistance
- Conflicts and rules within organizations
- Acceptability in society
- Governmental regulations
- Is management supportive of the project?
- Are consumers dissatisfied with present business practices?
- Will it significantly cut the time required for the operation?
- Have users been engaged in the project's planning and development?
- Is the suggested method really beneficial to the organization?
- Is there an increase in overall response?
- Will information become inaccessible?

- Will the system have a significant impact on the customers?
- Legal ramifications
- How do end users see their position in the new system?
- Which end users or supervisors are likely to reject or abstain from using the system?
- How will the end-working user's environment change?
- Are end users and management capable of adapting to the change, or will they?

Operational feasibility refers to the ability to use, support, and execute required program, system, or project responsibilities. It encompasses everyone who designs or runs a system. To determine if a project or system is operationally viable, it must fulfill particular criteria. These criteria take the form of questions that demand specific responses.

Operational feasibility demands a thorough examination of the existing system. A system is operationally practicable when its development costs may be reduced without jeopardizing the system's quality or output. For example, if it is possible to boost worker productivity in a new firm by lowering working hours without sacrificing product quality, such an operation is conceivable.

To take advantage of operational feasibility, everyone in the manufacturing business must grasp how it works. You may do an operational feasibility analysis on both private and public organizations since it often focuses on a single essential purpose.

If, after an operational feasibility study, the system, product, or end-users do not grasp the program, the feasibility study's aim is undermined. In this case, the program or initiative is deemed unfeasible.

Legal and Contractual Feasibility

Legal feasibility establishes whether or not the proposed system violates a legal requirement. If this component is not addressed during the initial stages of a project, it may result in legal complications after completion.

The European Union has chosen a very different approach to internet privacy than the United States, which is market-driven. Individuals have almost complete control over how their acquired data is used under the EU's 1998 Data Protection Directive. Thus, if a European customer contributes personal information to an online retailer, such as an address, the company cannot lawfully send the purchaser an advertisement without first obtaining consent. Additionally, the directive forbids data transfers to nations outside the European Union that lack "adequate" privacy regulations.

Today's software is capable of monitoring every keystroke, file download, and Internet page that an employee views on his or her computer screen. According to a recent American Management Association poll of 840 US businesses, 60% currently utilize some kind of software to monitor their workers' incoming and outgoing e-mail, up from 47% in 2001. As a result, businesses may use some of these techniques to safeguard themselves against litigation. Employers desiring to undertake the monitoring program should inform their workers and require all employees to sign an acknowledgement, so that there is no doubt about an employee's expectation of privacy on computer systems.

Technical Feasibility

Technical feasibility assesses the expert system's technical difficulty and often entails analyzing whether the expert system can be implemented using cutting-edge methodologies and tools. In the case of expert systems, defining the shell in which the system will be created is a critical part of technological feasibility. The shell in which an expert system is developed may have a significant impact on its quality, making it critical to the system's success. Although the ideal properties of an expert system shell will vary according to the task and domain requirements, the shell must be sufficiently adaptable to allow for efficient integration of expert reasoning. Additionally, it must be simple to interface with current computer-based systems. Additionally, a shell with a graphical user interface encourages end users to interact with the system more often.

Technical Feasibility is the first phase in the feasibility stage. It entails the building of a functional model of the product or service. It is not required that the working model's initial materials and components correspond to those that will be utilized in the final product or service. The objective of the working model is to show that the product or service is functioning and producible to your satisfaction. Additionally, it gives a visual manner of communicating your notion to others.

A mechanical functioning model is a simpler notion to grasp and comprehend than software, e-commerce, or service-related items. E-commerce models must demonstrate the capacity to combine the computers, servers, software, and programming required to support the operational idea. Services should produce demonstrable advantages when bundled as a collection of value-added activities.

The following tasks must be done at the technical feasibility stage.

- Conduct a feasibility study
- Analyze the operating specifications
- Determine the existence of possible safety and environmental risks
- Conduct a preliminary feasibility study for production
- Conduct a preliminary evaluation of the production process
- Cost estimation for engineering prototypes

Technical feasibility analysis often yields information regarding the product or process's design, performance, manufacturing needs, and preliminary manufacturing costs.

Political Feasibility

A discussion of approaches for conducting systematic investigations into the political viability of policy-oriented forecasts. Political feasibility is described in three ways that are interdependent:

- An actor's power to influence and execute policies,
- A probability distribution for each policy option, and
- A range of "time-sensitive" policy alternatives.

Among the factors that influence political feasibility are the principal players' abilities and intents; public opinion and other relevant pressures; actor-actor interaction; and field

regulations, which are prone to change due to variables not included in the study. Three schemes are built from these preliminary findings that use the Delphi approach to provide policymakers with tools for dealing with time spans, probabilities, and diverse combinations of variables and assumptions that may occur when projecting political feasibility.

The purpose of determining political feasibility is to ascertain how important stakeholders within the organization evaluate the proposed system. The new information technologies have the potential to alter the power distribution and have political ramifications. As a result, those stakeholders who are opposed to the project may attempt to sabotage or interrupt it.

Political feasibility analysis studies the people and events that occur at each level of the political policy-making process and forecasts how a policy issue will likely be resolved as it proceeds through the policy process. Despite the dominance of policy analysis in the social sciences over the last decade or so, there has been almost little academic work on the examination of policy proposals' political viability.

Political scientists, by virtue of their primary interest with the design and influence of the policy-making process, have an unmatched obligation to develop a method for rigorously evaluating political feasibility. While all policy analysts, regardless of their academic backgrounds, should be concerned with political feasibility, political scientists should be especially cognizant of its critical role in influencing public policy. While forecasting the expected result of a dynamic policy process is inherently challenging, an examination of the political feasibility of a suggested alternative may shed light on the nature of the policy process and highlight the conditions that must be satisfied for an alternative to succeed.

Risk analysis

Risk analysis is the process of detecting and assessing possible problems that might have a detrimental effect on critical business efforts or projects. This approach is used to assist companies in avoiding or mitigating certain hazards.

Conducting a risk analysis entails examining the probability of unfavourable events occurring as a result of natural processes such as strong storms, earthquakes, or flooding, or as a result of deliberate or unintended human activity. A critical component of risk analysis is determining the potential for damage from these occurrences, as well as their probability of occurring.

- **What is the purpose of risk analysis?**

Risk analysis is used by businesses and other organizations to:

- Anticipate and mitigate the impact of unfavourable event-related damage.
- Examine if a project's potential risks are outweighed by its advantages in order to help in the decision-making process while deciding whether to proceed with the project.
- Reaction strategies for technology or equipment failure or loss due to adverse events, both natural and man-made; and
- Detect and plan for the effect of changes in the corporate environment, such as the potential of new rivals joining the market or changes in government regulatory policy.

- **What are the advantages of doing a risk analysis?**

Organizations must understand the risks connected with the usage of their information systems in order to secure their information assets effectively and efficiently.

Risk analysis may assist a business in a variety of ways. Depending on the nature and scope of the risk analysis, businesses may utilize the findings to assist in the following ways:

- Determine, assess, and compare the entire effect of risks on the firm, both financially and organizationally.
- Identify security gaps and decide the next measures necessary to reduce vulnerabilities and increase security.
- Increase the effectiveness of communication and decision-making processes related to information security.
- Enhance security policies and processes, as well as establish cost-effective strategies for executing these policies and procedures.
- Put in place security mechanisms to reduce the most serious dangers.
- Heightened staff understanding of security measures and threats via the use of best practices throughout the risk analysis process; and
- Recognize the financial consequences of possible security concerns.

When done correctly, risk analysis is a critical tool for reducing risk-related expenses and assisting an organization's decision-making process. The steps involved in the risk analysis procedure

Generally, the risk analysis method is as follows:

Conduct a risk assessment survey: The first phase in the risk assessment process is to get feedback from management and department heads. The risk assessment survey is intended to begin the process of identifying particular hazards or threats within each department.

Determine the dangers: Risk assessment is used to examine an information technology system or other part of a company and then ask: What are the dangers to the software, hardware, data, and IT employees? What undesirable occurrences, such as human error, fire, floods, or earthquakes, are possible? What is the risk that the system's integrity will be jeopardized or that it will become unavailable?

Analyze the risks: Once the risks have been identified, the risk analysis process should evaluate the chance of each risk occurring, as well as the associated repercussions and their potential impact on the project's goals.

Develop a risk management strategy: Based on a study of which assets are valued and which risks are likely to have a negative impact on those assets, the risk analysis should provide control suggestions for mitigating, transferring, accepting, or avoiding the risk.

Implement the risk management plan: The ultimate purpose of risk assessment is to put measures in place to eliminate or mitigate hazards. Begin by resolving or at the very least mitigating the highest-priority risk.

Monitor the risks: Any risk analysis approach should include a continual process of detecting, addressing, and managing hazards.

The study's scope and structure will vary according on the kind of risk analysis being conducted.

Qualitative vs. quantitative risk analysis

Qualitative and quantitative risk analysis are the two primary methodologies. Qualitative risk analysis is a term that refers to evaluating the possibility of a risk occurring based on subjective characteristics and the potential effect on an organization using specified rating systems. Risks are often classified into three categories based on their impact: low, medium, or high. The chance that a danger may occur can also be represented or classified in the same manner, ranging from 0% to 100%.

Quantitative risk analysis, on the other hand, aims to quantify bad occurrences by assigning a precise financial value to them, which represents the potential cost to an organization if the event happens, as well as the probability of the event occurring in a given year. In other words, if the projected cost of a big cyberattack is $10 million and the probability of the assault happening this year is 10%, the risk is worth $1 million this year.

Qualitative risk analysis generates subjective conclusions since it collects data from participants in the risk analysis process based on their assessments of a risk's likelihood and possible repercussions. Categorizing risks in this manner enables businesses and/or project teams to determine which risks are low priority and which must be actively handled to minimize the enterprise's or project's impact.

In comparison, a quantitative risk analysis assesses the entire risk of a project and is often undertaken after a qualitative risk analysis. Quantitative risk analysis computes the likelihood of each risk and its repercussions statistically.

A quantitative risk analysis's objective is to assign a definite financial value to each identified risk, indicating the potential cost to an organization if the risk materializes. Thus, a firm that has conducted a quantitative risk analysis and subsequently suffers a data breach should readily be able to quantify the financial effect of the event on its operations.

A quantitative risk analysis offers an organization with more objective facts and statistics than a qualitative risk analysis does, enhancing the utility of the process for decision-making.

Steps to complete a project risk assessment

Conducting a risk assessment for your project is critical to ensuring that you and your project team are prepared to deal with the unexpected. As any seasoned project manager will tell you, unexpected issues will arise. When concerns do develop, you must have a risk management approach for your project.

Consider the following scenario: you are the project manager for a building site and get an urgent call from someone on-site; an elephant has escaped from the zoo and is stampeding through town. Fortunately, it was a baby elephant, and no one was harmed. Regrettably, the new-born elephant plowed through your construction site, destroying thousands of dollars' worth of material. All fresh building on a brand-new technological headquarters – everything you've been working on for months – was destroyed. What comes next?

Life is unpredictable (at times of the circus variety!). Risk assessment enables you to plan for unpredictable and unforeseeable occurrences that might have a negative impact on your project. Risk is not only a matter of safety. It entails the use of technology, resources, people, and procedures. Risks in project management are classified into five categories.

- What is a risk event?
- When is the risk most likely to occur?
- Probability: What are the probabilities of this occurrence occurring?
- What is the effect?
- Factors: What can precipitate a risk event?

Consider the following scenario: You're on your way to the most critical business meeting of your life. A million dollars of your own funds are on the line. You're driving down the road and get a flat tire. There is no time to contact for assistance, and a tow truck may be hours away.

You did, however, do your assignment. The spare tire is located in the trunk, along with the equipment necessary to replace it, ensuring that you're back on the road quickly. Additionally, you left the home early to allow for the unforeseen. Your spare tire, tool pack, and time buffer all serve as risk mitigation measures.

Prudent preparation averts legal complications and injuries. And when conditions change or unforeseen situations happen, you can adapt with grace, since you prepared for them.

While planning will never be flawless, by following these steps to create a risk assessment, you may significantly enhance your risk management.

Step 1: Identify potential risks

Conduct a risk and opportunity analysis. Prior to beginning a project, spend some time to consider all of the possible outcomes: the good, the terrible, and the ugly. Conduct a thorough review of both best and worst case scenarios, leaving no stone left. While risk identification is a constant process, hazards should be addressed as quickly as feasible. Participate in the planning process with your customer. Diverse perspectives and expertise levels will aid in identifying as many hazards as feasible up front.

Step 2: Determine the probability

Examining the probability that a certain risk will occur is a critical stage in risk assessment for a project. While severe weather is more likely to cause a delay in breaking ground, you may want to account in a runaway elephant, for example, if you're developing adjacent to a zoo. Classify each scenario as having a high, a medium, or a low chance. This will guarantee that your efforts are directed toward reducing the risks that are most likely to affect your project.

Step 3: Assess the implications

Each risk has an effect; however some have a greater effect than others. While a key member of your team contracting the flu may not significantly impact your project's deadline, if your whole team becomes ill, this may be a different story. Consider what would happen if each of the risks you've listed materialized. Would this have an effect on the ultimate delivery date? What effect would it have on the budget? Determine the risks that will have a significant impact

on the result of your project. Classify those hazards as having a significant effect. Identify the remaining hazards as having a moderate to low effect.

Step 4: Address the risk

This step is referred to as risk response planning. Create a strategy for reducing the biggest risks to manageable levels. Risks may be mitigated by risk management methods, preventative measures, and contingency plans.

Step 5: Review and monitor the risk

Risk management is an ongoing effort due to the fact that situations change. Risks should be reviewed, monitored, and tracked on a regular basis throughout the duration of the project. Uncertainty is a significant component of risk management. By developing a procedure around that uncertainty, you may reduce the risk associated with your project. It increases your chances of completing your project on time and on budget.

Ergonomic Assessments

Ergonomics (or human factors) is a scientific discipline concerned with the study of interactions between humans and other system elements, as well as a profession concerned with the application of theory, principles, data, and methods to design in order to optimize human well-being and system performance.

The term ergonomics derives from the Greek words "ergon" for labour and "nomos" for rules. It is basically the "work rules" or "work science." A well-designed ergonomic workspace eliminates incompatibilities between the task and the worker and offers the ideal work environment.

Ergonomics integrates a variety of disciplines in order to maximize the interaction of the work environment and the worker.

Ergonomic evaluations are a scientific examination of how workers do their jobs. The evaluations assist in identifying ergonomic hazards such as repeated activities that might create strains, an improperly configured work environment, and poor tool usage, all of which can result in the development of work-related musculoskeletal illnesses (MSDs).

1. Conduct a review of current data and previous ergonomic studies.

The first step in developing or upgrading your ergonomics program is to conduct a history. You must create a baseline awareness of previous work-related events and injuries.

Examine injury and sickness logs, workers' compensation reports, first aid records, accident and near-miss investigation reports, insurance company reports, minutes of safety committee meetings, and any worker complaints of concerns.

This enables you to detect common concerns, injuries, and complaints—as well as to focus your efforts on high-risk departments or job categories. This, in turn, will set a data-driven standard for future success measurement.

2. Develop a standardized technique for ergonomic evaluation

Your business will almost certainly undertake initial and follow-up ergonomic evaluations in order to track success and identify areas for improvement. As a consequence, it's critical to build a consistent assessment technique and set of tools to enable apples-to-apples comparisons and reliable risk factor identification.

Create an ergonomic assessment brief outlining your approach framework and the instruments you'll use to gather subjective and objective data. Then, using the brief as a guide, verify that each evaluation uses the same set of tools and processes for documenting. Among the instruments to consider are the following:

- WISHA Checklist for Caution Zones
- Checklist for WISHA Hazard Zones
- WISHA Lifting Calculator or NIOSH Lifting Equation (both are available as mobile applications!)
- Rapid Assessment of the Upper Limb (RULA)
- Rapid Assessment of the Entire Body (REBA)
- Tables for Snook
- Calculator for Hand-Arm Vibration (HAV)

3. Obtain a realistic depiction of your facilities

To ensure the effectiveness of your ergonomics program, you must have first-hand knowledge of the environment in which workers operate.

Consider doing a Gemba walk around the facility. By travelling on-site to gather subjective observations, you may get a peek of employees in action. Take copious notes and consider collecting images and video to aid in recalling particular features and brainstorming improved suggestions.

If you have worldwide operations, hire a global EHS consultant with ergonomics expertise. A consultant brings a wealth of knowledge and skills to the table and can not only do the assessment but also conduct the analysis, providing you with clear next actions. Many environmental, health, and safety managers lack travel budgets yet have worldwide responsibilities. While hiring a consultant adds an upfront expense, it circumvents this problem and provides you with the facts necessary to make educated judgments.

4. Involve workers and get direct input on their work environments

While you should watch employees in their everyday activities during an on-site visit, you should also take time to speak with them. By including employees in the process, you may get comprehensive, first-hand information into how to enhance their work lives and promote your company's safety culture.

Introduce your purpose and ask them about what they do, how they do it, how long they've been doing it, who taught them, how they work, training requirements, and how they feel about their surroundings. Among the questions you might ask are the following:

- Is your employment characterized by heavy or rigorous lifting?
- Do you encounter pain in the course of your work?
- Are you quickly drained of energy while doing your job?

- What do you believe is the most serious safety hazard associated with your job?
- How would you resolve this situation?
- What would make your workplace more pleasant for you?

Another method of gaining information about employees is to conduct a comfort survey. A comfort survey enables workers to express themselves anonymously or freely about their working circumstances and any concerns they may have.

5. Accumulate objective data

After reviewing factual data on incidents and injuries, as well as seeing and engaging people in their work environments, it's time to move on to the more objective component of the evaluation process.

Utilize the information you've gathered to create a detailed, prioritized list of work responsibilities and departments that need evaluation. Then, using the list in conjunction with the technique and instruments you've selected, begin your objective review.

6. Analyze data and assign a risk priority

After gathering subjective and objective data and insights, it's time to assess your findings in order to discover work dangers and mitigation options.

Begin by reading the data in its entirety, noting any standout findings. Dive deeper into each job type or department area to have a more detailed understanding of the dangers and possibilities. Then, prioritize the task risks and mitigation opportunities that need to be addressed in the short- and long-term. Throughout this procedure, you should ask yourself the following questions:

- What is the risk of harm connected with this job?
- How serious is the injury?
- How likely is it that you will sustain an injury?
- Is it possible to limit or eliminate the risk?

7. Develop a mitigating strategy

After you've completed your analysis, it's time to put what you've learned into practice. Bring together your EHS team, safety committee, and/or operations management to develop a plan for addressing risks and mitigating opportunities based on your list. Several points to examine throughout your debate include the following:

- What is the schedule for implementation and is it realistic? (It is preferable if you are prepared with a proposed timeframe from the outset.)
- How long will it take to solve low-, medium-, and high-risk concerns?
- How will we assess our performance in mitigating risk?
- What kind of training and resources will be required to develop, monitor, and improve our ergonomics program?
- Which more stakeholder groups should we involve?
- How will we explain our strategy and ensure that we remain on track?

While there is no one-size-fits-all approach to workplace safety in lower-risk workplaces, these seven ergonomic evaluation procedures can assist you in developing a risk-reduction strategy for your firm. Discover how Antea Group's Risk Right EHS solution can offer you with customised help ranging from ergonomic examinations to the implementation of an entire ergonomic program.

Domains of Specialization in Ergonomics

The International Ergonomics Association classifies ergonomics into three basic categories: physical, cognitive, and organizational.

- **Physical Ergonomics**

Physical ergonomics is concerned with the relationship between human anatomical, anthropometric, physiological, and biomechanical features and physical activity.

This is the ergonomics area with which we are most concerned in the workplace, and the majority of information on this site is devoted to workplace ergonomics.

- **Workplace Ergonomics**

Fitting work circumstances and job demands to the skills of the working population is a science. Ergonomics is a method or technique for resolving a variety of issues, including work-related musculoskeletal illnesses.

At its heart, ergonomics is about creating a better workplace. When occupations are tailored to fit people's talents, better work is done and the employee has a better experience.

Through this viewpoint, ergonomics adds value in a variety of ways. It benefits both your people and your company.

- The Advantages of Ergonomics
- Cost savings
- Increased productivity
- Enhancement of product quality
- Enhancement of employee engagement
- Improved safety culture

The ergonomics improvement method detects ergonomic risks in a systematic manner and implements technical and administrative controls to quantifiably minimize risk factors.

- **Ergonomics Process**

Assessing risk is a critical component of the ergonomics process. Your ergonomic improvement initiatives will never succeed unless you are able to adequately examine occupations in your workplace for risk factors for musculoskeletal disorders (MSDs).

Improve Your Workplace: The ergonomics process's primary objective is to create improvements to your workplace that minimize risk. Making improvements on a large scale needs considerable preparation, which includes choosing occupations to improve, developing successful improvement ideas, and justifying the improvement projects' costs.

Measure Progress: Measuring progress is critical to the success of any continuous improvement effort. Ergonomic programs that function well are regularly monitored using both leading and trailing indications.

Scale Solutions: By building a standardized set of tools for training your staff, risk assessment, planning changes, tracking progress, and designing new work procedures, you may scale ergonomics best practices across your firm.

- **Cognitive Ergonomics**

Cognitive ergonomics is concerned with the effects of mental processes such as perception, memory, reasoning, and motor response on interactions between people and other system parts.

Individual Ergonomic Assessments

An ergonomic assessment is a process that evaluates an employee's workstation to verify that they have the ideal working postures and ergonomic work habits, as well as the proper workstation set-up. Bodycare's Ergonomic Assessments are conducted by fully licensed Occupational Physiotherapists who are adept at monitoring an individual's work environment and work behaviors. A written report summarizing all findings and suggestions may be presented to the employer.

Bodycare's Occupational Health Professionals guide your staff via interactive courses that provide practical ergonomic instruction and guidance in a "real world" scenario. Each session is meant to be given in 30-minute blocks at an employee's desk. Small groups (up to six persons) study the fundamentals of workstation setup in order to provide an efficient and successful work environment. Following the practical demonstration, workers may immediately use their newly acquired knowledge to their own workplace, with the Occupational Health Professional on hand to address any unique ergonomic concerns.

Request for Information

Requests for information arise in several spheres of our society, and generally pertain to the gathering of data by people from bigger organizations for a variety of purposes. The most often used definition of request for information is in the context of governmental requests for information, in which a person, frequently a member of the media, approaches a government entity and submits a request for information according to the freedom of information legislation.

A request for information has a similar, but somewhat different, meaning in project management. In terms of project management, a request for information refers to a specific type of procurement document in which the buyer or purchaser submits a formal request to a potential seller or offerer for a series of specific pieces of information pertaining to a list of services or products that this particular seller may have to offer.

Information requests may or may not be made in connection with a request for an estimate or a request for quote.

A request for information is more commonly referred to by the acronym RFI. It is a document that a business uses to request information from suppliers about a product or service. This way,

the organization can get a sense of the options available from each vendor, compare different providers, and gather market information in a more structured manner.

RFIs are particularly advantageous for businesses that wish to or are required to research a large number of potential partners.

There is no one-size-fits-all approach to writing an RFI. Each business determines the specific data it wishes to collect from various suppliers. Additionally, it selects the number of details to request.

Nonetheless, this does not mean that each RFI is unique. Several distinct elements are typically included in a request for information form:

- The fundamentals of your business
- A request for basic information about the supplier's organization from the supplier (such as business activity and contact details).
- Agreement on confidentiality to prevent providers from disclosing information to third parties.

Apart from the information listed above, a business can request a wide variety of different things. The following is a non-exhaustive list of frequently used elements:

- The applicant's business is presented.
- Justification for the RFI.
- Inquiries on the vendor's expertise with comparable projects.
- Inquiries on the supplier's action strategy, financial status, and technical capabilities.
- References from clients.
- Matrix of selection criteria by which the asking firm will choose the provider.

Request for Proposal (RFP)

A request for proposal (RFP) is a business document that announces, describes, and solicits bids for the completion of a project from competent contractors. The majority of corporations prefer to initiate projects using RFPs, and many governments always do.

When an RFP is used, the organization soliciting bids is responsible for reviewing the offers received, the financial condition of the bidders, and each bidder's capacity to complete the project.

A request for proposal (RFP) is a public notification made by an organization announcing that it is seeking bids from contractors to accomplish a project.

The RFP describes the project for both the corporation issuing it and the firms responding to it.

The RFP details the project, its objectives, and the sponsoring organization, as well as the bidding procedure and contract conditions.

RFPs are utilized by the majority of government bodies as well as many private businesses and organizations.

The alternative is a less formal approach that may fail to find the most qualified vendor and the most effective strategy for completing a project.

RFPs are used for large, complicated projects that often include a large number of subcontractors. They specify the entity that is issuing the RFP, the scope of the project, and the evaluation criteria for submissions. Additionally, they include the bidding procedure and contract details.

The requests contain a statement of work outlining the tasks that the successful bidder will complete and the deadline for completion.

Additionally, RFPs include assistance to bidders on how to create proposals, including detailed instructions on how bids should be prepared and presented. They often provide guidelines on the information that the bidder must include and the format that should be used.

The majority of RFPs are issued by government agencies and other public sector entities. They are often necessary to promote competition between private businesses and to eliminate bias from the process. The agencies want to guarantee that they get the most affordable and competitive proposal possible.

However, any corporate or governmental body may issue an RFP in order to solicit different offers and viewpoints on the project.

For instance, a firm that wishes to transition from a paper-based to a computer-based reporting system may issue a request for proposal for hardware, software, and a user training program to develop and integrate the new system. A competitive bidding procedure may provide them with a better understanding of the available choices.

Government agencies or other organizations may be compelled to solicit bids in order to ensure fair and open competition and to reduce the cost of a solution. Accepting the most responsive proposal to requirements does not necessarily entail accepting the lowest-priced offer.

A request for proposal written with care may determine the success or failure of the eventual solution. If the criteria are too broad, the bidder may be unable to create and deliver an appropriate solution. If the specifications are too comprehensive and restricted, bidders' creativity may be constrained.

The request for proposal (RFP) procedure starts with the creation of a request for proposal. Bidders analyze the solicitation and make changes. Following feedback implementation, the final request for proposal is sent. Following that, bidders submit their bids.

The client narrows the field of bids to a chosen few and engages into talks with the selected bidders about price and technical issues. Before awarding a contract, the client may request that the remaining bidders submit their best and last offer. The contract is then awarded to the business that offers the greatest solution to the problem.

A request for proposals is, in part, an advertising. It indicates that a project is underway and invites suitable persons to apply.

In government, the RFP has been embraced as a means of ensuring that favoritism is not a factor in contract award. Additionally, it exposes the process to competition, which should result in cheaper project costs.

In lieu of an RFP, a less formal approach is used in which a project manager does research and identifies suitable providers for a project. The number of possible replies may be restricted depending on the extent of the search. It is possible that new suppliers and creative solutions will be less likely to be discovered.

- **Example of a Request for Proposal (RFP)**

For instance, suppose the Federal Railroad Administration releases a call for bids for the financing, design, construction, operation, and maintenance of a high-speed rail system.

Interested parties submit ideas that adhere to the document's specifications. The Department of Transportation sets commissions to analyze and develop ideas that are submitted by the deadline.

The DOT selects the proposal that best meets its objectives and hires the business to do the job.

Invitation to Bid

An invitation to bid, sometimes known as an invitation for bid or sealed bid, is a request for contractors to submit proposals for a certain product or service. Typically, it is for needs exceeding $100,000. While an ITB is comparable to an RFP (request for proposal), it is more focused with cost than with the project's basic concepts. As with all other forms of bids, the contractor that submits the lowest offer is normally granted the contract. However, keep in mind that this is not always the case. Other considerations come into play, such as the quality of items or the skills required to complete a job.

Therefore, how can a vendor ascertain if an offer is an RFP, RFQ, RFI, or ITB? Almost often, the agency that is soliciting bids will state this on their website or online portal. If it is not included, it will be in the bid materials, often in the title or first few paragraphs. Bids come in a variety of formats and understanding the distinctions between them can assist you in determining if the project is a suitable match for you and, ultimately, whether it is worthwhile to pursue.

An Invitation to Bid (ITB) or Invitation for Bid (IFB) is a request for proposals from contractors for a particular product or service that an organization desires or requires. While an ITB is similar to a Request for Proposal (RFP), it is often more price-sensitive and entails a more streamlined bidding procedure.

It's easy to mistake an ITB with an RFP if you're unfamiliar with their respective purposes and peculiarities. Let's begin by examining the areas in which they are unlike. When collecting bids from contractors whose goods and services cannot be assessed only on the basis of cost, an RFP is employed. For instance, a beverage business may release an RFP to select an event planning and production firm to organize a corporate retreat.

On the other hand, firms may opt to issue an ITB if there are no significant differences between the goods or services they provide. In this case, the primary criterion for assessment is price. Rather of examining your approach to the project, concentrate on the cost components throughout your proposal. In this scenario, a beverage firm may issue an ITB to get 50,000 red Solo cups.

It's all about the project, which has already been picked for you in this instance! When businesses have a certain project in mind, they will issue an ITB. They already know precisely what product or service they want, the quantity required, and the time and location for delivery. Frequently, an ITB request would outline the proposed project and include submission conditions such as deadlines, project scope and duration, minimum qualifications, mandated service standards, and needed warranties. Additionally, it will describe the general selection process and the criteria for picking a successful contractor.

With this information in mind, it is critical for the bidder to have a firm grasp of the offeror's procurement procedure. Always have your contact information for the bid ready in case you have any questions. Because the bidder is not submitting their own solution, as they would in an RFP, but rather is executing the offeror's solution through the ITB, it is critical that the bidding organization understands precisely what is expected of them. Make it very apparent why your pricing makes you the best candidate for the job.

When it comes to invitations to bid, cost, rather than the bidder's strategy for completing the project, is critical. Generally, the bid is granted to the contractor who delivers the lowest total cost proposal for the project while still meeting all specifications. As such, you'll want to devote the majority of your effort on accurately calculating the cost of delivering on the contract's objectives. Consider all expenditures that will need to be included and how they will affect the final project costing.

Generally, an ITB results in one of the following fixed-price contracts:

- A contract with a set price
- A contract with a fixed price and economic price adjustment
- A contract having a set price that is subject to price redetermination in the future.

While cheap rates will help you get bids, you'll want to be candid with the offeror about your charges. This is because ITBs are evaluated in a much more basic manner. While there is undeniable pressure on contractors to bid as cheap as possible, be cautious not to give price that does not cover your operational expenses, since this will make it impossible to adhere to the contract's criteria.

Naturally, some businesses make more use of ITBs than others. As a result, depending on the industry in which you work, you may encounter them more or less often. For example, government entities often employ ITBs to meet mandated transparency criteria while also assisting in the prevention of corruption and partiality.

Academic institutions, like the public sector, often adopt ITBs for the same transparency reasons. When a school or institution want to give any kind of supply to students, it may opt to issue an ITB (say, a 100-pack of disposable masks per university student, for example). The institution is already aware of its requirements, needs, and schedule. Price therefore takes precedence over all other considerations in the decision-making process.

However, just because ITBs are more focused on pricing than their RFP counterparts does not imply that many of the same requirements apply. When responding to ITBs, always read the criteria thoroughly, react systematically, and submit with purpose. Maintain the same degree of attention for ITBs as you do for RFPs. Begin early and make certain that all deliverables are completed prior to the submission date.

If your organization delivers an item or service that can be standardized and applied to an ITB format, including these prospects into your revenue development plan may be quite profitable. By following our guidelines above, businesses in construction, manufacturing, and a variety of other industries will be well-positioned to develop a solid ITB plan.

Have you recently joined the party? If such is the case, we are here to assist you! The Bid Lab assists businesses like yours in honing their ITBs and gaining confidence in their work. Whether you're a seasoned professional or are entirely unfamiliar with the procedure, contact us to schedule a free 15-minute consultation for your firm. We'll assess your pain spots and provide practical, proven solutions that can help you succeed in the bidding process. Dispute our assertions? Read our Case Studies to see how we assisted firms just like yours in achieving success!

Proposal Evaluation Techniques

Proposal evaluation is the process of evaluating the proposal and the offeror's capacity to effectively complete the potential contract. The agency must examine competing bids and then rank them according to the variables and subfactors listed in the request. Evaluations may use any rating technique or combination of techniques, including colour or adjectival ratings, numerical weights, and ordinal ranks. The contract file must include a summary of the proposal's relative strengths, flaws, major shortcomings, and risks.

Throughout the project's lifecycle, sellers often make bids to the buyer in the aim of being awarded the project. In most circumstances, the buyer gets a large number of offers from potential sellers, making it rather difficult to choose the proper vendors.

The term "proposal assessment procedures" refers to the process of examining supplier bids in order to support the buyer's and project team's contract award choices. Proposal assessment methods are one of the instruments used in Conduct Procurements, which is the process of eliciting replies from the seller, as well as selecting and awarding the contract.

Simple projects may not always need the use of such elaborate project management approaches. The buyer will analyze the bids and award the contract to the most qualified vendor.

When it comes to complicated procurements, the proposal will be chosen based on the seller's replies to a weighted set of criteria established by the buyer. Following that, a formal evaluation review procedure will be set by the buyer's procurement policy. Additionally, there will be an assessment committee that will present a recommendation to management for approval prior to any awards taking place.

Cost or price evaluation

Typically, competition determines the appropriateness of prices. Thus, whether contracting on a firm-fixed-price or fixed-price with economic price adjustment basis, a comparison of the proposed prices often satisfies the criteria for conducting a price analysis, and no cost analysis is required. In some circumstances, a cost analysis may be necessary to determine the appropriateness of the price charged by the otherwise successful offeror. When contracting on a cost-reimbursement basis, assessments should include a cost realism analysis to ascertain what the Government should reasonably anticipate paying for the proposed effort, the offeror's

comprehension of the job, and the offeror's capacity to complete the contract. Cost realism assessments may also be used to fixed-price incentive contracts and, in extreme circumstances, to other competitive fixed-price contracts. Cost or price evaluations should be documented by the contracting officer.

Past performance evaluation.

Past performance data is one indication of an offeror's ability to successfully complete the contract. The information's currency and relevancy, its source, its context, and overall trends in the contractor's performance should all be examined. This comparative evaluation of historical performance data is distinct from the requisite determination of culpability.

The solicitation shall describe the methodology for evaluating past performance, including evaluation of offerors with no relevant performance history, and shall provide an opportunity for offerors to identify prior or current contracts (including Federal, State, and local government and private) for similar efforts to those required by the Government. Additionally, the solicitation should permit offerors to give information on issues that have arisen on specific contracts and the offeror's remedial efforts.

When analyzing the offeror's prior performance, the Government must take into account this information, as well as any additional information collected from other sources. The source selection authority should examine the applicability of comparable historical performance data.

When pertinent to the present purchase, the appraisal should take into consideration historical performance data for antecedent organizations, important employees with appropriate expertise, or subcontractors who will fulfill significant or crucial components of the demand.

When an offeror lacks a record of accomplishment of relevant prior performance or when information on past performance is unavailable, the offeror's past performance may not be appraised favourably or negatively. The assessment should take into account the offerors' prior performance in meeting the aims of the small, disadvantaged enterprise subcontracting strategy.

Best Project Management Features

The term "project selection" refers to the process of developing and selecting a team's next endeavour. Because projects generally compete for resources, you must prioritize them based on the needs and objectives of each possible project.

At any one moment, the majority of organizations have numerous prospective initiatives in the works. Successful businesses have a consistent strategy for comparing these initiatives to discover the next best match. Once an organization has chosen a project, it must outline it and create a project plan.

An experienced project manager often has unique information and abilities that a higher-level executive may lack, such as a better understanding of the risks and resource needs associated with a proposal. A project manager should also have a firm grasp of the demands and capabilities of their team.

Additionally, project managers may serve as sounding boards for executives, influencing the project's scope and execution. It is critical to provide objective feedback during project selection to ensure that the whole team has the greatest potential chance of success.

A project manager's most critical duty is to serve as a bridge between the team and the executives. Determine the most influential decision makers and their organizational objectives. When providing feedback, emphasize your team's strengths appropriately. Simultaneously, be candid about any gaps in your team's capabilities or resources.

The project manager's responsibility is to provide unique insight into an organization's overall capabilities. If you feel your organization lacks the necessary resources or time for a certain project, bring it up as early in the planning and selection process as feasible.

After the business has chosen a project, the project manager should start the planning phase. Assemble your project plan and develop a communication strategy to keep yourself and your team on track.

Management often prioritizes variables such as total budget and payback duration, resource availability, and profit and growth potential. On the other hand, a project manager may be familiar with aspects such as deadline management, risk management, and the success of previous projects.

It is critical to understand your leaders' fears in order to allay them. Simultaneously, get familiar with your team's strengths and limitations so that you can advocate for them effectively. The project manager should address issues raised by all stakeholders and discover and assist strategies for resolving them and ensuring the project's success.

You may pick projects in a number of ways, the most of which fall into one of two categories. While constrained optimization techniques emphasize numerical and mathematical advantages, benefit assessment techniques emphasize more approachable notions such as opportunity cost and payback periods.

Constrained optimization techniques often make use of sophisticated mathematical principles to account for specific factors throughout the project selection process. They often incorporate numbers and hard figures, and they assist solve real-world issues by converting them to equations.

The following are a few examples of frequently used restricted optimization techniques:

- Integer Programming: This technique places a higher premium on full integers than on partial solutions. For instance, a corporation would not wish to construct a half automobile but rather a whole vehicle, and hence the decision is phrased in terms of complete vehicles.
- Linear Programming: This technique focuses on increasing a particular variable's value by manipulation of other linear variables. For instance, you may minimize the overall cost of a project by shortening its duration. If you can sell automobiles at the rate at which they are manufactured, you can sell more cars by manufacturing them quicker.
- Dynamic Programming: This technique divides a huge issue into digestible bits. Rather of "creating a vehicle," a corporation may choose to concentrate on building each component separately and then assembling them together.

- Nonlinear Programming: More difficult than linear programming, this technique entails maximizing a particular variable in a setting where other variables are not linearly related to it. When expanding assembly line production, you may need to factor in the higher expenses of expedited bulk shipment and customs from numerous nations.
- Multiple Objective Programming: This technique is a hybrid of the previous three. In this section, you will design a set of functions that will assist you in quantitatively optimizing your selections. By defining the time and cost of each stage in the process of building a vehicle using equations, you may modify variables at any point and get a model of projected consequences.

Project Selection Criteria

The phrase "project selection criteria" refers to the variables that a business considers while deciding on its next project. Budgetary constraints, timing constraints, and the availability of certain teams and individuals may all factor into this choice.

Each project's success is unique," adds Marissa Taffer, PMP, Founder and President of M. Taffer Consulting. "While delivering on schedule, within scope, and within or below budget is a victory in certain cases, there is often more to consider. Was the project successful in achieving its objectives? Was the team cohesive? What lessons did we take away from this experience?

The factors for project selection are specific to the company and the project. Generally, an organization will examine factors such as the team's technical expertise, the amount of time and money available to accomplish the project, and the business's overall objectives.

As your business grows in success, it adapts. At first, you take on any project in order to grow your firm, establish relevance, and obtain visibility. Once you've established a name for yourself, you can be a bit choosier. We now chose initiatives based on their alignment with our company, rather than vice versa, and our selection criteria have been altered appropriately.

The project selection process encompasses all of the actions that an organization engages in while considering the costs and advantages of a possible venture in order to pick a new one. Generally, high-level management selects and finally outsourced a new project to a team.

While the exact phases vary each business, the process typically include discovering prospective projects, comparing them to one another, assessing your results, and choosing a project.

Models for project selection depict the structure of a project in relation to the rationale for its proposal. These non-numerical models may be used to identify initiatives based on their requirement for market competitiveness or their position as an executive's pet project.

The following are some popular project selection models:

- Comparative Advantage: This methodology examines numerous possible projects and identifies the best.
- Competitive Necessity: This initiative is critical to the business's competitive advantage.
- Operating Necessity: Successful completion of this project is crucial to the business's continuing functioning.

- Product Line Extension: This project adds to or enhances the business's current product line.
- Sacred Cow: This endeavour was the idea of an organization's senior or executive member.

Contract Negotiations

Negotiation is a procedure that involves two or more individuals who have opposing viewpoints. These individuals make an effort at agreement by altering their initial stances. Typically, a satisfactory solution needs negotiating. However, the agreement should not be seen as a lose-lose scenario. The solution should be mutually advantageous, or in certain cases, mutually unprofitable.

While procurement managers typically lead negotiations, both buyer and seller project managers are involved in contract negotiations, particularly when cost-reimbursable and time and material contracts are involved, as there will almost certainly be negotiations to finalize the contract price, and project managers are responsible for project management and resolution of technical issues on the project. Without the participation of the project manager throughout the negotiating process, it is very uncommon for a contract to be signed that the project manager later realizes cannot be executed.

- **Negotiation Goals:**

The purpose of negotiations is to:

- Negotiate a reasonable and fair pricing
- Establish a positive connection with the vendor.

The second purpose may surprise many who believe that negotiations are win-lose situations. In this case, the seller is less concerned with completing the work than with recouping the money lost during the negotiations, and the buyer's project manager will spend time ensuring that the seller does not add additional costs, propose unnecessary work, or initiate other activities to recoup the money lost during the negotiations. A win-win scenario is one in which the customer receives the finished job and the seller earns a respectable profit. Numerous projects fail as a result of how they were negotiated, not because of the project's inherent difficulties.

- **Tactics for Negotiation:**

Successful negotiators have a number of personality characteristics. Empathy, respect, fairness, patience, adaptability, and a sense of humor are just a few examples. Each of these characteristics will enable you to have a good negotiation experience, even more so if the situation is difficult or lengthy.

When negotiating with a vendor/seller, the following negotiation methods may be used depending on the situation:

Fait Accompli - Non-negotiable contract conditions. (In actuality, everything in the contract is negotiable, notwithstanding your adversary's denials.)

A deadline is a predetermined date by which the other party must decide or act. Make it clear that this is the deadline for them to complete the task at hand. As the deadline approaches, raise

the emotional strain by discussing the consequences of missing the deadline. This may take the form of menacing behaviors or ominous undertones.

Good guy Vs terrible guy- One individual is forceful and overbearing, demanding ridiculous things and demanding obedience. The other individual then behaves with kindness and friendliness, politely requesting obedience.

The negotiator's missing man - The negotiator's missing man is the individual who can truly make the choice.

The negotiator might then pursue a cheaper price or more favorable conditions with which they believe they can agree.

Limited authority - Refusing to concede on things because you lack the authority to do the desired action.

Fair and reasonable - You might engage the other person by inquiring as to what is reasonable. Additionally, you may offer something to the table that is, by definition, fair. Additionally, you might reject an adversary's standards on the grounds that they are unjust.

Unreasonable/Extreme Demands - Indicates that the other party is making unreasonable demands during the discussion.

Delay – Extending the discussion, particularly at vital points. This strategy may be very successful when a resolution to the discussion is needed immediately.

Withdrawal - This may be emotional or physical and might indicate waning interest.

Assault - A direct attack on your integrity, trustworthiness, competency, or any other kind of bullying aimed to coerce cooperation from you. An agreement must be established, agreed upon, and understood at the conclusion of the negotiation.

- **Strategies for Negotiation: Underlined text**

Jeffrey Pinto, author of the Project Management Handbook, has identified five negotiating tactics.

1. Making concessions - This entails altering your plan in such a way that it benefits the opposing party more than you. You may agree to make the suggested adjustments without incurring extra costs or delaying the completion of the project.

2. Contending - Involves attempting to convince the other party to make a proposition that is more advantageous to you than to them. Threats and disputes are examples of tactics. You are adamantly opposed to making any extra compromises.

3. Compromising - A middle ground between concessions and contention. A compromise is sought that entails some measure of sacrifice on both parties. Two project managers may agree to split the cost of the revisions or to extend the deadline for completion.

4. Problem resolution — Efforts to reach mutually beneficial agreements. Project managers are free to speak candidly about their aims and priorities. A solution may be discovered by sharing information about finances and deadlines.

5. Inaction or disengagement - Involves evading or delaying real talks. Withdrawal is a tactic that entails ending discussions without reaching an agreement.

- **Negotiable Items: Underlined text**

The primary issues to discuss while negotiating a contract vary significantly based on the object being bought. To get a signed contract, the following factors are often negotiated: scope, timetable, and pricing. Additionally, roles, authority, relevant legislation, project management techniques to be implemented, and payment schedules might be agreed. Many individuals are unaware that price is not always the key segment criterion or the primary point of contention during negotiations. Often, it is irrelevant. Schedule may be more essential than cost, and a buyer may make a financial compromise to get quickness.

- **Finally, italicized text**

Among the specific tips for negotiating in a project context are the following:

- Ensure that the project is chartered and supported correctly.
- Establish defined corporate objectives with the sponsor's and leadership team's buy-in and support.
- Align the project's outcomes with the company's objectives
- Connect project objectives and outcomes to underlying business objectives
- Clearly outline and clearly explain the activities necessary to accomplish the project's objectives
- Defining and graphically depicting the project's resource needs
- Establish trust and credibility via meticulous project planning and scheduling, as well as open and honest communication.
- Conduct risk assessments for resources that are absent
- Be aware of the cost of delay
- Calculate the cost of not having the necessary resources.
- Be aware of and respectful of cultural differences

Service Level Agreement

A service level agreement (SLA) for project management is an agreement with suppliers or contractors whose work is critical to the project's delivery or completion on time. For instance, if you're planning an event and need to rent staging, lighting, and audio equipment to accommodate the attendees, you'll need a project SLA that specifies the level of service you expect from the vendor, as well as the service level the vendor must maintain to ensure the event runs smoothly.

A project management services agreement is often included in a contract with a vendor or service provider and details the customer's recourse in the event that the specified quality of service is not met. A service level agreement, on the other hand, might be beneficial to a company in a more informal role. For instance, the marketing department may agree on a SLA with the other departments with whom it works closely to define the service they plan to deliver, the process for reporting difficulties, and the deadline for servicing.

- **Service level agreement basics**

Our project service agreement should be divided into two distinct components: services and management. The service section should include a list of services provided and excluded, the roles and responsibilities of each party, the anticipated response and resolution time, as well as escalation procedures and service credits in the event that the vendor or provider does not meet the agreed level of service. The management component of the SLA for project management should contain techniques and criteria for measuring the service, as well as protocols for reporting and resolving conflicts.

A project service level agreement is an effective tool that project management teams may and should use to guarantee that related suppliers or contractors do not cause delays in the project's timetable and that the project management process is simplified from the outset.

In project management, project service agreements provide numerous critical advantages to both managers and suppliers or contractors. They reduce inter-party uncertainty, specify the acceptable and desired level of service quality, and pre-negotiate fines.

- **Issue resolution in service level agreements**

While fines are a common component of service level agreements for project management, it's critical to incorporate mechanisms for rapidly and effectively resolving service concerns. After all, fines may serve as an incentive for suppliers to meet deadlines. Resolving service difficulties will almost certainly assist you in meeting your deadline and achieving your target end more rapidly.

Because a project SLA also specifies how difficulties with services or the management process should be reported, it may assist project managers in gaining an understanding of a specific vendor's achievements or failures. This may aid in future planning, since the reporting results specified in a project management service level agreement enable management to determine which suppliers are best suited for a certain project.

SLAs assist service providers in managing customer expectations and defining the severity levels and conditions in which they are not responsible for outages or performance problems. Customers may also benefit from SLAs since they define the service's performance characteristics, which can be compared to those of competing providers, and outline the procedures for resolving service concerns.

Typically, the SLA is one of two fundamental agreements between service providers and their clients. Numerous service providers create a master service agreement to define the broad terms and circumstances under which they will engage with consumers.

Project management of information systems (IS) is a notoriously tough endeavour. A project manager is a critical component of a successful information systems development project. The purpose of this study is to determine how a project manager's past experience and risk tolerance affect their decision-making. An experiment demonstrated that both experience and risk proclivity had a considerable impact on decision-making.

Perhaps the most significant of all project management abilities is the capacity to make critical business choices. To analyze the various possibilities and determine the optimal course of action, strong decision-making abilities are required. Indecisiveness or bad judgment may put a project and your career on hold.

H. RISK MANAGEMENT IN IT PROJECTS

Risk Management

Risk management is the process of detecting, analyzing, and avoiding or managing risks associated with a project that have the potential to adversely affect the intended results. Typically, project managers are accountable for monitoring the risk management process throughout the length of a project.

To manage risk successfully, project managers must have a firm grasp on their goals in order to detect any potential impediments to the team's capacity to generate outcomes.

Risk management is essentially about examining your project goals and determining the dangers to those objectives, as well as what you can do to mitigate those threats from the start,"

Risk encompasses a vast range of events and situations that are often misrepresented. While project managers and others charged with the oversight of a project may be tempted to interpret risks only as threats, this is not necessarily the case.

To dispel this widespread mistake, Emerson defines project risk as "...a future event that may or may not occur and, if it does, will have an effect on the project's goals." It might be a favorable development, an opportunity or a bad development, a danger."

- **Types of Project Risk**

Apart from the fundamental definition of "risk," project managers should be familiar with the many sorts of hazards they may experience. The criteria that should be examined vary according on the kind of project.

Numerous forms of dangers arise often, independent of the project's characteristics. Among the most prevalent categories of risk are the following:

Cost: The possibility of occurrences affecting the budget, particularly those that result in the project being finished late. Cost estimating errors can create risk in addition to external variables.

Schedule: The possibility of unanticipated schedule issues, such as incidents that postpone the project. Scope creep is a frequent source of scheduling conflicts and project delays.

Performance: The risk of events that cause the project to bring results that are incongruent with the project requirements.

Numerous different forms of dangers may develop depending on the specifics of the project. For instance, project managers may also need to account for risks associated with implementation, training, and testing.

Once project managers have identified the risk categories that should worry them, they may begin to comprehend how these risks could affect the project's results and what they can do to mitigate their consequences. Additionally, they will need to examine the breadth and depth of each risk class in relation to the total project.

- **Steps in the Risk Management Process**

To guard against unexpected risk, project managers often use a continuous risk management approach that assists them in identifying, comprehending, and responding to threats and opportunities. Prior to commencing this process, however, it is critical to have a thorough understanding of your organization's procedures and the manner in which you will execute risk management for that project. This strategy will then guide the next steps:

- **Determine the dangers that may affect your project.**

Assign responsibility for each identified risk to a team member who will be responsible for monitoring the danger or opportunity. While some project managers prefer to transfer ownership after risk analysis and prioritization, doing so early on might be useful. "Many times, I immediately designate an owner to a risk because I want that individual to lead the risk analysis," Emerson observes.

Analyze each risk to have a thorough understanding of the underlying variables and possible consequences. Consider the breadth and depth of each danger at this stage to determine the risk's seriousness in the context of the whole project.

- **Prioritize project risks based on their immediacy and the potential severity of their effect.**

Respond to recognized risks in line with your risk management strategy, either by preventing the occurrence of the risk event or by mitigating its effect if it does occur. This stage should contain both response development and execution.

- **Maintain an eye on your risk management plan and make any adjustments.**

While the risk management process is structured, it should ideally be a continual endeavour. After all, risk is inherently unpredictable, and project managers must possess the agility and discipline necessary to respond to changing conditions throughout the duration of a project.

Tips to Reduce and Manage Risk

While it is hard to totally remove risk, project managers may take efforts to manage projects efficiently while minimizing risk. To begin started, here are four pointers:

- **Develop a risk management strategy.**

Anyone with project management expertise understands how critical a robust project plan is to the project's success. Numerous auxiliary plans, including the risk management plan, are often included in this plan.

Emerson recommends that your risk management strategy include your process for detecting and prioritizing risk, your risk tolerance, how your team will react to risk, and how you will communicate risk, among other things. While developing such a strategy requires time and work, investing in the planning phase often pays off by providing a path for your team to follow throughout the project's execution phase.

- **Maintain an up-to-date risk registry.**

Your risk register, which may be included in or distinct from your risk management strategy, is a record of all potential risk events that might affect your project. While having this document

can assist you in staying on top of any concerns, it is critical to maintain it updated in order to always have an accurate picture to refer to.

Utilize your risk register to keep track of risk events that happened, how your team reacted, and which new risks emerged that you were unaware of originally. By keeping this document current and associating it with other planning deliverables, you, your team, and other key stakeholders will always have a clear view of the project's status.

- **Recognize the risk event.**

A frequent risk management error is for individuals to think about risk in terms of prospective outcomes rather than the actual risk occurrence. For instance, individuals may sometimes consider "missing the deadline" as a danger to their endeavour. While missing a deadline is undoubtedly a risk to the project, it is not the risk that matters, but rather the consequence.

Rather than that, evaluate risk in the following manner: As a result of X, Y may occur, resulting in Z effect. This will assist you in determining the source of the risk, the risk event, and the appropriate response.

- **Take a proactive stance rather than a reactive one.**

Occasionally, project managers make the error of adopting a reactive rather than proactive approach to risk management. While the agility to respond to unanticipated events will always be vital, it is also critical to take a step back and assess your project from a proactive perspective.

By devoting effort to the risk management process's early phases and thoroughly understanding each risk, you may position yourself to take preventive measures that lower the likelihood of a risk event happening, rather than attempting to react after it has occurred.

- **Strengthen your project management abilities.**

Above all, managing projects and their associated risks efficiently demands a solid foundation of project management abilities. Along with practicing, keeping current on business trends, and attending conferences and seminars, one of the greatest ways to hone these abilities is to acquire a project management certificate or graduate degree.

Those who find themselves in charge of a project but lack formal training stand to profit significantly from project management education; nevertheless, those already in the profession may benefit from perfecting their trade.

I. INFORMATION SYSTEMS SECURITY

Information security management system

The term "information security management system" refers to a system that manages information security. It is a documented management system comprised of a collection of security measures designed to safeguard the confidentiality, availability, and integrity of assets against threats and vulnerabilities.

By developing, deploying, administering, and maintaining an ISMS, enterprises can guard against the compromising of their private, personal, and sensitive data.

While no profession is recession-proof, the profusion of information technology and information asset protection requirements is offering many possibilities for project managers motivated and capable of undertaking and delivering information security initiatives.

The worlds of information access and information security are closely linked, and as such, data must be easily available and accessible to those who need it while also maintaining its confidentiality and integrity. We have all managed technical change as project managers, but the current pace of technological advancements, combined with an influx of increasingly sophisticated security threats and attacks, as well as the requirement to comply with a plethora of privacy laws and security protection standards, virtually guarantees increased interaction and benefits from partnering with our local information security group.

Who are these security personnel and what do they do? Simply said, information security's responsibility is to balance risk and value in order to empower the company. Security practitioners comprehend and explain threats, as well as deliver solutions in the context of generating corporate value. Solutions that mitigate risk are selected, and may involve a variety of security activities, such as isolating important data networks, installing intrusion prevention devices, recording and monitoring security events, or adhering to security standards.

While no profession is recession-proof, the profusion of information technology and information asset protection requirements is offering many possibilities for project managers motivated and capable of undertaking and delivering information security initiatives.

The worlds of information access and information security are closely linked, and as such, data must be easily available and accessible to those who need it while also maintaining its confidentiality and integrity. We have all managed technical change as project managers, but the current pace of technological advancements, combined with an influx of increasingly sophisticated security threats and attacks, as well as the requirement to comply with a plethora of privacy laws and security protection standards, virtually guarantees increased interaction and benefits from partnering with our local information security group.

Who are these security personnel and what do they do? Simply said, information security's responsibility is to balance risk and value in order to empower the company. Security practitioners comprehend and explain threats, as well as deliver solutions in the context of generating corporate value. Solutions that mitigate risk are selected, and may involve a variety of security activities, such as isolating important data networks, installing intrusion prevention devices, recording and monitoring security events, or adhering to security standards.

Additionally, information security organizations exist to educate and raise awareness about enterprise security policies and procedures, as well as to execute real-time threat monitoring and mitigation.

Four key topics to consider and keep in mind when allocated your next information security project are as follows:

- **Obtain Executive Sponsorship and Formal Financial Support. Executive Leadership Must Support the Scope, Objectives, And Strategic Fit Of The Initiative.**

The involvement and support of the CSO or senior security leadership, as well as the project's public alignment with major corporate priorities, convey to users at large that the project or security endeavour is not just another "nice to have." This is especially critical if your project requires participants to attend security training or perform a security-related job. In many circumstances, having the continued support and endorsement of top leadership will be your saving grace.

Executive leadership is vital for information security initiatives since the company's competitive advantage is primarily dependent on the protection and accessibility of key data. Once leadership recognizes and supports this, these initiatives become investments in developing and enabling trustworthy, controllable, and scalable information protection and access. While you have the Sponsor's attention, enquire about the Sponsor's overall IT security strategy (or strategy). This will provide clarity and emphasis to the role your project plays in the big picture. Additionally, take use of this chance to learn as much as possible about the critical resources given to your project.

- **Become Aware of Your Security Solution (S)**

Conducting research on the security solution that will be implemented will not only give context for a more complete knowledge of the situation at hand but will also indicate to your team and stakeholders that you are dedicated and goal-oriented. This care should be applied to all contractual and internal working arrangements. Without this understanding, you may have trust difficulties with the client and an increased lag in overall resolution since the customer will expect the project manager to address the majority of concerns and inquiries. A more complete knowledge of the functional environment may also give insight into connected operational security efforts. IT security must be operationalized to be successful, and the most effective method to do this is via integrated and well-managed initiatives.

- **Adopt A Consistent Risk Management Approach**

The commonly acknowledged approach to risk in information security is somewhat different from the usual project management technique. While project managers are familiar with individual risk events, their likelihood, and related consequences, security practitioners prefer to think in terms of threats and the prospect of these being exploited to disclose specific vulnerabilities. This strategy often involves assigning a value to corporate assets in order to quantify the danger and susceptibility, if exposed. Given the somewhat different approach to risk management, it will be advantageous to meet as early as possible in the project's lifecycle to build a shared strategy to detecting, documenting, and managing total risk. This will provide the groundwork for the often unsettling risk talks and create the way for essential assignments and follow-ups.

- **Become acquainted with your project's team, vendors, and subcontractors.**

Never overlook the critical nature of joint planning and communication. When a team is cohesive, teamwork and communication may be more productive. Prior to the meeting, attempt a one–on–one with each team member, vendor, or subcontractor to explain their position, specialized areas of expertise, and to express any issues or questions in a non-threatening setting. This will set the way for future knowledge and experience exchange. Encourage frank discussion of individual responsibilities and input items at the launch meeting to better establish each party's interest in and commitment to the project.

Solid executive support, familiarity with the solution(s) under consideration, a shared and agreed-upon risk strategy, and familiarity with team and vendor connections all contribute significantly to the likelihood that your next information security project will be a smashing success.

Cybercrime

Cybercrime, often known as computer crime, is the illicit use of a computer to accomplish illegal goals such as fraud, trafficking in child pornography and intellectual property, stealing identities, and invading privacy. Cybercrime, particularly over the Internet, has increased in prominence as the computer has become indispensable for business, entertainment, and government.

Because computers and the Internet were widely used in the United States early on, the majority of the initial victims and perpetrators of cybercrime were Americans. By the twenty-first century, however, barely a hamlet remained unaffected by some kind of cybercrime.

While new technology generate new criminal possibilities, they do not always result in new sorts of crime. What differentiates cybercrime from other forms of criminal activity? Obviously, one distinction is the use of a digital computer, but technology alone is inadequate to establish any distinction between other spheres of illegal conduct. Criminals do not need a computer to conduct fraud, traffic in child pornography and intellectual property, steal an identity, or infringe on another person's privacy. All of these activities existed prior to the ubiquity of the "cyber" prefix. Cybercrime, particularly as it relates to the Internet, is a continuation of current criminal behavior, as well as some unique illicit behaviors.

The majority of cybercrime is directed against data on people, businesses, or governments. While the assaults do not target a physical body, they do target the personal or corporate virtual body, which is the collection of data qualities that distinguish individuals and organizations on the Internet. In other words, in the digital era, our virtual identities are critical components of daily life: we are a collection of numbers and identifiers stored in many government and corporate-owned computer systems. Cybercrime demonstrates both the significance of networked computers in our lives and the fragility of apparently infallible concepts such as human identification.

A significant characteristic of cybercrime is its nonlocal nature: acts may take place over huge geographical distances. This creates significant difficulties for law enforcement since crimes that were formerly committed on a local or even national level now need worldwide collaboration. For instance, if a person downloads child pornography stored on a computer in a country that does not prohibit it, is that person committing a crime in a country that does prohibit such materials? Where does cybercrime occur? Cyberspace is essentially a more developed form of the space between two persons conducting a telephone call. As a global network, the Internet provides thieves with several hiding spots both in the physical world and inside the network itself. However, much as humans walking on the ground leave traces that a good tracker can follow, cybercriminals leave traces of their identity and position despite their best attempts to conceal their identities and whereabouts. However, before such hints may be followed over national borders, international cybercrime conventions must be adopted.

In 1996, the Council of Europe created a preliminary international convention on computer crime in collaboration with government officials from the United States, Canada, and Japan.

Civil libertarian organizations quickly objected clauses in the pact mandating Internet service providers (ISPs) to retain and pass over information about their users' transactions on demand. Nonetheless, work on the pact continued, and on November 23, 2001, 30 governments signed the Council of Europe Convention on Cybercrime. The convention became law in 2004. Additional standards were established in 2002 and went into force in 2006, encompassing terrorist actions and racist and xenophobic cybercrime. Additionally, several national legislation, such as the 2001 USA PATRIOT Act, have increased law enforcement's authority to monitor and defend computer networks.

- **Types of cybercrime**

Cybercrime encompasses a broad variety of actions. At one end of the spectrum are crimes involving basic invasions of personal or corporate privacy, such as attacks on the integrity of information stored in digital depositories and the use of unlawfully acquired digital information to blackmail a business or individual. At the other end of the range comes identity theft, an increasing crime. At the other end of the scale are transactional crimes such as fraud, child pornography trafficking, digital piracy, money laundering, and counterfeiting. These are individual crimes with specific victims, yet the culprit conceals himself behind the Internet's relative anonymity. Another aspect of this sort of crime is when persons inside organizations or government agencies purposefully change data for profit or political gain.

On the opposite end of the scale are offenses that entail efforts to impair the Internet's real operation. These include spam, hacking, and denial of service assaults on particular websites, as well as acts of cyberterrorism, defined as the use of the Internet to create public disorder or even death. Cyberterrorism is concerned with nonstate actors' use of the Internet to attack a nation's economic and technical infrastructure. Since the September 11, 2001, terrorist attacks, public awareness of the danger of cyberterrorism has increased substantially.

- **Identity theft and invasion of privacy**

Cybercrime impacts both virtual and physical bodies, but the repercussions are very distinct. The most egregious manifestation of this issue is identity theft. Individuals in the United States, for example, do not have an official identity card; instead, they have a Social Security number, which has long acted as a de facto identifying number. Taxes are collected using a citizen's Social Security number, and many private organizations utilize it to monitor their workers, pupils, and patients.

Access to an individual's Social Security number enables the gathering of all documentation pertaining to that individual's citizenship—in other words, to steal his identity. Even stolen credit card information may be used to reassemble a person's identity. When fraudsters steal a business's credit card information, they have two separate consequences. To begin, they steal digital information on people that is helpful in a variety of ways. For instance, they may use the credit card information to build up enormous bills, causing the credit card companies to incur significant losses, or they could sell the information to others who could exploit it similarly. Second, they may utilize specific credit card numbers and names to establish new identities for additional crooks.

For instance, a thief may call the issuing bank of a stolen credit card and request that the account's postal address be changed. Following that, the offender may get a passport or driver's

license with their own photograph but bearing the victim's name. With a driver's license in hand, the criminal may quickly get a new Social Security card; they can then create bank accounts and obtain loans using the victim's credit history and background. The original cardholder may be ignorant of this until the debt accumulates to such an extent that the bank approaches the account holder.

Only at that point does the identity theft become apparent. Although identity theft occurs in a broad variety of nations, academics and law enforcement authorities are constrained by a global dearth of data and statistics on the crime. However, cybercrime is unquestionably a global issue.

In 2015, the United States Bureau of Justice Statistics (BJS) issued a study on identity theft; about 1.1 million Americans had their identities used illegally to create bank, credit card, or utility accounts the previous year. Additional 16.4 million Americans were harmed by account theft, including the use of stolen credit cards and automated teller machine (ATM) cards, according to the study. While the overall number of identity theft victims in the United States increased by around 1 million during 2012, the total loss experienced by individuals decreased by almost $10 billion to $15.4 billion since 2012. The majority of such fall was due to a precipitous decline in the number of those who lost more than $2,000. The majority of identity theft occurred on a modest scale, with losses of less than $300 accounting for 54% of total losses.

- **Internet fraud**

On the Internet, consumer fraud schemes abound. The Nigerian, or "419," fraud is one of the most well-known; the number refers to the portion of Nigerian legislation that the fraud breaches. Although this trick has been utilized with fax and regular mail, the Internet has given it fresh life. The plan begins with a person receiving an e-mail from the sender requesting assistance in moving a big quantity of money out of Nigeria or another foreign nation. Typically, this money comes in the form of a saleable item, such as oil, or a significant sum of cash that needs "washing" to disguise its origins; the possibilities are unlimited, and new details are continuously being devised.

The letter requests that the receiver pay part of the costs associated with transporting the monies out of the nation in exchange for a considerably bigger quantity of money in the near future. If the receiver responds with a check or money order, they are informed that issues have arisen and more funds are necessary. Over time, victims may incur financial losses in the thousands of dollars that are completely irrecoverable.

In 2002, the newly founded United States Internet Crime Complaint Center (IC3) stated that over $54 million had been lost to a variety of fraud schemes, a threefold rise over 2001's projected losses of $17 million. Annual losses increased in successive years, reaching $125 million in 2003, over $200 million in 2006, almost $250 million in 2008, and more than $1 billion in 2015. The primary cause of fraud in the United States is what IC3 refers to as "non-payment/non-delivery," in which products and services are either supplied but not paid for or paid for but not delivered. In contrast to identity theft, which happens without the victim's awareness, these more classic kinds of fraud take place in full view. Because the victim voluntarily supplies private information necessary to commit the crime, they are transactional crimes. Few individuals would trust someone who approached them on the street and offered

quick money; but getting an unsolicited e-mail or browsing a random Web website is enough dissimilar that many people readily open their wallets. Despite widespread consumer education, Internet fraud continues to be a lucrative business for criminals and prosecutors. Europe and the United States are by no means the sole cybercrime hotspots. South Korea is one of the world's most connected nations, and its statistics on cybercrime fraud are expanding at an alarming pace. Japan has also seen a dramatic increase in similar incidents.

- **ATM fraud**

Computers also enable more banal forms of deception. Consider the automated teller machine (ATM), which many people now use to get cash. A user must provide a card and a personal identification number in order to access an account (PIN). Criminals have discovered methods for intercepting both the magnetic strip data and the user's PIN. The information is then utilized to produce fraudulent cards that are used to withdraw monies from the unknowing victim's account. For instance, the New York Times revealed in 2002 that a single organization involved in unlawfully getting ATM information had swiped over 21,000 American bank accounts.

The usage of ATMs in shopping malls and convenience shops has shown to be a particularly efficient method of fraud. These devices are self-contained and are not physically attached to a bank. Criminals may simply put up a machine that seems to be authentic; however, instead of distributing money, the system collects information on customers and notifies them when the machine is out of service after they enter their PINs. Given that ATMs are the main means of cash distribution around the globe, ATM fraud has developed into a global concern.

- **Wire fraud**

Wire fraud is a prime example of cybercrime's worldwide character. Vladimir Levin, a Russian programmer at a computer software business in St. Petersburg, staged one of the biggest and most well-organized wire fraud swindles in history. Levin started moving around $10 million from Citibank, N.A. subsidiaries in Argentina and Indonesia to bank accounts in San Francisco, Tel Aviv, Amsterdam, Germany, and Finland in 1994, with the assistance of hundreds of confederates. Citibank said that all money save $400,000 were finally retrieved when Levin's accomplices sought to withdraw them. Levin was detained in 1995 while passing through Heathrow Airport in London (at the time, Russia had no extradition treaty for cybercrime). Levin was ultimately extradited to the United States in 1998, where he received a three-year prison term and was compelled to repay Citibank $240,015. Levin's exact method of obtaining the account names and passwords remains unknown, but no Citibank employee has ever been prosecuted in connection with the case. Because financial institutions place a premium on security and privacy, determining the scope of wire fraud is challenging. Wire fraud remained a global concern in the early twenty-first century.

Computer Abuse

Computer abuse is the legal term for the use of a computer to do inappropriate or unlawful acts that do not qualify as wire fraud.

Computer abuse occurs when a computer is used to expose personally identifiable information (PII) such as Social Security numbers, when a computer is used to alter the content of another's website, when a computer is intentionally infected with a virus or worm that spreads to other computers, when a computer is used to illegally share copyrighted items, and when a computer

is used to gain unauthorized access to another. Cyberbullying and utilizing a work computer for personal chores on business time are other instances of computer misuse.

Computer abuse occurs when a computer is used to cause damage to another person in some manner. Individuals who engage in computer abuse may be in violation of corporate or institution regulations, as well as federal law. Responding to computer abuse entails identifying the offending computer(s) and then attempting to track down the perpetrator (s).

According to certain definitions of computer abuse, computer crime is a subset of computer abuse. Other definitions believe the two terms to be mutually exclusive, referring to computer misuse as dishonest or unethical and computer crime as criminal. However, these perspectives are immaterial when it comes to the federal legislation that regulates computer abuse: the Computer Fraud and Abuse Act of 1984. (CFAA).

By prohibiting "unauthorized access" to computers and networks, the CFAA criminalizes some sorts of computer misuse. The legislation has been effectively utilized to punish both high-level and low-level hackers in civil and criminal cases. For example, early in the law's history, it was used to prosecute the individual who launched the first computer worm in 1988. However, over time, the law's ambiguity has resulted in sentences as harsh as decades in jail for small infractions that did not result in economic or bodily damage.

While the law was originally intended to prosecute hackers who committed computer abuse by stealing valuable personal or corporate information or causing damage when they gained access to a computer system, Congress has expanded the CFAA's scope five times, making previously considered misdemeanours federal felonies. As a consequence, even apparently small violations of an application's terms of service might result in punishment.

For example, the CFAA criminalizes white falsehoods such as misrepresenting your age or weight on a dating service (even though this is rarely if ever prosecuted). Additionally, it makes breaching a company's policy against personal use of a work computer a crime. If the law were strictly followed, almost every white collar worker in America would face jail time for computer misuse. Because it is applied arbitrarily and sometimes excessively, federal courts and experts have argued for amending the legislation to decriminalize terms of service infractions. One hurdle to easing the legislation has been opposition from firms that profit from it. For example, one of the 1994 amendments to the CFAA allowed for civil lawsuits, allowing firms to sue workers who stole corporate secrets.

- **Computer Abuse Examples**

A common example of computer misuse that many people overlook is establishing a fictitious social network account. If the terms and conditions of the social media site require users to submit correct information about their identities when registering for an account, they may face prosecution under the CFAA. Although this is rare unless if someone creates a false account for evil objectives, such as cyberbullying, it is a possibility—and the prospect of being punished for something as small as the establishment of a phony account is a significant flaw in the CFAA. Attorneys have used the legislation's flaws to defend clients who should have been penalized, while prosecutors have used the statute to win convictions for minor offenses.

The most well-known example of the unintended consequences of expanding the Computer Fraud and Abuse Act was the threat of a 35-year prison sentence against internet activist Aaron

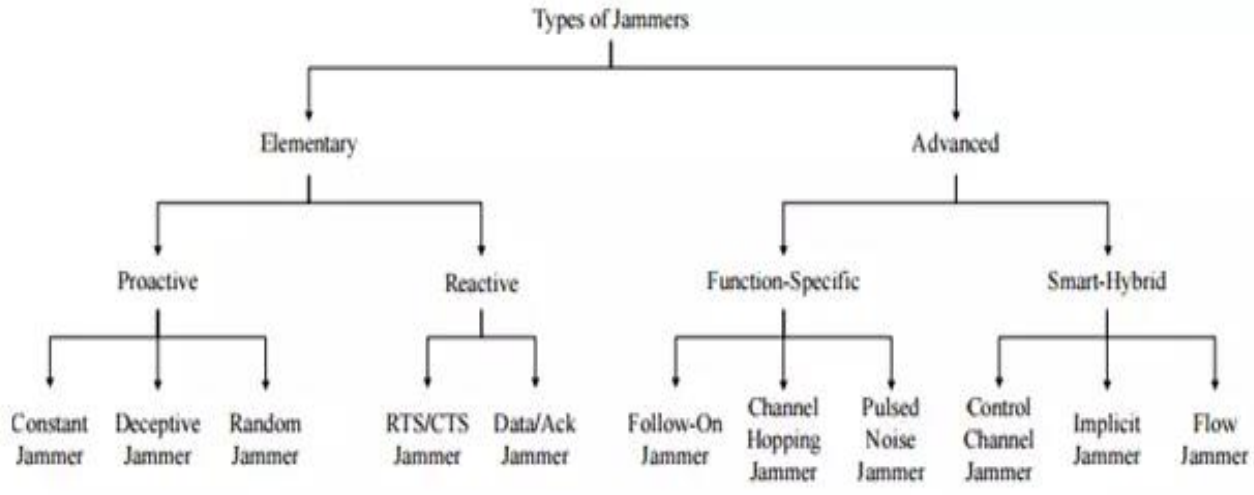
Swartz for allegedly downloading millions of pay-walled academic articles that required a subscription service in order to freely distribute them. While one may argue that Swartz's claimed activities constitute theft, was the recommended sentence proportionate to the purported crime? Swartz did not seem to believe this – he committed himself before the matter could get to trial.

Jamming and anti-Jamming Techniques

Wireless networks are intended for exchanging information of any sort between two or more places that are not physically linked. Wireless networks are subject to many sorts of assaults because of their shared media. There is need to cope with different security challenges. Attackers using a transceiver may be able to delay wireless transmission, introduce undesirable messages, or jam signals of great value. Jamming may be seen as one of a primary means of reducing network performance. In the simplest kind of jamming, the adversary corrupts the content of the original communication by sending radio frequency signals in the network or by blocking the message so that it cannot arrive to the intended recipient. Radio interference threats cannot be readily countered by standard security approaches

Types of jammers

Jammers are malicious wireless nodes that an attacker plants in order to intentionally disrupt a wireless network. A jammer's capabilities might be identical to or different from those of the legal nodes in the network they are assaulting, depending on the attack technique. A jammer's jamming impact is determined by the strength of its radio transmitter, its position, and its affect on the network or targeted node. A jammer may jam a network in a variety of ways to maximize the effectiveness of the jamming. In general, depending on its functionality, a jammer may be classified as basic or sophisticated. We separated the elementary jammers into two subgroups: proactive and reactive. Additionally, the sophisticated ones are divided into two sub-categories: function-specific and smart-hybrid. The comprehensive categorization of various jammers is displayed in the figure below.



A proactive jammer delivers jamming (interfering) signals regardless of whether data transmission is occurring in a network. It transmits packets or random bits through the channel on which it is functioning, thus shutting down all other nodes on the channel. It does not, however, change channels and remains on one until its energy is depleted. Proactive jammers

are classified into three types: persistent, misleading, and random. From now on, anytime we deploy proactive jammers, all three of these scenarios are possible. Constant jammer emits random bits indefinitely and does not adhere to the CSMA standard. A legal node must first determine the state of the wireless medium before sending, according to the CSMA process. The medium is not meant to send a frame until it has been idle for a DCF Interframe Space (DIFS) time.

If the station discovers that the channel is busy during the DIFS period, it should postpone broadcast. By keeping the wireless medium continually active, a persistent jammer stops genuine nodes from connecting with one another. This form of assault is inefficient in terms of energy consumption and detection, but it is very simple to launch and may cripple network connectivity to the point where no one can communicate at all.

Instead of releasing random bits, the deceptive jammer constantly sends normal packets (as in constant jammer). It convinces other nodes that a real signal is occurring, causing them to continue in receiving states until the jammer is switched off or dies. In comparison to a continuous jammer, detecting a deceptive jammer is more difficult since it sends valid packets rather than random bits.

As with the constant jammer, the misleading jammer is wasteful in terms of energy consumption owing to continual transmission, but it is very simple to install. The random jammer sends random bits or regular packets into networks on an irregular basis. Unlike the previous two jammers, this one is designed to save energy. It alternates between two stages on a continual basis: sleep and jamming. It sleeps for a length of time and then activates for the purpose of jamming before returning to sleep. Periods of sleeping and jamming might be set or sporadic. Because it cannot jam during its resting phase, there is a trade-off between jamming efficacy and energy savings. The ratios of sleeping and jamming time may be adjusted to optimize this efficiency-effectiveness trade-off.

The reactive jammer only begins jamming when it detects network activity on a particular channel. As a consequence, a reactive jammer's primary objective is to disrupt a message's receipt. It is capable of disrupting packets of any size. The reactive jammer consumes more energy than a random jammer since it must continually check the network. However, detecting a reactive jammer is far more difficult than detecting a proactive jammer, since the packet delivery ratio (PDR) cannot be reliably established in reality.

When it detects a request-to-send (RTS) message being broadcast by a sender, a reactive RTS/CTS jammer clogs the network. As soon as the RTS is sent, it begins blocking the channel. Since a result, the receiver will not provide a clear-to-send (CTS) response, as the RTS packet delivered by the sender is warped.

The sender will then refrain from transmitting data in the belief that the recipient is already engaged in another transfer. Alternatively, the jammer might wait for the receiver to transmit the RTS then jam when the receiver transmits the CTS. This also results in the transmitter failing to transmit data and the receiver constantly waiting for the data packet.

By distorting data or acknowledgment (ACK) packet transmissions, a reactive data/ACK jammer disrupts the network. It remains inactive until the transmitter end initiates data transmission. This sort of jammer may damage data packets or waits for data packets to reach the recipient before corrupting the ACK packets. Both data packets and ACK messages will be

re-transmitted at the sender end due to corruption. In the first situation, data packets must be re-transmitted since they were not accurately received by the receiver. In the second situation, since the sender does not get ACKs, it assumes that something is wrong on the receiver's side, such as a buffer overflow. As a result, the data packets will be resent.

Function-specific Jammers : Jamming that is function-specific is accomplished by having a pre-determined function. Apart from being proactive or reactive, they may jam a single channel to preserve energy or many channels to enhance jamming throughput regardless of energy consumption. Even though the jammer is jamming a single channel at a time, they are not limited to that channel and may vary their channels to match their specialized functions. The follow-on jammer repeatedly travels across all accessible channels (thousands of times per second) and jams each one for a brief period of time.

If a transmitter discovers the jamming and changes its channel, the follow-on jammer scans the whole band for a new frequency to jam. Alternatively, it might adhere to a pseudo-random frequency hopping sequence. This sort of jammer conserves power by attacking just one channel before moving on to the next. The follow-on jammer's high-frequency hopping rate makes it especially effective against certain anti-jamming systems, such as frequency hopping spread spectrum (FHSS), which use a sluggish hopping rate.

A channel-hopping jammer actively switches between multiple channels. By overcoming the CSMA algorithm given by the MAC layer, this form of jammer has direct access to channels. Additionally, it is capable of jamming several channels simultaneously. The jammer is silent and invisible to its neighbours throughout the finding and vertex colouring stages. Then, according to a specified pseudorandom pattern, it begins launching assaults on various channels at different times.

The pulsed-noise jammer is capable of switching channels and jamming on various bandwidths at different times. As with random jammers, pulsed-noise jammers may save energy by turning on and off according to a timetable. In contrast to the basic proactive random jammer, which targets just one channel, the pulsed-noise jammer targets many channels. Additionally, it may be used to jam several channels simultaneously.

Intelligent Hybrid Jammers – We refer to them as "smart" due to their energy-efficient and excellent jamming capabilities. The primary objective of these jammers is to amplify the impact of their jamming on the network they plan to jam. Additionally, they look after themselves by saving energy. They concentrate enough energy in the proper places to significantly reduce the communication bandwidth for the whole network, or a significant portion of it, in extremely large networks. Each of these types of jammers may be used in a proactive or reactive manner, thus the term hybrid.

In multi-channel networks, control channel jammers operate by jamming the control channel, or the channel that is used to coordinate network activities. A random jammer targeting the control channel might significantly degrade network performance, whilst a continuous jammer targeting the control channel could prevent users from accessing the network entirely. These attacks are often carried out through compromising a network node. Additionally, the hacked nodes might provide future control channel locations.

Implicit jamming attacks are ones that, in addition to impairing the intended target's functionality, also create denial-of-service status on other network nodes. This attack takes use

of the rate adaptation technique employed in wireless networks, in which the AP (Access Point) reduces the rate of the weak node. As a result of this procedure, the AP communicates with this weak node more often than with the other nodes. As a result, when an implicit attacker jams a node talking with the AP, the rate adaptation effect increases the AP's emphasis on the jammed node, resulting in the detriment of other clients.

Flow-jamming attacks use several jammers distributed around the network to disrupt traffic flow. These attacks are initiated by using network-layer information. This form of jamming assault is advantageous for attackers with little resources. If centralized control is used, the minimal amount of power required to jam a packet is calculated and the jammer operates appropriately. To improve efficiency in a non-centralized jammer concept, each jammer exchanges information with neighbouring jammers. We assess the proactive or reactive nature of each jammer, its energy efficiency, and its capacity to jam single or many channels.

Consider a situation in which a jammer disrupts the channel by blocking one or more nodes and corrupting or blocking packets. This continual jamming may be used to launch distributed denial of service attacks. The jammer manipulates the jamming probability and transmission range in order to inflict the greatest amount of harm on the network in terms of faulty transmission connections. When the jammer is detected by a monitoring node and a notification message is sent out of the jamming zone, the jammer operation terminates. Several statistics are utilized to identify jamming assaults, including signal strength, carrier sensing time, and packet delivery ratio. The present approach assumes that the jammer's purpose is to interfere with genuine wireless networks. Assuming that A and B are participating nodes and X is the jamming node, A is now unable to deliver packets for a variety of reasons. For instance, X may broadcast the signal continually such that A never detects the channel as idle; alternately, A can send packets to A and cause A to constantly receive the garbage packets. Thus, it is vital to quantify the jammer's efficacy, and two matrices have been established for this purpose: packet send ratio and packet delivery ratio.

Jamming attacks are often initiated by transmitting radio frequency signals; these assaults are impossible to avoid using traditional security methods. A jammer's purpose is to disrupt lawful wireless transmission. A jammer may accomplish this purpose by either obstructing legitimate traffic or by inhibiting message receipt. There are several jamming models that a jammer might use to combat jamming assaults. This is the primary reason detecting jamming is very difficult and critical since it is the first step toward establishing a secure and reliable wireless channel. In conventional systems, a jammer blocks a portion of a single wireless channel. The jammer manipulates the likelihood of jamming and the broadcast range in order to inflict maximum harm.

Anti-jamming measures in mobile wireless networks

The majority of jamming detection and mitigation techniques are developed and assessed in static networks. In a mobile network context, where jammers might roam and cause jammer detection and localization algorithms to fail, the ant jamming issue becomes more difficult. Thus far, it seems as if spatial retreats are the only method used on mobile nodes. Developing a cost-effective method for wireless mobile networks remains a challenge. Anti-jamming systems for mobile networks should be capable of rapidly detecting and responding to jamming in wireless networks. Additionally, since the same jammer may migrate and cause jamming in

different sections of the network, determining ways to avoid jamming using prior jamming data would be very intriguing.

- **Anti-jamming technique applicable to everyone**

Finally, we'd want to raise the ultimate question: is it conceivable to have a single realistic anti-jamming system that works across all sorts of wireless networks (static or mobile, sensor or Wi-Fi, infrastructure-based or ad-hoc) and detects all forms of jammers?

Furthermore, with so many powerful jamming methods at our disposal, can we employ them for any constructive purpose?

Regardless of how efficient a jammer is, there is always one or more anti-jamming procedures that correlate. After discussing many sorts of jamming detection and countermeasure strategies, we realize that ant jamming is such an intriguing topic that numerous approaches have been attempted to resolve it. Artificial intelligence, game theory, mobile agents, cross layer, spatial retreat, consistency check, and channel or frequency hopping are all examples of techniques that have been used to this topic. Certain techniques, such as JAM, map out the blocked region in order to prevent sending packets inside it. Other techniques, such as the Hermes node, detect jamming and alter channels or physically relocate nodes. In summary, when nodes detect network jamming, they may either switch to a non-jammed channel, route packets outside the jamming zones, or simply migrate to a non-jammed area.

Hacking

Hacking is the act of attempting to gain access to a computer system or a private network contained inside a computer. In a nutshell, it is the illegal access to or control of computer network security systems for the goal of committing an unlawful act.

To characterize hacking more accurately, one must first comprehend hackers. One may readily presume they are clever and tech savvy. Indeed, breaching a security system takes a higher level of intellect and ability than developing one. There are no clear and fast criteria that allow us to neatly compartmentalize hackers. However, in common computer jargon, they are referred to as white hats, black hats, and grey hats. White hat professionals hack to test the security of their own systems in order to make them more hack-proof. They are often affiliated with the same organization.

Black hat hackers hack in order to get control of a system for their own personal advantage. They are capable of destroying, stealing, and even preventing authorized users from gaining access to the system. They do this by exploiting systemic flaws and vulnerabilities. Some computer specialists refer to them as crackers rather than hackers. Grey hat hackers are interested individuals who possess just enough computer language abilities to hack a system in order to discover possible security flaws. Grey hats differ from black hats in that the former inform the network administrator of found vulnerabilities in the system, whilst the latter is exclusively interested in personal benefit. All forms of hacking are considered unlawful, with the exception of work performed by white hat hackers.

Sniffing and its Types

Sniffing is the technique of monitoring and recording all data packets that traverse a network. Network/system administrators employ sniffers to monitor and troubleshoot network traffic.

Sniffers are used by attackers to collect data packets carrying sensitive data such as passwords and account information. Sniffers may be placed as hardware or software on the system. A hostile attacker may collect and analyze all network traffic by running a packet sniffer in promiscuous mode on a network.

There are two distinct types:

- **Active Sniffing:**

Active sniffing is sniffing in the switch. A switch is a network device that connects two points. The switch controls the flow of data between its ports by continuously monitoring the MAC address assigned to each port, ensuring that data is sent to its intended destination. To collect communication between targets, sniffers must actively inject traffic into the LAN. This may be accomplished in a variety of ways.

- **Passive Sniffing:**

This is the technique by which the hub gets sniffed. All traffic travelling across the non-switched or unbridged network segment is visible to all computers on it. Sniffers function at the network's data connection layer. Any data sent via the LAN is truly transmitted to every computer linked to it. This is referred to as passive sniffing because the attackers' sniffers passively wait for data to be delivered and record it.

Malware | What is Malware & How to Stay Protected from Malware Attacks

Malware is a catch-all word for viruses, trojans, and other disruptive computer programs that threat actors employ to infiltrate systems and networks in order to get access to sensitive information.

Malware (short for "malicious software") is a file or piece of code that is generally sent through a network and is capable of infecting, exploring, stealing, or conducting nearly any action an attacker desires. Additionally, since malware comes in a variety of flavors, there are multiple ways to infect computers. Though malware may take on a variety of forms and capabilities, it often has one of the following objectives:

- Provide an attacker with remote control over an infected system.
- Send spam to unsuspecting recipients from the compromised system.
- Investigate the local network of the affected user.
- Steal confidential information.

Malware is classified into the following categories:

Malware is an umbrella word that refers to all forms of harmful software. Malware examples, malware attack definitions, and malware distribution strategies include the following:

While certain kinds of adware may be regarded legal, others gain unwanted access to customers' computers and cause significant disruption.

Botnets, An abbreviation for "robot network," these are networks of compromised computers controlled by a single attacker through command-and-control servers. Botnets are very adaptive and agile, able to maintain resilience via redundant servers and traffic relaying through

infected PCs. Botnets are often the army behind distributed denial-of-service (DDoS) assaults in the modern day.

Cryptojacking is a form of malicious cryptomining (the process of using computing power to verify transactions on a blockchain network and earning cryptocurrency in exchange for providing that service) that occurs when cybercriminals hack into business and personal computers, laptops, and mobile devices in order to install software.

Malvertising - The term "malvertising" is a combination of the words "malware" and "advertising," and refers to the practice of using web advertising to propagate malware. It is often accomplished by inserting malicious code or adverts containing malware into legal internet advertising networks and websites.

Polymorphic malware — Any of the above-mentioned varieties of malware that has the ability to "morph" on a regular basis, changing the look of the code while preserving the algorithm. The change of the software's surface appearance evades identification by conventional viral signatures.

Ransomware - Is a criminal business model in which malicious software is used to encrypt valuable files, data, or information. Businesses that fall victim to a ransomware assault may have their operations significantly harmed or completely shut down.

Remote Administration Tools (RATs) — Software that enables remote control of a system by a remote operator. Although these technologies were first developed for lawful purposes, they are currently being employed by threat actors. RATs provide an attacker administrative power, enabling them to do almost any action on an infected machine. They are difficult to identify because they do not appear in lists of currently running applications or processes, and their behaviors are often confused with those of legal programs.

Rootkits — Programs that provide a computer privileged (root-level) access. Rootkits come in a variety of flavors and conceal themselves inside the operating system.

Spyware - Malware that gathers information about the infected computer's use and transmits it to the attacker. Botnets, adware, backdoor activity, keyloggers, data theft, and net-worms are all included in this phrase.

Trojans Malware - Malware that is camouflaged as genuine software. Once triggered, malware Trojans will do the task for which they were intended. In contrast to viruses and worms, Trojans do not multiply or spread through infection. The term "Trojan" refers to the ancient account of Greek troops concealed within a wooden horse given to the hostile city of Troy.

Malware Viruses - Programs that replicate themselves throughout a computer or network. Malware viruses attach themselves to existing applications and are triggered only when the user starts the software. At its most destructive, viruses may damage or destroy data, propagate through the user's email, or completely wipe out a hard drive.

Worm Malware — Self-replicating viruses that take advantage of security flaws to propagate automatically across systems and networks. In contrast to many viruses, malware worms do not infect existing programs or modify existing data. They generally go undetected until replication grows to a point where system resources or network bandwidth are depleted.

- **Types of Malware Attacks**

Malware also employs a number of tactics to expand beyond the original attack vector. Malware attack definitions may include the following:

Unsuspecting consumers may open email attachments containing malicious malware. If such emails are sent, the virus may go even farther within a business, compromising the network further.

File servers, such as those based on the standard Internet file system (SMB/CIFS) or the network file system (NFS), may facilitate the propagation of malware by allowing users to view and download infected files.

Malware may propagate on removable media and then on computer systems and networks through file-sharing applications.

By exchanging things as apparently innocuous as music or images, peer to peer (P2P) file sharing might introduce malware.

Remotely exploitable vulnerabilities allow a hacker to get access to a computer system regardless of its geographic location with little or no input from the computer user.

Learn how to secure your network against all sorts of malware, both known and unknown, by using Palo Alto Networks' next-generation threat prevention capabilities and Wildfire cloud-based threat analysis service.

- **How to Prevent Malware:**

To identify and prevent malware, a range of security technologies are deployed. Firewalls, next-generation firewalls, network intrusion prevention systems (IPS), deep packet inspection (DPI) capabilities, unified threat management systems, antivirus and anti-spam gateways, virtual private networks, content filtering, and data leak prevention systems are just a few examples. To avoid malware, all security solutions should be thoroughly tested against a variety of malware-based assaults to guarantee they are functioning effectively. A strong, up-to-date malware signature library must be employed to guarantee that testing is carried out against the most recent threats.

Cortex XDR combines multiple prevention methods at critical stages of an attack's lifecycle to halt the execution of malicious programs and prevent the exploitation of legitimate applications, regardless of the operating system, the endpoint's online or offline status, or whether it is connected to an organization's network or roaming. Due to the fact that the Cortex XDR agent is not reliant on signatures, it is capable of preventing zero-day malware and undiscovered vulnerabilities using a variety of protection measures.

- **Malware Detection:**

There are sophisticated malware analysis and detection methods available, including firewalls, intrusion prevention systems (IPSs), and sandboxing solutions. Certain varieties of malware are easy to detect, such as ransomware, which becomes visible immediately after encrypting your information. Other malware, like as spyware, may linger quietly on a target machine, allowing an adversary to keep access. Regardless of the nature or meaning of malware, its detectability, or the person who deploys it, malware usage is always malevolent.

When behavioral threat prevention is enabled in your endpoint security policy, the Cortex XDR agent may additionally monitor endpoint activity constantly for Palo Alto Networks-identified harmful event chains.

Malware Removal:

Antivirus software is capable of removing the majority of common infection types, and several off-the-shelf solutions are available. Following an alert or investigation, Cortex XDR enables administrators to initiate a variety of mitigation steps, including isolating compromised endpoints by disabling all network access on compromised endpoints except for traffic to the Cortex XDR console, terminating processes to prevent any running malware from continuing to perform malicious activity on the endpoint, and blocking additional executions, before quarantining malicious files.

Malware Protection:

To safeguard your business against malware, you need an enterprise-wide, comprehensive malware prevention plan. Commodity attacks are fewer complex exploits that are more readily discovered and blocked when combined with antivirus, anti-spyware, and vulnerability prevention tools on the firewall, as well as URL filtering and application identification capabilities.

Spoofing – Definition and Explanation

Spoofing is a term used in cybersecurity to describe when fraudsters appear to be someone or something else in order to gain a person's confidence. Typically, the motivation is to obtain access to systems, steal data, steal money, or distribute malware.

Spoofing is a general word that refers to the act of a cybercriminal impersonating a trusted entity or device in order to convince you to do an action advantageous to the hacker — and destructive to you. Spoofing occurs whenever an online fraudster disguises their identity as something else.

Spoofing is applicable to a variety of communication mediums and entails varying degrees of technological sophistication. Spoofing attacks sometimes have a social engineering component, in which fraudsters psychologically influence their victims by exploiting human weaknesses like as fear, greed, or a lack of technical understanding.

Spoofing often consists of two components: the spoof itself, such as a forgery of an email or website, and the social engineering component, which prompts victims to act. For instance, spoofers may send an email purporting to be from a trusted senior co-worker or boss, requesting that you make an online money transfer and offering a compelling justification for the request. Spoofers often know which strings to tug in order to convince a victim to do the required action in this case, approving a fraudulent wire transfer without raising suspicion.

A successful spoofing attack may have major repercussions, including the theft of personal or corporate information, the harvesting of credentials for use in subsequent attacks, the propagation of malware, illegal network access, and evading access restrictions. Spoofing attacks may sometimes result in ransomware attacks or expensive data breaches for corporations.

There are several sorts of spoofing attacks: the most common use emails, websites, and phone calls. Technical assaults using IP addresses, Address Resolution Protocol (ARP), and Domain Name System (DNS) servers are increasingly sophisticated. Below, we'll look at some of the most popular spoofing cases.

Spoofing techniques

- **Email forgery**

Email spoofing is one of the most often utilized assaults. It happens when the sender forges email headers so that the recipient's client software shows the false sender address, which the majority of users believe at face value. Unless they carefully scrutinize the header, email recipients think the message was delivered by the bogus sender. If people recognize the name, they are more inclined to believe it.

Spoof emails often seek money transfers or access to a system. Additionally, they may include attachments that, when opened, install malware — such as Trojans or viruses. Oftentimes, malware is meant to move beyond your computer and attack your whole network.

Email spoofing is highly reliant on social engineering – the capacity to persuade a human user that what they are seeing is authentic, motivating them to act and open an attachment, transfer money, and so on.

How to detect and prevent email spoofing:

Unfortunately, it is hard to totally eliminate email spoofing since the protocol used to transmit emails – called the Simple Mail Transfer Protocol – does not need authentication. Ordinary people, on the other hand, may mitigate the danger of email spoofing attacks by selecting a secure email service and following basic cybersecurity hygiene:

When enrolling for websites, use disposable email addresses. This minimizes the possibility of your private email address being included in lists used to mass send faked email messages.

Ascertain that your email password is both secure and complicated. A strong password makes it more difficult for fraudsters to get access to your account and use it to send dangerous emails.

Inspect the email headers if possible. (This is dependent on your email provider and is only available on desktop.) The email header includes information about how and where the email was routed to you.

Enable your spam filter.

This should prevent the majority of fake emails from reaching your inbox.

Spoofing an IP address

While email spoofing is largely directed at the individual, IP spoofing is primarily directed at a network.

IP spoofing is a technique used by attackers to obtain unauthorized access to a system by sending messages with a forged or spoofed IP address that seems to originate from a trustworthy source, such as another computer on the same internal computer network.

Cybercriminals do this by stealing the IP address of a valid host and modifying the packet headers transmitted from their own system to make them seem to originate from the legal host. IP spoofing attacks must be detected early, since they often occur as part of DDoS (Distributed Denial of Service) assaults, which may bring a whole network down. You can learn more about IP spoofing in our in-depth article.

How to avoid IP spoofing — website owners' tips:

- Keep an eye out for unexpected behaviour on networks.
- Utilize packet filtering systems that are capable of identifying irregularities, such as outgoing packets from sources that do not match those on the network.
- Verification procedures should be used for every remote access (even among networked computers).
- Verify the authenticity of all IP addresses.
- Utilize a network assault preventative measure.
- Ascertain that at least a portion of your computer's resources are protected by a firewall.
- Spoofing a website

Website spoofing sometimes referred to as URL spoofing — occurs when criminals create a phony website that seems to be authentic. The counterfeit website will have a recognizable login page, stolen logos and comparable branding, and even a legitimate-looking URL. These websites are created by hackers in order to steal your login information and perhaps install malware on your machine. Frequently, website spoofing occurs in connection with email spoofing for instance, fraudsters may send you an email including a link to the bogus website.

How to protect yourself against website spoofing:

Examine the URL bar - a faked website is improbable to be safe. To verify, the URL should begin with https:// rather than http:// - the "s" stands for "secure," and the address bar should also have a lock symbol. This indicates that the site's security certificate is current. If a site lacks this, it does not always indicate it has been faked, search for other indicators as well.

Keep an eye out for incorrect wording or language, as well as logos or colors that look slightly off. Verify that the material is full for instance, faked websites sometimes neglect to fill the privacy statement or terms & conditions with true text.

Consider using a password manager - software that automatically fills in login credentials will not function on faked websites. If the program fails to automatically fill in the password and username boxes, this may indicate that the website has been faked.

- **Caller ID forgery or telephone spoofing**

Caller ID spoofing – also known as phone spoofing – occurs when fraudsters purposefully alter the information supplied to your caller ID in order to conceal their identity. They do this because they know you are more likely to pick up the phone if you believe the call is from a local number rather than an unknown number.

Caller ID spoofing is accomplished via the use of VoIP (Voice over Internet Protocol), which enables fraudsters to fake any phone number and caller ID. Once the receiver accepts the call, the fraudsters attempt to gather crucial information in order to commit fraud.

How to prevent a spoofer from using my phone number:

Consult your phone carrier to see if they provide a service or software that assists in identifying or filtering out spam calls.

Consider utilizing third-party applications to assist in blocking spam calls – but keep in mind that you will be providing personal information with them.

Often, it is advisable not to answer a call from an unknown number. Responding to spam calls attracts further spam calls, since the fraudsters now see you as a possible victim.

- **Spoofing text messages**

Text message spoofing – also known as SMS spoofing – occurs when the sender of a text message deceives recipients by displaying false sender information. Legitimate firms may use this for marketing reasons by substituting a short and easy-to-remember alphanumeric ID for a lengthy number, presumably to make it simpler for consumers. However, fraudsters do the same thing - they conceal their true identities behind an alphanumeric sender ID, often posing as a respectable firm or institution. Frequently, these counterfeit messages include links to SMS phishing (commonly referred to as "smishing") websites or malware downloads.

How to prevent text messaging spoofing:

As far as possible, avoid clicking on links included in text messages. If an SMS purporting to be from a firm you know urges you to take immediate action, go straight to their website by entering in the URL or using a search engine, rather than clicking on the SMS link.

Never click on "password reset" links included in SMS messages they are almost always frauds.

Bear in mind that banks, telecommunications companies, and other respectable service providers never request personal information by SMS - therefore do not submit personal information in this manner.

Caution should be used when receiving "too good to be true" SMS messages offering prizes or discounts they are almost always frauds.

ARP spoofing is a technique that allows network messages to reach a specified device on a network. ARP spoofing, alternatively referred to as ARP poisoning, happens when a hostile actor transmits forged ARP packets over a local area network. This establishes a connection between the attacker's MAC address and the IP address of a genuine network device or service. This connection enables the attacker to intercept, change, or even prevent data intended for that IP address from being sent.

- **Preventing ARP poisoning:**

Individuals may protect themselves from ARP poisoning by using a Virtual Private Network (VPN).

Organizations should use encryption – specifically, HTTPS and SSH protocols – to help mitigate the likelihood of an ARP poisoning assault succeeding.

Additionally, organizations should investigate the use of packet filters - filters that prevent malicious transmissions and packets with questionable IP addresses.

- **Spoofing of the DNS**

DNS spoofing – also known as DNS cache poisoning – is a kind of attack in which manipulated DNS records are used to redirect internet traffic to a bogus website that seems identical to the legitimate destination. Spoofers do this by changing the DNS server's IP addresses with the ones desired by the hackers. You can read our whole essay on DNS spoofing attacks here.

- **How to protect against DNS spoofing:**

Individuals should never click on an unknown link, utilize a Virtual Private Network (VPN), check their devices for malware on a regular basis, and flush their DNS cache to resolve poisoning.

Use DNS spoofing detection tools, domain name system security extensions, and end-to-end encryption for website owners.

- **GPS eavesdropping**

GPS spoofing happens when a GPS receiver is duped into transmitting erroneous signals that seem to be genuine. This indicates that the fraudsters are feigning to be in one area while they are really in another. This can be used to hack a car's GPS and direct you in the wrong direction, or – on a much larger scale – to potentially interfere with the GPS signals of ships or aircraft. Numerous mobile applications depend on location data from smartphones and hence are susceptible to this kind of spoofing attack.

- **How to protect yourself against GPS spoofing:**

Anti-GPS spoofing technology is being developed, however it is being targeted mostly at big systems, such as marine navigation.

The most straightforward (though inconvenient) approach for people to safeguard their smartphones or tablets is to switch them to "battery-saving location mode." In this mode, your position is determined only by Wi-Fi and cellular networks; GPS is deactivated (this mode is unavailable on some devices).

- **Spoofing facial expressions**

Facial recognition technology is rapidly being used to unlock mobile devices and computers, as well as in a variety of other applications, including law enforcement, airport security, healthcare, education, marketing, and advertising. Facial recognition spoofing may occur as a result of unlawfully acquired biometric data, which can be gained directly or surreptitiously from an individual's internet profile or via hacked networks.

- **How to protect yourself against face spoofing:**

The majority of anti-spoofing techniques for face recognition rely on Liveliness Detection. This identifies if a face is genuine or a forgery. Two strategies are used:

Eye blink detection which detects patterns in blink intervals – denies access to fraudsters who cannot match these patterns.

Interactive detection - in which users are prompted to do particular facial motions in order to verify their authenticity.

How to guard against spoofing

In general, the following online safety practices can help reduce your vulnerability to spoofing attacks:

Avoid clicking on links or opening attachments from strange sources. They may include malware or viruses that are capable of infecting your device. When in doubt, avoid.

Never respond to emails or phone calls from unknown senders. Any interaction with a scammer entails the danger of receiving further unsolicited texts.

Configure two-factor authentication wherever feasible. This provides an additional degree of protection to the authentication process, making it more difficult for attackers to get access to your devices or online accounts.

Utilize secure passwords. A strong password is one that is difficult to guess and should preferably include a mix of upper- and lower-case letters, special characters, and digits. Avoid using the same password across several accounts and change it often. A password manager is a fantastic method to keep track of all of your passwords.

Conduct an audit of your internet privacy settings. If you use social networking sites, use caution in who you connect with and get familiar with how to utilize your privacy and security settings to keep secure. If you see strange activity, click on spam, or are a victim of online fraud, take measures to safeguard your account and report it.

Make no online disclosures of personal information. Avoid giving personal or private information online unless you are absolutely certain the source is a reputable one.

Maintain an up-to-date network and software. Security patches, bug fixes, and new features are all included in software updates, staying current decreases the chance of malware infection and security breaches.

Keep an eye out for websites, emails, and messages that have faulty spelling or grammar – as well as any other elements that seem to be wrong, such as logos, colors, or missing material. This might be an indication of spoofing. Visit only websites that display a genuine security certificate.

In the United States, victims of spoofing may submit a complaint with the Federal Communications Commission's Consumer Complaint Center. Other jurisdictions have equivalent bodies with their own complaint processes. If you have suffered financial loss as a result of spoofing, you may contact law police.

The most effective method of ensuring internet safety is via the use of a comprehensive antivirus software solution. We propose Kaspersky Total Security, a comprehensive cybersecurity solution that will safeguard you and your family online and provide a more secure browsing experience.

Identity theft

Identity thieves often get personal information about their victims, such as passwords, identification numbers, credit card numbers, or social security numbers, and use these to commit fraud in their name. These sensitive facts may be utilized for a variety of illicit

objectives, including loan applications, internet purchases, and gaining access to a victim's medical and financial information.

Identity theft is inextricably related to phishing and other social engineering methods that are often used to coerce victims into disclosing personal information. Additionally, public profiles on social media platforms or other prominent internet services may be exploited as a source of data, assisting thieves in impersonating their targets.

Once identity thieves have gathered this information, they may use it to place orders, take over victims' internet accounts, and file lawsuits in their names. Individuals who are impacted may incur financial loss in the near term as a result of illicit withdrawals and transactions made in their names.

In the long run, victims may be held accountable for the offenders' activities and investigated by law enforcement authorities, as well as face penalties like as legal charges, changes to their credit status, and harm to their good reputations.

- **How to protect yourself from identity theft**

Secure your connection: If you're going to utilize your personal information online, do it exclusively over a secure connection - ideally through your home or office network or cellular data. Avoid free public Wi-Fi that does not need a password. If you are unable to avoid it, utilize a virtual private network (VPN) to encrypt all your communications and therefore protect you from eavesdropping thieves.

Maintain the security of your devices: Utilize a dependable, multi-layered, and up-to-date security solution to safeguard your laptop, smartphone, and tablet from harmful software and attackers.

Avoid suspicious communications and websites: Visit our spam and phishing pages to learn how to identify social engineering attempts that are attempting to steal your personal data.

Maintain a strong password hygiene policy: Create lengthy, difficult-to-guess, and unique passwords. Additionally, you may use passphrases to make passwords simpler to remember, or you can save all your passwords in a password manager to ensure their security. Utilize two-factor authentication wherever feasible to give another degree of safety to your credentials.

One critical point to remember: Never reuse a password across different accounts or services. This manner, even if attackers succeed in obtaining this password, their harm is restricted to the compromised account (or service).

Monitor your bank and credit accounts: Keep an eye out for odd behavior in your online banking account and credit ratings. This may assist you in detecting an assault prior to it wreaking havoc on your cash or reputation. Additionally, establish transaction restrictions to prevent money from being misused.

Take care with sensitive data: If you choose to dispose of any physical papers containing personal information, ensure that you do so securely either by rendering them unrecoverable or destroying them. Your electrical gadgets follow a similar logic: When selling or discarding outdated cell phones, tablets, or computers, ensure that any sensitive data on them has been deleted.

Avoid excessive sharing: In an age where the majority of users have many social media accounts, over sharing may be a big issue. Even more so when the postings, images, or videos include sensitive information that may be used to impersonate you – for example, your identification, purchase orders, travel tickets, or other such papers. Avoid sharing any of them, as well as excessive data about your personal life and past, which might be exploited to commit crimes in your name by criminals.

J. CASE STUDY MY HANDS-ON EXPERIENCE SOFTWARE TESTING

Security testing

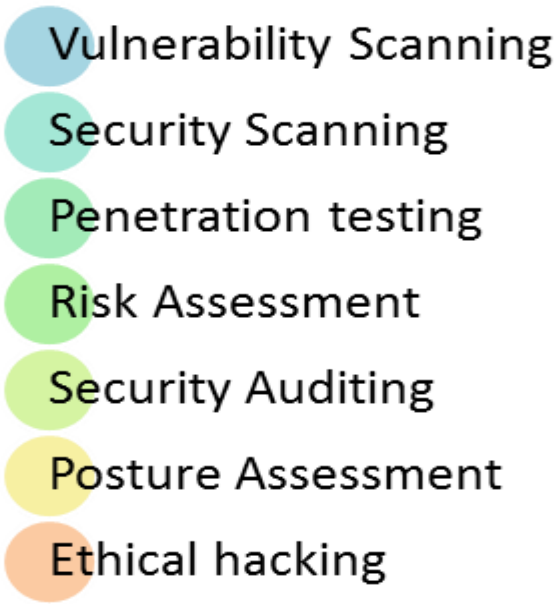
Security testing is a procedure that identifies faults in an information system's security measures that safeguard data and ensure that the system operates as intended. Due to the logical constraints of security testing, passing the procedure does not imply that no faults exist or that the system fulfils the security criteria satisfactorily.

Specific security needs may include the following: confidentiality, integrity, authentication, availability, authorisation, and non-repudiation. The actual security requirements that are tested are determined by the system's security needs. The word "security testing" has a variety of distinct connotations and may be carried out in a variety of different ways. As such, a Security Taxonomy enables us to comprehend these disparate methods and interpretations by establishing a common denominator.

The primary objective of security testing is to discover threats inside the system and to quantify its possible vulnerabilities, ensuring that threats may be confronted and the system does not cease to operate or is not exploited. Additionally, it assists in identifying any potential security concerns inside the system and assisting developers in resolving them via code.

Types of Security Testing

There are seven basic forms of security testing as per Open Source Security Testing methodology document. They are explained as follows:



Vulnerability Scanning: This is accomplished by scanning a system against known vulnerability signatures using automated tools.

Security Scanning: This process identifies network and system vulnerabilities and then recommends solutions for mitigating these risks. This scanning may be conducted manually or automatically.

Penetration testing: This kind of testing replicates a hostile hacker's attack. This testing entails an examination of a specific system in order to identify possible vulnerabilities to an external hacking effort.

Risk Assessment: This phase of testing includes an examination of the organization's security risks. Risks are categorised into three categories: Low, Medium, and High. This testing offers risk-reduction controls and strategies.

Security Auditing: This is an internal examination of applications and operating systems for vulnerabilities in terms of security. Additionally, an audit may be conducted by inspecting the code line by line.

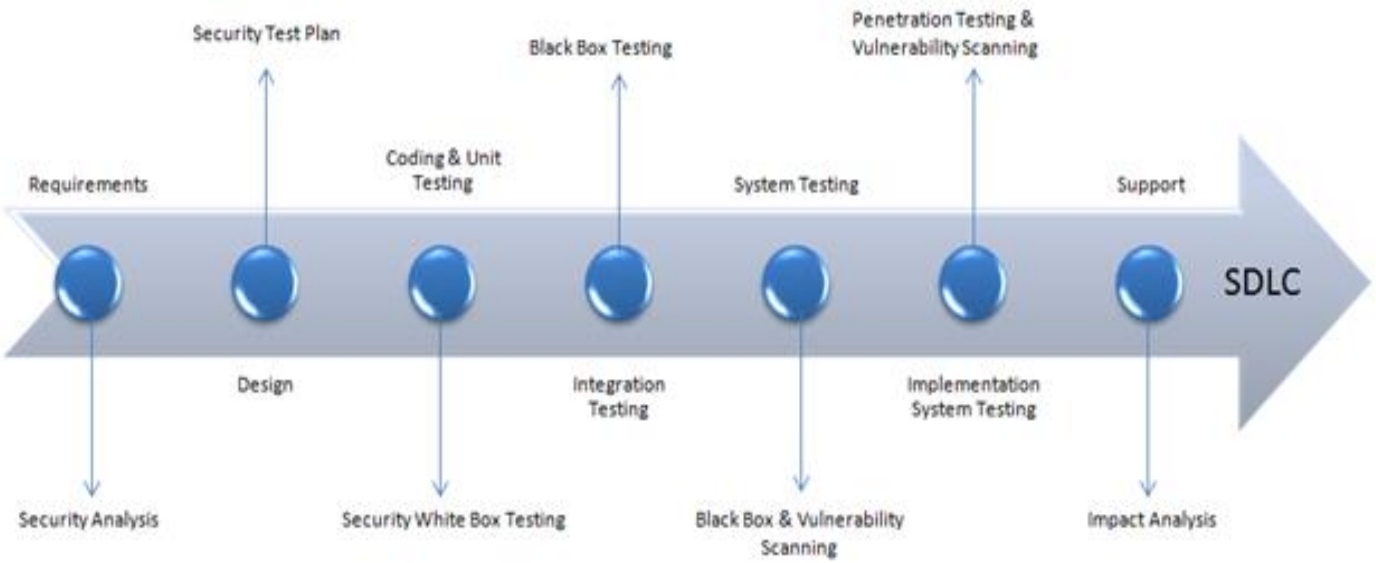
Ethical hacking is a term that refers to the act of hacking into an organization's software systems. In contrast to criminal hackers who steal for their personal benefit, the objective is to disclose system security problems.

Posture Assessment: This combines security scanning, ethical hacking, and risk assessment to determine an organization's overall security posture.

How to do Security Testing

It is well accepted that the expense of security testing will increase if we delay it until after the software implementation phase or after deployment. As a result, it is critical to include security testing early in the SDLC life cycle.

Consider the security procedures that should be used for each step of the SDLC.



SDLC Phases	Security Processes
Requirements	Security analysis for requirements and check abuse/misuse cases
Design	Security risks analysis for designing. Development of Test Plan including security tests
Coding and Unit Testing	Static and Dynamic Testing and Security White Box Testing
Integration Testing	Black Box Testing
System Testing	Black Box Testing and Vulnerability scanning
Implementation	Penetration Testing, Vulnerability Scanning
Support	Impact analysis of Patches

The test plan should include

- Security-related test cases or scenarios
- Test Data related to security testing
- Test Tools required for security testing
- Analysis of various tests outputs from different security tools

System Testing

System Testing is a kind of testing that verifies the software product as a whole and completely integrated. A system test is used to examine the end-to-end specifications of a system. Typically, software is a subsystem of a larger computer-based system. The program is ultimately interfaced with other software/hardware systems. System testing is essentially a collection of distinct tests designed to exercise the whole computer-based system. System testing is a blackbox exercise. There are two types of software testing.

- Black Box Testing
- White Box Testing

System testing is a kind of black box testing in the context of software testing.

White box testing is the examination of a software application's internal operations or code. Black box or system testing, on the other hand, is the polar opposite. System testing examines the software's exterior operations from the user's viewpoint.

As with practically every other aspect of software engineering, software testing follows a specified sequence of operations. The following is a chronological list of software testing categories. The following are the methods used to thoroughly test new software prior to selling it:

During development, unit testing is conducted on each module or block of code. Typically, unit testing is performed by the programmer who wrote the code.

Integration testing is performed before to, during, and after a new module is integrated into the main software package. This entails doing tests on each individual code module. A single piece of software might comprise many modules, which are often built by multiple programmers. It is critical to evaluate the impact of each module on the overall program model.

Before a finished software product is offered to the market, it is subjected to system testing by a professional testing agency.

Acceptance testing product beta testing conducted by real end consumers.

Different Types of System Testing

System testing is classified into more than 50 subtypes. Click here for a complete list of software testing types. The following section discusses the many forms of system testing that a major software development business may do.

Usability Testing - primarily focuses on the user's ease of use, control flexibility, and the system's capacity to accomplish its goals.

Load Testing — is required to ensure that a software solution performs as expected under real-world load conditions.

Regression Testing - is used to ensure that no modifications made during the development process resulted in the introduction of new problems. Additionally, it ensures that no existing flaws are introduced as a result of the gradual integration of new software components.

Recovery testing - is used to show that a software solution is dependable, trustworthy, and capable of recovering effectively from a probable crash.

Migration testing- is performed to guarantee that software can be successfully transferred from legacy system infrastructures to modern system infrastructures.

Functional Testing — Also referred to as functional completeness testing, functional testing entails considering any potential missing functionalities. During functional testing, testers may compile a list of possible enhancements to a product's functionality.

Testing of Hardware and Software - IBM refers to testing of hardware and software as "HW/SW Testing." This is the phase of system testing during which the tester focuses only on the interactions between hardware and software.

The Interview and assessment

An interview is "a formal face-to-face encounter, particularly one convened for the purpose of assessing an applicant's credentials, such as for employment or admittance.... A discussion, such as one conducted by a reporter, in which someone is elicited to provide facts or claims.

During the systems analysis phase of a development project, the interview is the key tool for acquiring information. It is a talent that every analyst must learn. The analyst's interviewing skills dictate what information is acquired, as well as the quality and depth of that information. The analyst's key tools are interviewing, observation, and research.

The interview is a unique kind of meeting or conference that often involves just two people: the interviewer and the interviewee. In exceptional cases, more than one interviewer or

interviewee may be present. In these instances, one primary interviewer and one primary interviewee should remain.

- **Different Types of Interviews**

Interviews are done throughout the analytic process for a number of reasons and with a range of objectives in mind. An interview might be done at any point along the process to ascertain

- Initial introduction
- Familiarity or antecedents
- Compilation of facts
- Verification of data collected in other locations
- Confirmation of the interviewee's information
- Suggestions, elaboration, and clarification

Components of the Interview

The interview procedure is divided into many stages.

- The interviewee is chosen and the interview time is scheduled.
- Developing interview questions or a script
- The interview in its entirety
- The interviewee's facts and information are documented.
- With the interviewee, go through the interview transcript.
- Corrections to the draft, signature, and filing

During the data collection phase of the analysis process, one of the analyst's first and most critical jobs is to decide who needs to be questioned. This involves interviewee selection, a comprehension of what can be anticipated from an interview with a person at a given level, how to check the information obtained during an interview, and, most importantly, an understanding of the person being interviewed's viewpoint.

In the majority of analysis projects, the analysis team is given a user liaison. This individual is responsible for introducing the analyst to persons being questioned, providing background information, and interpreting (or translating) the information gathered during the interviews. This person is often also responsible for supporting the analyst in selecting individuals to interview, arranging the interviews, and, in certain situations, attending the interviews.

Under typical circumstances, the analyst will have access to all users in the user area, but they will not all be interviewed. This is particularly true for those with a big user area.

In general, the list of individuals to interview may be classified into three categories:

- The most senior executive,
- Subordinates and junior managers,
- Line workers, clerks, manufacturing personnel, and sales personnel, among others.

Automated Testing

Automated testing, often known as test automation, is a technique used in software testing that use specialized software tools to manage the execution of tests and then compares the actual

test results to projected or expected outcomes. This is all accomplished automatically, with little or no assistance from the test engineer. Automation is used to supplement manual testing by doing tasks that would be too complex to execute manually.

Testing is a critical component of the development process. It assures that all defects are resolved and the product, whether software or hardware, performs as anticipated or as near to the target performance as feasible. Even yet, certain jobs are too time consuming to do manually, despite their simplicity. Automated testing comes in handy in this situation.

Among the primary benefits of automated testing are the following:

- Saves time and money by increasing the efficiency of testing
- Increases testing accuracy as compared to human-directed testing
- Increases test coverage by enabling the simultaneous deployment of numerous testing tools, allowing for concurrent testing of various test scenarios.

Contributes to the development process by assisting developers in locating problems and mistakes more rapidly.

Manual testing is still used at different stages of development, although it is mostly used by developers or hardware engineers to rapidly determine whether changes, they have made had the expected impact. Extensive overall testing will be conducted later on when a product has undergone a series of modest alterations or a significant change.

Agile Testing

Agile testing is based on the premise that continuous testing is as critical to development as coding.

Testing is included into the development process in Agile to ensure that issues are detected as early and often as feasible. As a consequence, testers may detect issues at any stage of the development process, expediting the product's delivery.

- **Types of Testing in Agile**

Agile testing techniques have resulted in the development of a plethora of approaches. The following are four of the most widely used agile testing approaches today. While no one technique is ideal for every product, these frameworks serve as good beginning points for developing a customized approach:

- **Acceptance test-driven development**

ATDD is a subtype of TDD (test driven development). It embraces Agile testing's collaborative nature by bringing customers, developers, and testers together to produce acceptance tests from the customer's perspective. After these tests are written, the associated functionality is built. With this workflow approach, it's simple to develop test cases. This provides developers with direct insight into what consumers want and how the product will be utilized, eliminating uncertainty and lowering the likelihood of making huge mistakes.

- **Behavior-driven development**

BDD is based on test-driven development and acceptance test-driven development and complements them. By using their structure, they enable the discovery of desirable business objectives and the execution of tests based on those desired outcomes.

BDD consists of five stages:

- Distinguish the conduct
- Create a step description.
- Attempt and fail
- Create code to execute the step.
- Run and overtake

Exploratory Testing in Agile

Exploratory testing is a cyclical process that begins with test creation and ends with analysis and learning. The tests themselves are not written; rather, they are developed by Agile testers as they explore the product, pushing the tester to fully use their particular skill set.

Exploratory testing is the closest testers will go to engaging with a product in the manner in which it will appear 'in the wild.' It's an excellent approach to rapidly determine if you have functional software, and it enables testers to detect flaws that would be missed by conventional testing methods.

- **Session-Based Testing**

Session-based testing, as BDD does for ATDD, builds on and refines exploratory testing.

Exploratory testing's greatest strength - the ingenuity of those who do it - may also be its biggest shortcoming. By introducing structure, session-based testing seeks to address this. Prior to initiating a test session, a charter is generated. Second, uninterrupted testing sessions are conducted, with the primary emphasis being on a single charter. After the exam, the whole session is reported on, and the manager is debriefed. The added structure guarantees that all aspects of the product are adequately examined and prevents any one section from developing backlogs.

Agile Testing Quadrants

With these and other testing approaches, determining which sort of test to run, how often to run it, when to run it, and by whom may be challenging. There are several sorts of tests, including acceptance testing, regression testing, and unit testing. Additionally, there is the issue of whether human or automated testing is more appropriate for the product's current version.

Gregory and Crispin coined the term "agile testing quadrants," which serve as a classification system for tests. According to Crispin, the two left-hand quadrants assist teams in determining which code to develop and when to stop. The two right-hand quadrants assist teams in understanding their own code by offering input to the left-hand quadrants.

Q1 - The Automated quadrant comprises tests that are meant to enhance the code for the product being developed; they are run to assist the team in developing a better product.

Q2 - The Automated & Manual quadrant comprises tests that are intended to enhance the business outcomes of the product being developed; they are conducted to assist the team in developing a product that adds value to the company and its consumers.

Q3 - The Manual quadrant comprises tests designed to provide feedback for tests in quadrants 1 and 2, as well as to evaluate the product and user experience in order to achieve business results.

Q4 - The Tools quadrant includes tests that use technology to guarantee that the code satisfies all non-functional criteria, such as security and compatibility.

- **Advantages of Agile Testing**

Adopting Agile testing has three straightforward benefits: a happy workforce, a higher-quality product, and quicker delivery. However, that trifecta makes the effort required to establish a good Agile testing system worthwhile.

- **A product of superior quality**

Agile helps testers to identify faults more quickly throughout the development phase.

Continuous feedback' is one of the Agile concepts. The philosophy of concurrent testing and development enables defects to be eradicated quickly after they are generated. Each iteration of the product is rigorously tested and debugged throughout development, rather than after completion. Testing also incorporates every member of the development team, maximizing the abilities of both developers and testers in the quest of a flawless product.

Additionally, testers get an intimate understanding of the product as a result of continual feedback mixed with early and frequent testing. They may combine that expertise with consumer feedback to assist developers in creating a greater product, depending on the testing process employed.

- **Prompt delivery**

The earliest phases of development and final market release are separated by months, if not years, with waterfall testing. As a consequence, by the time a product reaches clients, its features or perhaps the whole product may be utterly useless.

Agile testing methodologies shorten the development cycle while providing continuous consumer input, ensuring that the product adapts to the market throughout development and reaches customers as quickly as feasible.

- **A more contented team**

The last criteria on the Agile testing checklist is, without a doubt, fun. Agile testing involves strong collaboration amongst all team members, resulting in a more positive, fun, and productive work environment. Developers, testers, and consumers collaborate to develop the finest possible product with the most possible value.

Crispin and Gregory put it succinctly:

A team guided by Agile ideals and principles will have a greater team morale and higher velocity than a team of brilliant people that functions badly."

- **Possible disadvantages of Agile methodology**

However, no system is without flaws. When Agile testing is not correctly executed, it may erode team structure and product development, thereby impeding the delivery of a viable product. Even when implemented correctly, all Agile techniques have flaws. For instance, exploratory testing may lack the framework required to thoroughly evaluate a product; ATDD considers user input but not business results.

Agile testing's focus on people may potentially be its undoing. Agile testers are deemed ineffective if they are isolated from the team with whom they must work closely. If a single talented Agile tester departs, it might be a significant setback for the product's development.

Finally, since every member of the team is responsible for testing, the muddled structure may result in misunderstanding and disagreement. Scrum attempts to sidestep this by utilizing ‘scrum masters,' however this risks reverting to a more conventional manner rather than being really Agile.

- **Agile Testing Strategy**

Each of these hazards may be conquered with determination, resulting in the three significant rewards. The first step toward effective Agile testing is recognizing when it is not appropriate to employ Agile testing. Adopting Agile testing blindly might result in a product that is unstable and prone to crashes.

Following are some tips for situations in which Agile may not be the optimal method of testing:

- When the project's scope is unambiguous and very unlikely to alter
- When a project is overseen by a single product owner or stakeholder and has few criteria
- When the members of your team lack the depth and breadth of knowledge required to do Agile testing
- When the client is adamant about testing in the classic waterfall fashion

After determining that Agile testing will help your team, your product, and your consumers, you should devote as much effort as required to selecting the appropriate methodology and developing a process for testing using the four-quadrant model.

To minimize the risk of testers being excluded, testers should work in close physical proximity to developers. They should meet with them often to learn about their current projects and to allow them to examine the tests that have been produced. Iterative approaches here, as well as throughout the testing phase, may aid in early team connection and cooperation.

By offering relevant input based on interactions with developers and consumers, testers may create opportunities for themselves. In summary, they must become necessary to developers in order to do their job properly.

The most effective way to assure the success of Agile testing for a product is to employ individuals who exhibit the basic traits of an Agile tester and to foster an organizational culture of self-organization and independent thinking across the organization.

This atmosphere will automatically result in ‘stable infrastructure' without compromising speed, which will result in happy employees providing a better, more value product - quicker - to a delighted client.

Python Programing

Python is an object-oriented, high-level programming language with dynamic semantics that is interpreted. Its high-level built-in data structures, together with dynamic typing and dynamic binding, make it particularly well-suited for Rapid Application Development, as well as for usage as a scripting or glue language for connecting existing components. Python's straightforward, easy-to-learn syntax places a premium on readability, which lowers the cost of program maintenance. Python allows modules and packages, which promotes the modularity and reuse of code in programs. Python's interpreter and substantial standard library are available free of charge in source or binary form for all major platforms and are freely distributable.

Frequently, programmers fall in love with Python due to the productivity boost it delivers. Due to the absence of a compilation phase, the edit-test-debug cycle is lightning quick. Python scripts are simple to debug: a bug or improper input will never result in a segmentation fault. Rather than that, when the interpreter detects a mistake, it throws an exception. The interpreter produces a stack trace if the program does not catch the exception. A source level debugger enables you to examine local and global variables, evaluate arbitrary expressions, create breakpoints, and walk through the code one line at a time. The debugger is developed in Python, demonstrating Python's introspective capabilities. On the other hand, adding a few print statements to the source code is often the fastest method to debug a program: the rapid edit-test-debug cycle makes this basic technique quite successful.

Python is a general-purpose high-level programming language that may be used to solve a wide variety of issues.

The language includes a large standard library that covers topics such as string processing (regular expressions, Unicode, calculating file differences), internet protocols (HTTP, FTP, SMTP, XML-RPC, POP, IMAP, and CGI programming), software engineering (unit testing, logging, profiling, and parsing Python code), and operating system interfaces (system calls, filesystems, and TCP/IP sockets). Take a look at The Python Standard Library's table of contents to get a sense of what's included. Additionally, a large number of third-party extensions are available. Consult the Python Package Index to locate packages that may be of interest.

Python versions are denoted by the letters A.B.C. or A.B. A is the major version number; it is increased only when there are really significant modifications to the language. B denotes the minor version number, which is increased for less seismic changes. The micro-level is denoted by C, which is increased with each bugfix release. PEP 6 contains further information on bugfix releases.

Not all versions include bug fixes. A series of development releases, labelled as alpha, beta, or release candidate, are created in the run-up to a new main release. Alphas are early versions with unfinished interfaces; it is fairly uncommon for an interface to alter between two alpha releases. Betas are more stable, keeping current interfaces while allowing for the addition of new modules, whereas release candidates are frozen, with no modifications made except to address major defects.

There is an extra suffix for alpha, beta, and release candidate versions. An alpha version's suffix is "aN" for some small number N, a beta version's suffix is "bN" for some small number N, and

a release candidate version's suffix is "rcN" for some small number N. In other words, all 2.0aN versions predate 2.0bN versions, which in turn precede 2.0rcN versions, which in turn precede 2.0.

Additionally, you may see version numbers with a "+" suffix, for example, "2.2+". These are unreleased versions that were generated straight from the CPython development repository. In practice, upon the completion of a minor release, the version number is increased to the next minor version, which becomes the "a0" version, e.g. "2.4a0".

3. CONCLUSION

Project management information systems, which are often obtained as software packages by enterprises, are designed to assist managers in planning, coordinating, and controlling projects. However, the extent to which project management information systems contribute to the success or performance of a project is uncertain. The goal of this research is to empirically analyze the quality of project management information systems already in use in businesses and to investigate their influence on project managers and project performance using a success model for project management information systems.

This study examines five constructs: the quality of Project management information systems, the quality of Project management information systems information output, the use of Project management information systems, the individual impacts of Project management information systems, and the project success impacts of Project management information systems.

However, security is the primary constraint on this system. The ability to share information in a Web-based process management system necessitates the implementation of security measures. The problem of trust is critical when putting up Web-based process management systems, some customers will be entirely trustworthy, while others will need constant monitoring. There is without a doubt a need to urge people to see this technology as an advantage rather than a danger.

The system information of project management is critical to the success of a project and should continue to be the subject of project management study.

The purpose of this research was to ascertain the real-world effects of information technology-based (Web)-based project management information systems on project performance. More precisely, one purpose was to discover the primary drivers of project management information systems and the degree to which these systems aid project managers in terms of enhanced efficiency, productivity, and efficiency. Another purpose was to get a better understanding of how these systems contribute to project success.

Following earlier research findings that project management information system success models should be evaluated and challenged, the results of this study demonstrate that project managers benefit from the employment of a project management information system. Improvements in project planning, scheduling, monitoring, and control were noticed here, as well as improvements in the efficacy and efficiency of management responsibilities. Additionally, productivity gains were reported in terms of more timely decision-making. The benefits of using a project management information system are not confined to individual performance; they also extend to project performance. These methods were discovered to have a direct effect on project success, since they aid in budget management, reaching project

deadlines, and adhering to technical standards. As a result, one may infer that PMIS contribute significantly to project success and should remain the subject of project management study.

4. BIBLIOGRAPHY

[Online] https://www.britannica.com/technology/telecommunication.

** <img src="/cimages/videopreview/videopreview-full/rpkdwr8rgz.jpg" width="400" height="225" style="width: 400px; height: 225px;"> . [Online]**

http://en.wikipedia.org/wiki/A_Guide_to_the_Project_Management_Body_of_Knowledge#Contents. [Online]

http://gates.comm.virginia.edu/rrn2n/Feasibility.htm. [Online]

http://www.arma.org/rim/101/articles.cfm?key=rim101rim. [Online]

http://www.freetutes.com/systemanalysis/sa3-%20%20%20%20%20%20technical-economic-operational-legal.html. [Online]

http://www.freetutes.com/systemanalysis/sa3-%20%20%20%20%20%20technical-economic-operational-legal.html. [Online]

http://www.maxwideman.com/guests/ministry/components.htm. [Online]

http://www.mgt.ncu.edu.tw/~ylchen/sasd-%20%20slide/chap03.ppt. [Online]

http://www.project-management-knowledge.com/definitions/p/project-management-information-system-pmis/. [Online]

https://ecomputernotes.com/mis/information-and-system-concepts/business-value-of-information. [Online]

https://ecomputernotes.com/mis/what-is-mis/managementinformationsystems. [Online]

https://economictimes.indiatimes.com/definition/hacking. [Online]

https://ergo-plus.com/ergonomic-design-checklists/. [Online]

https://ergo-plus.com/workplace-ergonomics/. [Online]

https://project-management-knowledge.com/de/definitionen/p/projektmanagement-information-system-pmis/. [Online]

https://project-management-knowledge.com/definitions/p/project-management-body-of-knowledge-pmbok/. [Online]

https://project-management-knowledge.com/project-management-process-groups/. [Online]

https://searchapparchitecture.techtarget.com/feature/Enterprise-architect-role-is-more-about-business-than-ever?_gl=1*1u2ronu*_ga*Mzg3MzMwMTczLjE2NDExOTQyMzM.*_ga_TQKE4GS5P9*MTY0MTIwNDk3MS4yLjEuMTY0MTIwNTIxMy4w&_ga=2.214718740.2019757570.1641194233-387330. [Online]

https://searchapparchitecture.techtarget.com/tip/Enterprise-architecture-model-helps-to-maximize-mobile-empowerment?_gl=1*2csgf*_ga*Mzg3MzMwMTczLjE2NDExOTQyMzM.*_ga_TQKE4GS5P9*MTY0MTIwNDk3MS4yLjEuMTY0MTIwNTIxMy4w&_ga=2.211415062.2019757570.1641194233-3873. [Online]

https://searchcio.techtarget.com/definition/business-process. [Online]

https://us.anteagroup.com/projects/ergonomics-assessment-philippines. [Online]

https://www.aipm.com.au/blog/5-must-know-risk-management-strategies. [Online]

https://www.aipm.com.au/blog/articles/risk-control. [Online]

https://www.amazon.co.uk/Agile-Testing-Practical-Addison-Wesley-Signature/dp/0321534468. [Online]

https://www.britannica.com/technology/cloud-computing. [Online]

https://www.britannica.com/technology/digital-computer. [Online]

https://www.britannica.com/technology/Internet-service-provider. [Online]

https://www.britannica.com/technology/software-as-a-service. [Online]

https://www.britannica.com/technology/telecommunications-network. [Online]

https://www.britannica.com/topic/identity-theft. [Online]

https://www.britannica.com/topic/open-source. [Online]

https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwjFrKmKlJv1AhVSkGgJHbqJCuwYABAAGgJ3Zg&ae=2&ohost=www.google.com&cid=CAESQOD2mQ-A2BI3b-_-pJSGqPzhPz61pMq66kY4m5J-9o4ZzaxOAlu4VLIYhLw92TEfciCm5XWjDnve1wBtbdl-DuQ&sig=AOD64_1Lieo5XmKXIaSIO7gHu4n43BrH. [Online]

https://www.mbaknol.com/management-information-systems/cost-benefit-analysis-in-information-systems-development/. [Online]

https://www.mbaknol.com/management-information-systems/enterprise-resource-planning-erp-definition/. [Online]

https://www.paloaltonetworks.com/cyberpedia/what-is-malware-protection. [Online]

https://www.precisely.com/solution/data-quality-solutions. [Online]

https://www.projectmanagement.com/articles/147259/SLAs-for-Dummies. [Online]

https://www.thebidlab.com/learning-center/what-is-the-request-for-proposal-process/. [Online]

https://youtu.be/MHyXOsHGinE. [Online]