FOUNDATIONAL INFORMATION TECHNOLOGY GENERAL CONTROL

AKINGBADE AKINFENWA

TABLE OF CONTENTS

INTRODUCTION

An IT control is a procedure or policy that provides a reasonable assurance that the information technology (IT) used by an organization operates as intended, that data is reliable and that the organization is in compliance with applicable laws and regulations. IT Controls can be categorized as either general controls (ITGC) or application controls (ITAC).

An IT general control should demonstrate that the organization has a procedure or policy in place for technology that affects the management of fundamental organizational processes such as risk management, change management, disaster recovery and security. IT application controls, which are actions that a software application does automatically, should demonstrate that software applications used for specific business processes (such as payroll) are properly maintained, are only used with proper authorization, are monitored and are creating audit trails.

ITGCs govern the technology that other parts of the enterprise use to do their jobs. For example, a large business might have applications that support finance, procurement, inventory, research, sales & marketing, and human resources. All of those teams use their own IT applications, and depend on those applications operating in certain ways. At most large businesses, each of those applications will be part of one enterprise resource planning (ERP) system, such as Oracle or SAP. ITGCs work out of sight from most employees, but they're incredibly important for security, compliance, and operational success. Compliance officers, therefore, need a keen appreciation of how ITGCs support a strong compliance program. They need tools to assess the performance of ITGCs and to mitigate any weaknesses that might endanger your ERP system or other technology your business units use. And as always, compliance officers also need to understand how their internal control actions will affect the people within your organization, or else your work won't go very far.

The scope of the ITGC commonly includes access control to physical facilities, computing infrastructure, applications and data; security and compliance aspects of the system development life cycle, change management controls, backup and recovery, and operational controls over computing systems.

There are several accepted standards for ITGC audits, including the Control Objectives for Information Technologies framework (COBIT, developed by ISACA), SP 800-34 Contingency Planning Guide for Information Technology Systems (by NIST), and the Information Technology Infrastructure Library (ITIL) framework.

ITGC audits can involve monitoring the ITGC on an ongoing basis, identifying issues and responding to them, as well as proactive internal audits of ITGC components, and adjustment of policies and controls according to audit results.

The one overriding fact, however, is that the modern business enterprise will only rely more on technology as we move into the future. The stronger your grasp over the ITGCs that support your business, the better your business will be able to compete in our highly regulated, highly risky world.

IMPORTANCE OF IT GENERAL CONTROL

Information technology (IT) serves as a critical enabler that enables a business to perform its core business activities effectively and efficiently. I can't think of a business that is not enabled by IT to carry out its business activities. The dependence on IT has brought about its own risks and challenges. Think about it, cloud technology creates the ability to operate a business completely on the internet.

IT general controls are measures and safeguards put in place to protect the integrity of data processed and stored by information systems. Information systems are used to process a company's financial records. The general ledger, income statement and balance sheet all rely on data and transactions processed through IT systems. It is therefore imperative to ensure that measures are put in place to safeguard the integrity of data processed and stored on IT systems.

One of the key IT control domain for consideration is Access control. Access controls address the risk that users might have inappropriate access or access rights beyond those necessary to perform their specified job duties. This could in turn result in improper segregation of duties.

Examples of controls that can mitigate this risk are requesting management approval prior to granting system access and only granting the access rights that the user will need to perform their specified job duties, revoking access assigned to terminated users in a timely manner, updating access rights assigned to transferred users and performing a periodic user access review to re-certify the appropriateness of the access assigned to users. Authentication and privileged access management are some key controls to implement. NIST has defined good best practices in terms of password management and privileged access should be restricted to System Administrators.

Change Management is another key domain to consider. Change Management poses a risk that unauthorized changes could be made to application systems and system logic and this could result in the erroneous processing of data. Key controls to consider is to ensure that changes are approved by management and appropriately tested before they are implemented on the production environment. The development and production environments should be segregated and developers should not be granted access to deploy changes to the production environments.

Management should ensure that controls are appropriately documented and performed in a timely manner. This ensures that the mapped risks are properly addressed. Another key consideration is to ensure that controls are performed consistently as the performance of controls is not a once-off activity.

TYPES OF INFORMATION TECHNOLOGY GENERAL CONTROL

INFORMATION SECURITY

The term “information security” refers to all practices, processes, and tools used to protect a company’s information assets and systems. It is critical to implement standardized forms of information security, to ensure that information remains secure and protected. This typically involves processes that prevent data loss of all types, including data theft, exfiltration, and corruption, and accidental modification, as well as processes that protect against known cyber threats and techniques, and strategies for dealing with unknown and zero day attacks.

PHYSICAL AND ENVIRONMENTAL SECURITY

Data centres must be protected from unplanned environmental events and unauthorized access that could potentially compromise normal operations. Access to data centres is usually controlled by keypad access, biometric access technologies, or proximity cards. These techniques enable single-factor and or multi-factor authentication. Organizations often add more layers of protection against unauthorized access. For example, closed-circuit video cameras are deployed as part of the overall physical security monitoring system. Additionally, data centres need technologies that control the temperature within the facility, to ensure it is suitable for human staff as well as machinery. These systems often trigger alarms when the temperature changes or an emergency occurs.

INCIDENT MANAGEMENT

T infrastructure is constantly targeted by attackers. Organizations should establish continuous incident management practices and tooling that enables them to constantly monitor the environment, receive alerts on anomalous events, and rapidly respond to threats. However, since systems tend to send many false positive alerts, it is critical to set up automated processes that prioritize and validate incidents before notifying human teams.

LOGICAL SECURITY

All company employees require access to digital assets, but they do not require the same type of privileges. When providing stakeholders with access to company assets, administrators should apply the least privileges principle, and supply exactly the level of access needed to perform the responsibilities of a certain role. To establish access levels, IT can work with HR to determine what assets each employee requires to perform their job. Additionally, organizations should protect credentials using several mechanisms, such as encryption, strong passwords, password rotation, multi-factor authentication, and biometric authentication.

BACK-UP AND RECOVERY

To maintain normal operations, organizations must establish backup and recovery strategies and practices. It is critical to protect resources, including data, business processes, databases, virtual machines (VMs), and applications. There is a wide range of backup and recovery options available, including cloud-based services, on-premises systems, and hybrid solutions.

DIFFERENCE BETWEEN INFORMATION TECHNOLOGY GENERAL CONTROL AND APPLICATION CONTROL

General controls include any controls related to the security, use, or design of computer programs. Similarly, it consists of any methods that help secure data or information within these systems. General controls apply throughout the organization. Any department or area within a business that uses information technology will include general controls as well. General controls apply to any computerized application. Usually, these include a mixture of manual procedures and system software. Using these, companies can create an overall control environment. General controls are crucial in ensuring the effective operation of any programmed procedures within a company. These may also include physical controls that protect computer hardware. Example of general controls includes software controls, physical hardware controls, data security controls, computer operations controls, etc. For example, a company may ensure that the hardware is only physically accessible to authorized personnel. It is an example of physical hardware controls, which are a part of general controls.

APPLICATION CONTROL

Application controls, as the name specifies, include safeguards related to specific computer applications. For companies, these may consist of both automated and manual procedures. The software ensures that only authorized data gets processed by the application. Application controls relate to the accuracy and completeness of the data that enters the technology systems. Application controls use several methods to ensure the data entered into the systems is complete and accurate. For some systems, these controls may be more crucial than others. For example, application controls may exist to check whether the data entered into a system is reasonable and meets the required format. There are three primary categorizations of application controls, including input, processing, and output controls.

For example, a company may require employees to fill forms for every order. Applications controls include checking whether the entered information meets the required format. For example, ensuring that employees can only put numbers for the units required. Similarly, it may include examining whether an order already exists with similar information to identify duplication.

The term control represents any policies, procedures, methods, or processes that help in managing risks. These processes help companies protect their assets and ensure the accuracy and reliability of their financial information. When it comes to controls related to information technology, there are two categories. These include general controls and application controls. Both of these are different in several key regards.

MAJOR DIFFERENCES

There are several key differences between general and application controls. For companies that employ information technology systems, these controls are critical. It is crucial to have both of these controls. However, it is still necessary to understand how they differ from each other. Some of the aspects in which general and application controls vary are as below.

IT General Controls are relevant for all areas of the organization, including IT infrastructure and support services. Examples of common controls are accounting controls, administrative controls, security policies, operational controls, procedures for documenting sensitive processes, and physical security for IT resources.

While, Application Controls are responsible for protecting the transactions and data associated with a specific software application. They are unique to each application, and focus on input, processing and output (IPO) functions. Application controls ensure the completeness and accuracy of records created by the application, the validity of data entered into those records, and the integrity of data throughout the lifecycle.

As mentioned, general controls include software, hardware, and manual procedures. Therefore, these controls may consist of software controls, computer operations controls, data security Control, administrative controls, physical hardware controls, and much more. On the other hand, application controls are more specific. As mentioned above, there are only.

Three types of application controls. These include input, processing, and output controls. Each of these may consist of more kinds, which all fall under application controls.

Also, General controls affect the operations of a company's whole information technology system. Therefore, it has a broader scope when it comes to its usage. On the other hand, application controls only apply to one application. Therefore, application controls have a narrower and defined scope. However, that does not suggest that these controls are futile.

As mentioned, general controls may include all controls related to information technology systems. Therefore, controls over data centre and network operations are an example of general controls. These controls are specific to any information that uses networks. Antivirus or firewall is a typical general control that applies to all information technology systems. On the other hand, application controls are application-specific. Therefore, input controls are a prime example of application controls. With these controls, it is possible to validate any information that enters the systems. This way, companies can ensure only valid data gets into their systems control to make sure every employee gets paid once using the payroll software is application control.

Controls are a crucial part of any company. When it comes to information technology systems, companies have two options. These include general and application controls. Both of them are different from each other in several regards. Similarly, the differences include their definitions, scopes, types, and examples. Both of the above controls are crucial in ensuring the effectiveness and reliability of a company's information technology systems.

Companies rely on information technology in several fields. However, it is also vulnerable to various security issues and breaches. Therefore, companies need to have measures or safeguard to protect their systems from such manipulation. Usually, they need to ensure that their systems perform according to both internal and prevalent standards. For that, they need to employ various controls.

HOW TO AUDIT IT GENERAL CONTROL

When auditing IT General Controls, you can audit them as separate control audits or you can incorporate some IT General Controls work into IT functional audits. Integrated audits can build on work that has already been done in relation to general computer controls. However we are not just relying on auditors. These are controlled environments so there are other business assurance processes such as continuous monitoring, vendor audits, and so on, which will also provide assurance. When you are thinking about getting assurance over IT General Controls, in addition to audits you should consider the other mechanisms we use to get assurance – such as taking part or observe at steering committees, and also ensuring you have access to metrics and dash boards that will give you a view as to what is currently happening in the IT environment. This can inform your view on the annual planning process and what they may need to change.

During audit planning, auditors must learn about the types of controls that exist within their client's IT environment. Then they may test those controls to determine whether they are reliable as a means of reducing risk. Tests of controls are sometimes referred to as “compliance tests,” because they are designed to determine whether the controls are functioning in compliance with management's intentions. The following section discusses how these controls are evaluated.

INFORMATION TECHNOLOGY CONTROL TESTING

Organizations have robust information technology systems to collect, store and analyse data. IT controls dictate how users interact with these systems, whether they encourage certain actions or prevent manipulation of information. Conducting IT control testing can help an organization secure its information and optimize employee productivity. IT control testing is the evaluation of an organization's information technology system to ensure effective implementation. Auditors determine the accuracy of the system's data and whether the organization complies with the appropriate regulations.

STEP-BY-STEP GUIDE TO CONTROL TESTING

- **Choose an auditing team:** Choosing an auditing method helps an organization apply consistency to IT control testing. Using the same steps and metrics to measure performance allows auditors to adhere to established quality standards and make accurate comparisons with past systems. A company can choose the appropriate auditing method by researching options in its industry and ensuring the goals align with its priorities. For instance, a company that values security might opt for an auditing method that has successfully helped similar companies restrict unauthorized user access.

- **Identify IT controls:** General IT controls are those that concern access to the overall information technology environment. These controls look similar across companies, but it's important for an auditor to identify those that are relevant to their organization. Examples of general IT controls include security badges and user credentials that grant access to company devices. Auditors also identify backup mechanisms that secure the organization's data, such as how often backups occur and whether the servers are digital or physical. Additionally, general IT controls can be physical barriers like locked rooms that store computers or devices bolted to desks. These restrictions are seemingly simple but essential to the safe implementation of IT systems.

- **Optimize general IT controls:** After identifying the organization's general IT controls, an auditor can conduct testing to optimize them. For instance, they might recognize the limitations of current policies and require users to make their passwords more complex. Common policies include requiring a certain number of unique characters and restricting the user from including their surname in their password. Another optimization technique an auditor can use is the implementation of secondary authorization, which requires users to provide proof of identity beyond their login credentials. Auditors may also choose to monitor login attempts to more quickly restrict unauthorized users from obtaining system access.

- **Identify application IT control:** Application IT controls differ from general IT controls in that they depend on the organization's software. Examples include user credentials specific to applications and user permissions for specific roles. Auditors often use audit trails to analyse all the actions users perform within an application and determine whether the software fulfils its intended purpose. For instance, consider an application that processes accounts receivable. When a clerk logs in to this app, they may only be able to post journal entries. Managers and financial controllers likely have more advanced responsibilities, such as approving entries.

- **Optimize application IT control:** Like with general IT controls, it's essential to optimize application IT controls. Starting by identifying them can help auditors better understand the organization's separation of duties and reorganize them if necessary. For instance, an app that processes accounts receivable may be more efficient if it grants clerks the ability to request adjusting entries. These additional permissions increase the clerks' independence, allowing managers and financial controllers to dedicate more focus to other duties.

Optimization of application IT controls may also involve the revision of internal requirements. For instance, an auditor might request mandatory information when employees submit forms or designate payment terms to clearly convey expectations to customers.

- **Conduct internal and external testing:** Many auditors focus on IT control testing from within the organization. They evaluate how employees access their applications and ensure users have the appropriate permissions to perform their duties. While this internal testing is essential, it's also important to evaluate the IT system's reliability in the face of external threats. Auditors can mimic breach attempts from third-party organizations or even hire a company that specializes in this type of service.
- **Establish a response protocol:** Regular IT control testing helps an organization optimize its information technology, but response protocols can help mitigate issues before they result in bigger problems. For instance, an organization might implement a system for managing failed login attempts. The first few attempts can be forgiving, as they account for employee forgetfulness or mistakes. When a user repeatedly enters invalid credentials, it might be appropriate for the company to alert management and lock the system to prevent unauthorized access.
- **Recognise testing limitation:** Even if an organization uses advanced testing equipment and conducts audits from internal and external perspectives, it's important to recognize the limits of IT control testing. Limitations include mistakes when collecting metrics and the sheer number of possible scenarios. By recognizing the limits, organizations can remain flexible when responding to failed IT controls and protect the organization's infrastructure.

INFORMATION TECHNOLOGY

Information technology (IT) is the use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data. Typically, IT is used in the context of business operations, as opposed to technology used for personal or entertainment purposes. The commercial use of IT encompasses both computer technology and telecommunications.

Information technology is a process that uses a combination of means and methods of data collection, processing and transmission to obtain new quality information about the state of an object, process or phenomenon. The purpose of information technology is the production of information for analysis by people and decision making on the basis of it to perform an action.

The introduction of a personal computer in the field of information and the application of telecommunication media have determined a new stage in the development of information technology. Modern IT is information technology with a "friendly" user interface using personal computers and telecommunication facilities. The new information technology is based on the following basic principles:

- Interactive (dialogue) mode of working with a computer.
- Integration with other software products.
- Flexibility in the process of changing data and task definitions.

CHARACTERISTICS OF INFORMATION TECHNOLOGIES

- User operation in data manipulation mode (no programming). The user must not know and remember, but must see (output devices) and act (input devices).
- Cross information support at all stages of information transmission on the support of an integrated database, which provides a unique way to enter, search, display, update and protect information.
- Paperless document processing during which only the final version of the paper document is recorded, intermediate versions and the necessary data recorded on the media are delivered to the user via the PC display screen.
- Interactive (dialogue) task solution mode with a wide range of possibilities for the user.
- Collective production of a document based on a group of computers linked by means of communication.
- Adaptive processing of the form and modes of information presentation in the problem solving process.

TYPES OF INFORMATION TECHNOLOGIES

The main type of information technology include the following:

Information technology for data processing- This is designed to solve well-structured problems, the solution algorithms for which are well known, and for which all the necessary input data exists. This technology is applied to the performance level of low-skilled staff in order to automate some routine and constantly repeated operations of administrative work.

Management information technology- This is intended for the information service of all employees of companies, related to the acceptance of administrative decisions. In this case, the information is usually presented in the form of ordinary or special management reports and contains information about the past, present and possible future of the company.

Automated office information technology- This is designed to complement the company's existing staff communication system. Office automation assumes the organization and support of communication processes both within the company, and with the external environment on the basis of computer networks and other modern means of transferring and working with information.

Decision support information technology- This is designed to develop a management decision that is produced as the result of an iterative process involving a decision support system (a computer link and the object of management) and a person (the management link, which sets input data and evaluates the output).

The information technology of expert systems- This is based on the use of artificial intelligence. Expert systems allow managers to receive expert advice on any problem for which knowledge has been accumulated in these systems.

INFORMATION TECHNOLOGY STAFF

Most IT staff have different responsibilities within the team that break into several key areas including:

- **Administration**: Administrators handle the day-to-day deployment, operation and monitoring of an IT environment, including systems, networks and applications. Admins often perform a range of other duties such as software upgrades, user training, software license management, procurement, security, data management and observing adherence to business process and compliance requirements.
- **Support**: Help desk staff specialize in answering questions, gathering information and directing troubleshooting efforts for hardware and software. IT support often includes IT asset and change management, helping admins with procurement, handling backup and recovery of data and applications, monitoring and analysing logs and other performance monitoring tools and following established support workflows and processes.
- **Applications:** Businesses rely on software to perform work. Some applications are procured and deployed from third parties, such as email server applications. But many organizations retain a staff of skilled developers that create the applications and interfaces -- such as APIs -- needed to deliver critical business capabilities and services. Applications might be coded in a wide array of popular languages and integrated with other applications to create smooth and seamless interactions between different applications. Developers might also be tasked with creating interactive business websites and building mobile applications. The trend toward agile or continuous development paradigms require developers to be increasingly involved with IT operations, such as deploying and monitoring applications.
- **Compliance**: Businesses are obligated to observe varied government- and industry-driven regulatory requirements. IT staff play a major role in securing and monitoring access to business data and applications to ensure that such resources are used according to established business governance policy that meets regulatory requirements. Such staff are deeply involved with security tasks and routinely interact with legal and business teams to prevent, detect, investigate and report possible breaches.

INFORMATION TECHNOLOGY CONTROLS

In business and accounting, information technology controls (or IT controls) are specific activities performed by people or systems designed to ensure that business objectives are met. They are a subset of a company's internal control. IT control objectives relate to the confidentiality, integrity and availability of data and the general management of the IT function of the business enterprise. IT controls are often described in two categories: IT general controls (ITGC) and IT application controls. ITGC includes controls over the technology of the Information Environment (IT), computer operations, program and data access, program development and program changes. IT application controls refer to transaction processing controls, sometimes called "input-output processing" controls. Information technology controls have been given increased prominence in listed companies in the United States by the Sarbanes-Oxley Act. The COBIT Framework (Control Objectives for Information Technology) is a widely used framework promulgated by the IT Governance Institute, which defines a variety of ITGC and recommended application control objectives and assessment approaches. Organizations' IT departments are typically headed by a chief information officer. (CIO), which is responsible for ensuring that effective information technology controls are used.

INFORMATION TECHNOLOGY GENERAL CONTROL

Whether employees know it or not, IT has a tremendous effect on their everyday working lives. IT is essentially the lifeblood of a company, ensuring employees' laptops work, procuring and installing the applications employees need to do their jobs, and instituting and upholding rules to help the company stay compliant. But how does the IT team accomplish those tasks in a standardized, secure way? The answer lies in IT General Controls. IT General Controls, or ITGCs, are a set of directives that govern how an organization's systems operate. Yet, knowing what ITGCs are and how they work in practice isn't always straightforward.

Information Technology General Controls (ITGCs) dictate how technology is used in an organization. ITGCs help prevent breaches, data theft, and operational disruptions.

ITGCs influence everything from user account creation, to password management, to application development. They prescribe how new software is set up, who the admins are, how the system is tested and implemented, and when security and software updates should take place.

Because ITGCs specify certain security protocols, they also impact vendor procurement. Applications that cannot uphold ITGCs put companies' data at risk, so investors and auditing firms may review ITGCs to ensure companies achieve and maintain regulatory compliance.

One important thing to note is that Information Technology General Controls are not the same as application controls. ITGCs govern the use of all systems within a company, from ERPs to servers, directory platforms, and project management tools. Application controls restrict what users can do within one particular platform, and typically these permissions are configured directly within that application and pertain to specific features or use cases.

ITGC represents the foundation of the IT control structure. They help ensure the reliability of the data generated by IT systems and support the claim that the systems are working as intended and that the output is reliable. ITGC generally includes the following types of controls:

- Control environment, or those controls designed to shape corporate culture or the "tone at the top."
- Change Management Procedures – Controls designed to ensure that changes meet business requirements and are authorized.

- Document / Source Code Version Control Procedures – Controls designed to protect the integrity of program code
- Software Development Lifecycle Standards – Controls designed to ensure that IT projects are managed effectively.
- Logical Access Policies, Standards, and Processes – Controls designed to manage access based on business need.
- Incident Management Policies and Procedures – Controls designed to address operational processing errors.
- Problem Management Policies and Procedures – Controls designed to identify and address the root cause of incidents.
- Technical Support Policies and Procedures – Policies to help users perform more efficiently and report problems.
- Hardware / software configuration, installation, testing, management standards, policies and procedures.
- Backup / recovery procedures and disaster recovery, to enable continued processing despite adverse conditions.
- Physical Security – Controls to ensure the physical security of information technology from people and from environmental hazards.
- IT application controls.

GENERAL INFORMATION TECHNOLOGY ADMINISTRATION

Both for-profit and non-profit organizations must remain at the forefront in their different fields of action, and in order to do this they must have the latest in information systems that can meet the needs of both their internal environment and their external environment. The redesign of an organization based on the acquisition of new information technologies that give way to a new information system is not an easy task, many aspects of the organization must be taken into account (human, economic and operational resources) and must be follow a previously defined process in order to be reborn and make this redesign successful. As mentioned at the beginning, the objective of the Administration of information technologies is the development of information systems that allow solving administration problems. In this sense, there are informational tools that strive to provide an infrastructure to meet the management needs of organizations.

A part of the administration in information systems used in many companies is the Management Information System (GIS), which is made up of the collaborative interaction between people, technologies and procedures, which together are called information systems. Its main objective is to solve business problems that arise every day. The GIS or MIS (also called by its acronym in English: Management Information System) differ from common information systems when analysing the information they use different systems to carry out the operational activities of the organization. In general, a GIS is an integrated user-machine system whose purpose is to provide information that supports operations, administration and decision-making functions in a company, for which it takes as its main tools computer equipment with specialized software, procedures, manuals and models for analysis, in turn, these tools go hand in hand with planning, control and decision making thanks to the systems.

Part of what an organisational administration get to have in mind is to:

- Relate ICT to strategic business planning.
- Integrate and align ICT with business objectives.
- Incorporate and retain the right set of resources and skills.
- Implement continuous improvement.
- Measure the effectiveness and efficiency of the ICT organization.
- Demonstrate the business value of ICT.
- Improve the successful delivery of projects.
- Procurement intelligently (outsourcing, insourcing).
- Maintain the constant change of business and ICT.

Most ITGCs fall under the “general IT” umbrella. General IT controls may refer to how IT systems are managed, who oversees those systems, where the IT roadmap is going, how and when to conduct risk assessments, and what best practices IT projects should follow.

ITGCs in this group may also refer to overall security measures like email filtering, firewalls, antivirus software, and routine pen testing. In this age of remote work, general IT administration may apply to corporate-owned device (COD) and bring your own device (BYOD) policies as well. An IT team is made up of IT people, and each team is different, depending on the culture and needs of the company they work for, the experience and skills of its members, and the types of systems they must deal with. . In that sense, some IT teams are generalists, working with a wide range of systems and services, while others are specialists, focusing on specific technologies (such as networks or web services) or on a specific type of system (sales support, manufacturing, logistics, etc.). On the other hand, some IT teams only work with technology, while others may include data specialists or analysts with deep business process experience.

The administration makes use of different equipment:

Operation Teams: IT operations management can be defined as the process of overseeing the various physical and virtual components of an IT infrastructure. Ensuring their performance, health and availability, and allowing them to work efficiently with other components of your infrastructure. IT operations management (ITOM) also plays an active role in broader IT management models, including IT infrastructure management (ITIM), data centre infrastructure management (DCIM), etc. These teams focus on the operation of technology infrastructure (such as networks, data centres, and web services), monitoring it, and ensuring it is available and functioning normally to support business operations. Often referred to as IT Service Management (ITSM) teams, their primary goal is to keep the technology ecosystem running. Operations teams are permanent and are often supported by sophisticated “command centre” style monitoring infrastructures.

CHALLENGES FACED BY IT OPERATION TEAMS:

- **Device Health And Performance**: If the health and performance of the device is not monitored, device downtime may occur, resulting in huge losses on a day-to-day basis. Today's customers have high expectations; they expect devices to be available 24/7, which means that fixing things when they break doesn't work anymore. Device performance monitoring allows you to proactively identify device outages, which would otherwise lead to a number of issues such as lost productivity, device unresponsiveness, device maintenance costs, etc.

- **Network Jamming**: Most of today's networks require high-speed Internet connections to efficiently operate the large number of devices present on them. If the traffic moving through an infrastructure is unregulated, applications and infrastructure components will be left competing for bandwidth. Unregulated bandwidth and traffic can lead to a number of issues and result in an unpleasant experience for the end user. This includes slow load time, closed connections, load interruptions, unresponsive apps, etc.

- **Poor Configuration Changes**: Configuration management focuses on ensuring consistency in product performance by identifying which components have been changed and why. In a multi-user environment, it is tedious and time consuming to monitor configuration changes and the users who made them. Bad configuration changes can cause deployment failures, lost productivity, and ultimately unexpected outages.

- **Attacks And Cyber Threats**: Cybercrime is on the rise, leading many companies to implement security measures to protect their data. Security threats like DDoS attacks, unauthorized IP addresses accessing your network, and malicious users can cause millions of dollars in losses. They can be economic losses (money, financial information, loss of business/contract), reputational losses (loss of customers, sales, and profits) or legal losses (failure to comply with security regulations, resulting in fines and regulatory penalties).

- **Application Performances**: One of the top priorities for businesses around the world is to have a quality web application, as well as to ensure that it runs smoothly. Some common application performance issues are network connectivity, slow server response time, unimproved bandwidth usage, traffic spikes, etc.

BENEFITS OF IT OPERATION MANAGEMENT TEAM

The benefits of ITOM are so obvious that it's not surprising that IT operations management solutions are so well received. ITOM has been gaining more and more popularity in the last decade. The IT operations management software market is estimated to have achieved a revenue of $9.5 billion in 2018 worldwide. Furthermore, the market as a whole is projected to grow at a compound annual growth rate of 6.9% over the period 2019-2023.

Knowing how ITOM works and why it is important will go a long way toward increasing understanding of its benefits. However, to increase infrastructure performance and gain maximum efficiency in managing IT operations, it is imperative that you choose the right tool to get the job done.

- **Efficiency:** This simply means getting the most out of the resources you have available. IT service management has many components that help organizations maximize their resources. One component is IT asset management, the set of processes used to optimize IT asset lifecycle management and seek the most cost-effective strategies for asset acquisition and disposition.

For organizations working within the ITIL framework, processes for continual service improvement are a critical component of the lifecycle of each service that results in continuous efficiency gains as service functions are optimized over time.

- **Reduces Operational Costs:** IT infrastructure and operations (I&O) spending accounts for total IT spending globally, with I&O staff accounting for approximately half of total IT staffing requirements. As they grow in size and maturity, these IT organizations must hire even more I&O staff, or else risk undue tactical operational processes. The adoption of IT service management can help IT organizations scale their operations more easily without the need to over-hire, thanks to automated features that reduce the manual workload for IT operators.
- **Limited Risk Of Implementing IT Changes:** When changes are poorly planned, tested, and communicated to the business, there is a significant risk that a newly implemented change could cause significant business or service disruption. The ITIL Change Management process describes a system for ensuring that your IT organization can implement new changes to the IT environment in a way that limits or eliminates the risk of harming your business with a change. Formalized roles, processes, and policies work together to create and support a change management process that clearly communicates with customers, approves changes through the appropriate channel based on their potential impact, and identifies potential issues with changes to the organization. Design stage, long before they manifest in deployment.
- **Improves Accountability:** Creating accountability through service standardization is a defining characteristic of IT service management, and one that helps IT organizations improve compliance with IT service delivery policies and procedures. One of the primary goals of ITSM is to standardize service delivery within the enterprise by implementing functions as the IT service, along with documented formal processes for the delivery of each type of IT service. IT service management software also allows IT managers to track the actions of operators and how incidents or service requests are addressed. These features create a high level of visibility into how the IT organization delivers services. IT managers can review incident logs to verify that services are delivered consistently across the enterprise and in accordance with policies and procedures.

Business functions are the activities performed by a company. They can be divided into core functions, which are the activities designed to generate income, and support functions, which serve to support and streamline core functions. IT itself is a critical support function in most businesses, especially those where the IT organization has embraced ITSM to more closely align its activities with the business.

IT service management includes implementing processes to monitor activity on the organization's network and IT infrastructure and detect violations of company security policies.

- **Effectiveness:** How do you measure the overall effectiveness of an IT organization? If you're an IT manager, it's up to you to choose the most important key performance indicators (KPIs) to use to measure your team's performance. You'll also need to track those KPIs over time to determine if your business is improving its effectiveness on those metrics. Organizations that adopt ITSM structures and processes benefit from formalized systems that drive improvement over time when executed effectively. Adopting a structured incident response can decrease mean time to response and mean time to resolution, while focusing on crisis management will help reduce mean time to recovery (MTTR) when a service interruption occurs. ITSM offers a framework for increasing the effectiveness of any aspect of IT service delivery through the process of continuous service improvement.
- **Improves Visibility:** Visibility describes the extent to which managers, executives, and staff in different areas of the business can see what is happening in other areas of the business. Lack of visibility into IT operations is a common problem for organizations that have not yet adopted IT service management. In the ITSM paradigm, there is a need to align IT and business strategy, a process that ensures that the business knows exactly what activities are prioritized in IT operations at any given time.
- **Increases Productivity With Self-service:** Organizations use ITSM best practices to drive self-service productivity improvements. Self-service is a convenient alternative to the traditional help desk model that can help tech-savvy users resolve incidents or fulfil service requests without the help of IT operators, reducing ticket resolution costs and increases customer satisfaction.

Establishing a robust self-service catalogue along with a knowledge base that allows users to solve more problems on their own are critical components of IT service management that drive increased self-service productivity.

- **Better Customer Service:** or enterprise IT organizations, customers are the business users who depend on IT services to support their daily activities. We can highlight two components of IT service management that help improve service delivery and customer experience; The service strategy process requires IT organizations to align their activities with business needs. Ultimately, this means that the IT organization is working on the services that the business wants, leading to a better customer experience. Another important aspect is a formalized ticketing and incident response system. The incident management process improves service by ensuring that the IT organization responds to every incident report or service request that is submitted.
- **Improves Access Communication Channel:** IT organizations that adopt ITSM can improve access to IT operators and support, as well as communication between the IT organization and the business. This is accomplished by establishing an IT service desk that acts as a single point of contact between the business and the IT organization and supports processes such as incident management, event management, and request fulfilment. The IT service desk ensures that all users can access IT support through the appropriate channel.
- **Reduces Unnecessary Work-Load:** Automation is a major focus for IT organizations that want to eliminate tedious manual work and the human error that often comes with it. However, to use automation effectively, IT organizations need to start managing their IT services using ITSM software. ITSM tools enable the transition between managing a process through human activity and managing a process through automated activities, resulting in decreased workloads for IT operators and more time available. To dedicate it to innovation and added value activities.
- **Achieves Better ROI On Corporate ITSM Solution Investment:** Some organizations invest in ITSM software only to find that it does little to improve the performance of their IT organization. These organizations often abandon their ITSM tool before ROI is measured, which is likely to be a negative. The truth is that adopting and implementing ITSM goes beyond simply buying a software tool.

IT service management is about adopting processes that reflect best practices for managing key IT services and functions, and then creating policies and procedures to ensure those processes are followed. Effective management, buy-in from staff and executives, and genuine process changes are requirements for an effective ITSM implementation. If your organization has already invested in an enterprise' ITSM solution, you can improve your ROI by focusing on the people and processes that support your ITSM initiatives.

- **More Effective Planning:** IT service management helps organizations engage in more effective planning activities with a variety of positive consequences. Without a structured approach to IT service management, IT organizations are more likely to make poor strategic decisions that lead to avoidable waste. ITSM best practices, such as establishing a service strategy with input from customer stakeholders or implementing a change review and approval process, help ensure that the IT organization plans effectively before making decision measures.
- **Saves Valuable Time:** Take a look at the ITIL 2011 framework and you will find a series of ITSM processes geared towards increasing efficiency by helping the company save time. The best example of a time-saving ITIL process is knowledge management, the goal of which is to reduce or eliminate the need for the business to rediscover information that you have already learned. With an effective knowledge management process, the IT organization maintains a knowledge base that supports the effective exchange of information between all areas of the business. The result is tremendous time savings, as IT organizations streamline information sharing and spend less time rediscovering information and searching for answers to known problems.
- **Saves Business Money:** IT service operations saves a company money in hundreds of different ways. From the knowledge management process that saves time by supporting the exchange of information (time is money, after all) to information security processes that protect the company from the negative financial and legal consequences of a breach of data, ITSM best practices are designed to drive cost savings and risk mitigation.

- **Efficient Changes:** ITSM offers a framework for change management that ensures that resources are allocated efficiently during the change management process. Minor changes that do not involve version deployment can be cleared quickly if they are well understood and low risk. Normal changes can be approved directly by the change manager, but they can also consult with a Change Advisory Board (CAB) before approving a large, unknown, or emergency change. The ability to tailor the approval process based on the nature of the change is one way ITSM processes help IT organizations manage change more efficiently.

- **Improves Collaboration Between Different Business Function:** If we define business functions as all the activities performed by the business, it's easy to see how implementing ITSM policies and processes can help IT collaborate with other functions more effectively. Under the ITSM framework, the IT department works with finance to optimize the deployment of IT investments. Facilities managers can collaborate with IT administrators to ensure compliance with information security protocols. ITSM also encourages users to report IT problems through the incident reporting process, helping the IT organization to gather more feedback and data on the performance of applications and services.

- **Transparency:** An IT organization without a service catalog is like a restaurant without a menu: it may have fantastic capabilities, but it won't get many orders. Users need transparency into IT processes and services so they know what types of services they can request and how to fulfil their requests. IT service management supports this transparency by establishing service catalogs that contain a comprehensive list of services that the IT organization offers to customers. This catalog helps ensure that customers get the most out of the services that IT can provide them.

- **Higher Return Of IT Investment:** If you have the money, you can invest in the best servers, the best network infrastructure, and the highest-end computers money can buy. Regardless of how much you spend, you probably won't be able to realize the value of those investments without proper processes in place to support your IT infrastructure. You can spend $1,000 on a server, but without proper scheduled maintenance and management, its performance will tend to degrade over time. IT organizations adopting ITSM may choose to establish a Configuration Management Database (CMDB) to better track the presence and utilization of IT assets.

This database is used to ensure that IT investments are deployed in a productive capacity and to maximize the uptime and availability of IT assets. A formal process for the disposition of IT assets helps ensure that organizations get the most money for their used IT infrastructure.

Project Teams: They meet to solve a specific problem, implement a system or make a change. By definition, projects are temporary initiatives, so once completed, it's common for the team to disband (with its members assigned to different locations) or for the entire team to move on to another project. IT project teams often focus on a single release or a group of releases, but rarely do they "own" a system once it goes live.

Support Teams: They share characteristics with operations and project teams. Support teams are permanent and, like operations teams, execute ITSM functions to help the business run without interruption. They are also similar to project teams in that they tackle specific problems. IT support teams are often thought of as operations teams that are assigned multiple "mini-projects" each day.

Process Equipment: They share characteristics with operations and project teams. Support teams are permanent and, like operations teams, execute ITSM functions to help the business run without interruption. They are also similar to project teams in that they tackle specific problems. IT support teams are often thought of as operations teams that are assigned multiple "mini-projects" each day.

ACCESS CONTROL

ITGCs should include various methods of preventing unauthorized access and data manipulation. Coupling robust password management with a least-privilege access policy can instantly lower the chances of a cyber-attack. Full disk encryption is also a common access-related ITGC because it completely locks devices, even while at rest. So if a device is stolen, the hard drive cannot be accessed without the proper recovery key. Access-related ITGCs may also entail quarterly or annual inventory audits to pinpoint the most valuable data and re-evaluate the controls designed to protect it.

SYSTEM LIFE CYCLE CONTROL

There's a reason why applications, systems, and networks have updates — releases contain new features or patch existing vulnerabilities. When users don't regularly update their programs, they do themselves a disservice and put their companies at risk of an attack. That's why many ITGCs focus on forcing regular updates and consistent monitoring of an organization's applications, systems, and network service-level commitments.

To that end, companies often weave ITGCs into the procurement process, asking vendors to supply a Service Organization Controls Report (SOC), and assessing whether extra controls are required to keep data safe and secure. Many companies also implement patch management tools to automatically deploy patches to the operating systems, browsers, and applications that are behind schedule.

PHYSICAL AND EVIRONMENTAL SECURITY CONTROL

When we think of hackers, we often think of a person behind a computer, but that's not always the case. Unfortunately, people with ill-intent enter an office to wreak havoc, so it's important to define and consistently test physical security controls, like key badge entry to sensitive areas and intrusion detection systems.

DATA PROTECTION AND RECOVERY CONTROLS

Accidents, natural disasters, or cyber-attacks can happen anytime, and without backup or recovery plans in place, companies can lose significant data. Most companies enact ITGCs to minimize data loss through database segregation, automated backups, and business continuity plans. ITGCs may also incorporate regular testing of these configurations and plans to confirm their effectiveness and make adjustments as needed.

COMMITTEE OF SPONSORING ORGANISATIONS (COSO)

The Committee of Sponsoring Organizations (COSO) Framework integrates controls into everyday business processes that validate ethical and transparent operations. COSO has five requirements:

- Control environments to uphold industry-standard practices and reduce organizations' legal exposure
- Control activities to make sure tasks are carried out in a way that minimizes risk and accomplishes business objectives
- Information and communications that help stakeholders understand and comply with legal requirements, such as privacy regulations
- Monitoring by internal and/or external auditors to ensure employees are following existing controls
- Risk assessment and management to identify and mitigate as many risks as possible

ISO

ISO 27001 is a framework related to information security and change management. More specifically, ISO 27001 sets out policies and procedures to lessen the legal, physical, and technical risks associated with implementing, monitoring, reviewing, maintaining, and improving an information security management system. ISO 27001 uses a top-down approach, with six steps to attain compliance:

- Define a security policy
- Define the scope of the information security management system
- Conduct a risk assessment
- Manage identified risks
- Select control objectives and controls to be implemented
- Prepare a statement of applicability

By following ISO 27001 conditions, companies show customers that they take security seriously and conform to industry standards. While these components are fairly vague, COSO has published detailed requirements for ESG, AI, and cloud computing-focused companies to observe corresponding regulations in those fields.

INFORMATION TECHNOLOGY CONTROLS: Control should be understood as those procedures intended to evaluate real performance, compare that performance with the objectives set, or correct the differences between the results and the objectives.

Control as part of the administrative process is essential, since if it did not exist, it would not be possible to know if what was planned, organized and executed has been carried out correctly, and therefore has worked well.

Control being the fundamental theme of this article, an analysis is carried out initially as an element of business management, considering what Mairena Romero states, who, in a report presented, analyses control as a phase of the administrative process, analysing the different definitions used by administrators like Stoner, Fayol, Robbins, among others; studying its importance, its classification and the areas of performance. The main objective of her work is to study control as a key element of administration, which allows detecting errors on time and correcting failures in due time, thus applying the appropriate control mechanisms for each case. IT program or application controls are fully automated (that is performed automatically by systems) and are designed to ensure complete and accurate data processing, from input to output. These controls vary depending on the business purpose of the specific application. These controls can also help ensure the privacy and security of data transmitted between applications. IT application control categories may include:

- **Integrity Checks**: Checks that ensure that all records were processed from start to finish.
- **Validity Checks**: Checks that ensure only valid data is entered or processed.
- **Identification**: controls that guarantee that all users are uniquely and irrefutably identified.
- **Authentication** – Controls that provide an authentication mechanism to the application system.
- **Authorization**: Controls that ensure that only approved business users have access to the application system.
- **Input controls**: controls that guarantee the integrity of the data fed from upstream sources to the application system.
- **Forensic controls**: control that ensures that data is scientifically correct and mathematically correct based on inputs and outputs.

INFORMATION TECHNOLOGY CONTROLS AND THE SARBANES-OXLEY ACT (SOX)

SOX (part of United States federal law) requires the CEOs and CFOs of public companies to vouch for the accuracy of financial reporting (Section 302) and requires public companies to establish adequate internal controls over financial reporting. Financial reports (Section 404). The SOX approval resulted in an increased focus on IT controls, as these support financial processing and therefore fall within the scope of management's assessment of internal control under Section 404 of SOX.

The COBIT framework can be used to help with SOX compliance, although COBIT has a considerably broader scope. The PCAOB [2] and SEC [3] SOX 2007 guidance states that IT controls should only be part of the SOX 404 assessment to the extent that specific financial risks are addressed, significantly reducing the scope of controls of IT required in the assessment. . This scoping decision is part of the entity's top-down SOX 404 risk assessment. In addition, Statements on Auditing Standards No. 109 (SAS109) [4] discuss IT risks and control objectives relevant to a financial audit and are referenced by SOX guidance.

Information Technology controls that typically fall within the scope of a SOX 404 assessment may include:

- Specific application control procedures (transaction processing) that directly mitigate identified financial reporting risks. There are usually a few such controls within the main applications of each financial process, such as accounts payable, payroll, general ledger, etc. The focus is on the "key" controls (those that specifically address risks), not the entire application.
- General IT controls that support assertions that programs are working as intended and that key financial reports are reliable, primarily change control and security controls;
- IT operations controls, which ensure that problems with processing are identified and corrected.

Specific activities that may occur to support the assessment of the above key controls include:

- Understand the organization's internal control program and its financial reporting processes.
- Identify IT systems involved in initiating, authorizing, processing, summarizing, and reporting financial data;
- Identify key controls that address specific financial risks;
- Design and implement controls designed to mitigate identified risks and monitor them for continued effectiveness;
- Document and test IT controls;
- Ensuring that IT controls are updated and changed, as necessary, to correspond with changes in internal control processes or financial reporting;
- Monitoring of IT controls for effective operation over time.

AUDITS AND CONTROL OF INFORMATION TECHNOLOGY SYSTEM

Any transfer of information throughout the company ends up blurring the message. That is why it is necessary in the future that companies have few management layers, although with great ability in managing information.

The information tends to blur in the route it has to reach the end users, which is why the audit of information systems arises. The audit of the information systems supports us to verify the current state of the company's information systems: but to better understand its function it is necessary to go to the root of its words and thus define it better, the following scheme gives us represents the definitions of each of its parts; So an information system is an organized set of elements, which can be people, data, activities or material resources in general, which interact with each other to generate information and this can serve as a basis for knowledge.

The audit of information systems is based on the way in which these elements are obtained and their security within the system. In the midst of the information age, companies have realized the importance that information plays within their organization, which is why they will look for the best way to protect it and verify that it is being real and fulfils the function of informing correctly. To the right people. That is why the general audit specialized and gave way to the computer audit and even more specialized to the audit of information systems that all information that interacts in the organization and has an impact on it.

ACCORDING TO UMBERTO ECO;

The audit is understood as a systematic process that consists of objectively obtaining and evaluating evidence on the relative affirmations, economic acts and events; in order to determine the degree of correspondence between those affirmations and the established criteria, that is to say, to verify the veracity of what is said. The beginnings of the audit were mainly accounting with a financial nature, since it was what most interested the owner of a company.

The capitalist society of the industrial era, was very concerned about this economic aspect, forgetting other aspects that were contained in the organization, but with the passage of time and technological advances, the ramification of the audit becomes necessary, leaving this in a general way of the following way:

Based on this generic classification, we can say that the financial audit was the origin, and later gave rise to the operational due to the scope and importance that the users of the audit report require on some operational areas of the company, returning to the audit even more specialized.

Thus, the financial audit examines financial statements in accordance with generally accepted international auditing standards, the corresponding records and operations to determine compliance with generally accepted accounting principles and thus give a sense of reliability in finances.

On the other hand, operational management is a systematic examination of the activities of an organization (or a stipulated segment thereof) in relation to specific objectives, in order to evaluate performance, identify opportunities for improvement and generate:

- Recommendations for improvement
- enhance the achievement of objectives

The audit of information systems belongs to the branch of operational audit. And this is in charge of carrying out the evaluation of standards, technical controls and procedures that have been established in a company to achieve reliability, timeliness, security and confidentiality of the information that is processed through information systems. Due to the fact that most of the Information Systems are regulated or supported by technology, this is a main area on which a lot of emphasis is placed, being in coordination with people specialized in computer science that the auditor supports himself to achieve a correct evaluation and Thus, a good report that provides the necessary information to those interested.

REFERENCES

- TECHTARGET SEARCH DATA CENTER
- CEUPE MAGAZINE
- CORPORATE AND EMPRESARIAL
- JUMPCLOUD
- FRESHWORKS
- MANAGE ENGINE
- HYPER PROOF
- PATHLOCK
- CAREER GUIDE.