IPPF
International Professional Practices Framework

# IT Essentials for Internal Auditors

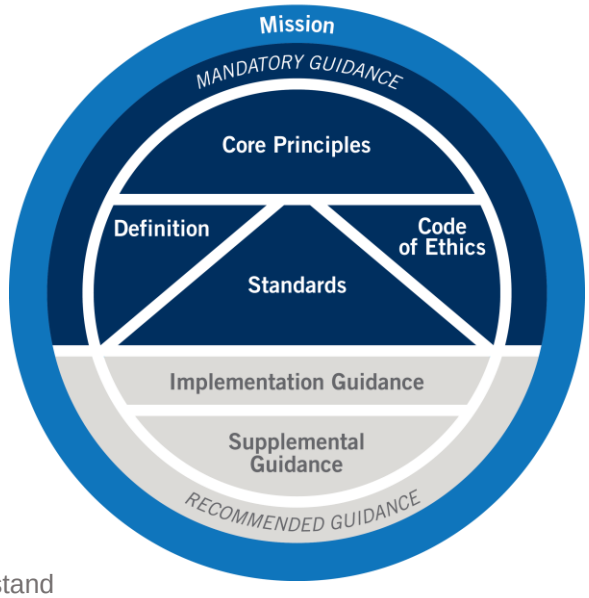
Supplemental Guidance | **Practice Guide**

GLOBAL TECHNOLOGY AUDIT GUIDE

The Institute of Internal Auditors

# About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.




**Mandatory Guidance** is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- International Standards for the Professional Practice of Internal Auditing.

**Recommended Guidance** includes Implementation and Supplemental Guidance. Implementation Guidance is designed to help internal auditors understand how to apply and conform with the requirements of Mandatory Guidance.

## About Supplemental Guidance

Supplemental Guidance provides additional information, advice, and best practices for providing internal audit services. It supports the *Standards* by addressing topical areas and sector-specific issues in more detail than Implementation Guidance and is endorsed by The IIA through formal review and approval processes.

### *Practice Guides*

Practice Guides, a type of Supplemental Guidance, provide detailed approaches, step-by-step processes, and examples intended to support all internal auditors. Select Practice Guides focus on:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

# Contents

# Executive Summary

**In today's world, technology is an integral part** of every organization and underpins almost every piece of data, every transaction or calculation, and every process or business activity. Internal auditors need a basic understanding of underlying information technology (IT) concepts and operations. Without this, internal auditors may not fully comprehend IT objectives and the associated risks, and may lack the ability to assess or audit the design or effectiveness of controls related to those risks.

### Note

The cover, logo, and references in this guide have been updated. The content has not changed.

This guidance introduces the basic IT competencies and understanding needed by any internal auditor and more fully provides discussions and overviews of IT operations, strategies, and the underlying technologies themselves. It does not go into details on information technology controls or how to audit IT; these are covered in other IIA guidance. Rather, it covers essential IT-related activities and concepts that all internal auditors should know.

Overviews are provided on IT governance, the relationship between IT and the business, and how IT creates value through ongoing operations, project delivery, system development, and support, and its monitoring of quality and service delivery levels. This guide also covers the basic understanding needed for three critical IT technical domains — infrastructure, network, and applications — along with a high-level review of applicable challenges and risks in those areas.

Another purpose of this guide is to introduce content from The IIA's IT Competencies Framework (Figure 1), and to align to the IT aspects covered in The IIA's Certified Internal Auditor (CIA) exam, which tests the basic level of IT understanding internal auditors need.

The guide also explores some emerging IT trends and topics. New risks and continued changes of the IT landscape are part of IT's inherent, evolving nature. As noted, specific IT audit activities, IT-related general and application controls, and more advanced topics on IT risks, controls, and audit techniques are covered in other guidance from The IIA, which can also supplement the study of IT when preparing for the CIA exam or for other general knowledge of IT.

# Introduction

**This guidance helps internal auditors** understand how IT operates broadly across an organization and the significant relationship that IT plays in an organization's success. The first section discusses the goals of IT, its relationship with the organization and overall **information technology governance**. Subsequent sections delve into details on the specific technologies and IT processes that should be fundamentally understood by internal auditors, whether they specialize in IT audit or not.

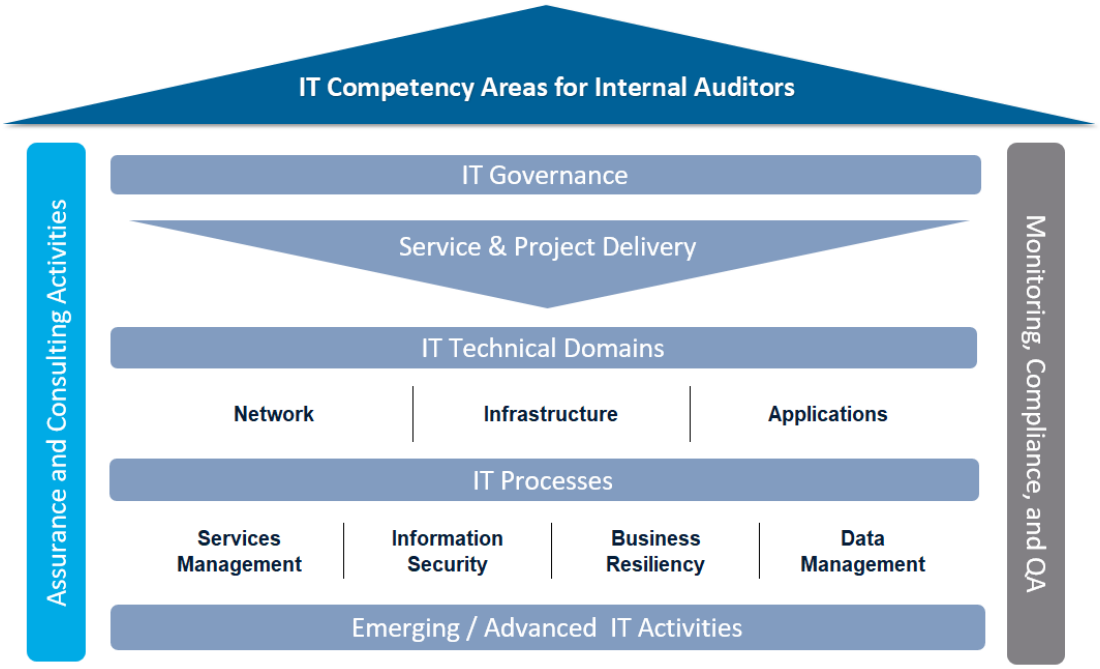
> **Note**
>
> Terms in bold are defined in the Glossary in Appendix B.

As IT is a fundamental part of every organization, it is crucial for the **chief audit executive** (CAE) and internal auditors to have a baseline understanding and knowledge of IT and the management of critical data within their organizations. Protecting enterprise data, supporting IT operations, and safeguarding technology are just a few of the challenges organizations face today. While these challenges may seem daunting, they are more than offset by the potential opportunities IT allows an entity, such as optimizing its operations, innovating product development, and leveraging processes including data analytics, and technologies such as robotic process automation (RPA), or artificial intelligence (AI).

IT is imperative to an organization's strategy, and understanding the impacts technology can have on business processes and **risk management** will help elevate internal audit as a trusted advisor and value creator.

Figure 1 depicts the significant IT areas in which internal auditors should have a foundational understanding.

**Figure 1: The IIA's IT Competencies for Internal Auditors**




Source: The Institute of Internal Auditors.

## Conformance with The IIA's Code of Ethics and Standards

Although this guide does not go into specific details of performing an IT audit, the general content will help internal auditors conform with the Competency principle of The IIA's Code of Ethics and multiple IIA standards, specifically Standard 1200 – Proficiency and Due Professional Care, which states, "**Engagements** must be performed with proficiency and due professional care," and Standard 1210 – Proficiency, which states, "Internal auditors must possess the knowledge skills, and other competencies needed to perform their individual responsibilities. The **internal audit activity** collectively must possess or obtain and apply the knowledge, skills, and other competencies needed to perform its responsibilities." Internal auditors should have sufficient knowledge of key IT **risks** and controls and available technology-based audit techniques to perform their assigned work.

### Additional Resources

This guide will reference standards from other governing bodies. IIA Standards will be noted as such and will include the standard number.

When assigning auditors to an engagement that may require specific skills and abilities, such as an audit with IT components, Standard 2230 – Engagement Resource Allocation states, "Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources." The interpretation of this standard states, "Appropriate refers to the mix of

knowledge, skills, and other competencies needed to perform the engagement." Strengthening general IT knowledge will assist the internal audit department and individual internal auditor in obtaining the skillsets required to perform IT related audits.

If an internal audit department lacks personnel with the skills necessary to perform an audit that encompasses aspects of the IT environment, it may choose to outsource or cosource engagements. In doing so, the internal audit activity retains responsibility for the audit as a whole. Standard 2340 – Engagement Supervision states, "Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed."

# Relationship with the Business and Overall IT Governance

**Technology is complex and rapidly changing**, yet organizations expect their IT services to be secure, efficient, reliable, up to date, and cost-effective.

This section will cover IT as a cross-functional business unit that is an essential service provider to the organization. The relationship between the organization and IT should be clearly understood, and IT governance should be set up to deliver value to stakeholders. Additionally, IT management should ensure that IT services and projects delivered are monitored for quality and compliance with laws and regulations that are increasingly disparate and changing rapidly.

In organizational and business activities, IT has become intrinsic to creating value, enabling competitive services, innovating and supporting critical strategies, and supporting internal devices and applications. No longer is IT a silo of activity operating with limited contact among employees, customers, and partners. Business interfaces and transactions, whether business-to-business (B2B) or business-to-consumer (B2C), are enabled by technologies and IT operations, such that devices (e.g., PCs, mobile phones, laptops, tablets) are part of daily life at work and home.

## Business Enablement – the Goal of IT

The overriding goal of IT is business enablement, which requires a strong relationship and understanding of the organization's business function. Technology enables almost all core business processes and the direction of IT should align to the organization's business strategies. There should be transparency between the organization and IT concerning costs, service levels, options, and what optimizes and provides the most value to business units and the overall enterprise.

Because of its fundamental organizational presence and because it operates as a business within a business, IT leadership should have a "seat at the table" to better understand business initiatives, strategies, priorities, and changes. IT should participate at the initiation stage of projects to provide meaningful input regarding key business decisions that will require direct or indirect IT support.

The chief information officer (CIO) must enable the organization while tactically balancing and optimizing the direction of IT strategies and architectures.

***IT Governance***

IT must be managed broadly in a way that ensures optimal delivery of services (such as networks, infrastructure, and applications) to the organization and end customer. IT must also create value and support organizational success. Sound IT governance helps deliver on these objectives. Key elements and components of IT governance include:

### Resource

For more information on the IT governance process, see The IIA's GTAG, "Auditing IT Governance."

- **Strategic alignment** – providing direction, services, projects, and objectives to support the organization's business goals and maximize return on investment (ROI).
- **Risk management** – determining processes and policies are in place to ensure risks are adequately addressed.
- **Value delivery** – ensuring maximum IT service is provided throughout the organization.
- **Resource management** – providing high-level direction for sourcing and use of IT resources to ensure adequate capability and overseeing the enterprise level of IT funding.
- **Organizational set-up** – addressing the necessary roles, functions, and reporting relationships allowing IT to meet organizational needs while assuring requirements are addressed via formal evaluation and prioritization.
- **Policy setting** – ensuring that industry standards, policies, and frameworks are implemented to address the organization's risk, compliance, and regulatory requirements.

## IT as a Business

IT is not just a cost center, it is an enterprisewide function that serves as an internal business. In most organizations, a CIO and/or chief technology officer (CTO) are responsible for managing and ensuring delivery of IT services and data access across the enterprise. Organizations may also have a chief information security officer (CISO) to oversee IT security, and often a dedicated data protection officer (DPO), chief data officer (CDO), and/or a chief privacy officer (CPO) to oversee the data and compliance aspects. It should be noted that the latter three roles are often outside of the IT organization. The function of these roles is more important than the actual title as organizations may use different titles and/or combine roles.

IT management must understand the organization it supports, its critical processes, priorities, and strategic objectives. CIOs should consider their organizational peers and related business units as customers or clients. In many large organizations, IT follows a "partnership" model in which the CIO manages and oversees multiple sources of internal and external service providers that are expected to deliver a seamless experience to the organization.

Like any business, IT services should be delivered timely, reliably, securely, and in compliance with legal and regulatory requirements. IT must also protect data and information assets against breaches of confidentiality, integrity, and availability. This can be a challenge as most IT teams

support internal devices and applications as well as coordinate with external or outsourced service providers (including “cloud” providers) and consultants.

The decision to perform duties in-house rather than outsource may be a matter of enterprise strategy (e.g., protecting intellectual property, maintaining control of core activities, or for economies of scale), budget and staffing requirements, or combinations thereof.

This reinforces the need for the CIO to manage IT as a business and be competitive with other potential external sourcing of technology options.

As part of managing IT as a business, the IT organization should manage and maintain service level agreements (SLAs), provide and monitor key performance indicators (KPIs) and key risk indicators (KRIs), and retain relationship managers to manage the services offered internally, externally, and to the organization as a customer.

### Outsourcing IT Elements to the Cloud

Outsourcing IT elements to external parties and/or use of the “cloud” is now commonplace, with different models and combinations to choose from. Typical services either fully or partially outsourced to external providers include: SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). More detail on the functionality and characteristics of these service models is available in the “IT Network” section of this guide.

From internal audit’s perspective, how technology is delivered in an organization, by whom, and for whom must be understood to assess most processes, functions, systems, or projects. Even strategic assessments will require a good understanding of the technology supporting the direction of an organization’s business.

## Process Oversight: IT Service Delivery and Project Portfolio Management

The IT function delivers processes and services to the organization through IT operations (supporting business processes), system development, IT infrastructure, and information security (IS). Overseeing the delivery of these processes and services in collaboration with non-IT management is essential. IT governance provides the strategies, mechanisms, and measurements for delivering business value, fosters a partnership with the organization, and helps ensure the establishment and oversight of jointly owned objectives.

In addition to delivering core IT processes, services, and IT infrastructure, IT manages and delivers a portfolio of projects in support of the organization (i.e., software development or acquisition) or in support of the overall IT direction (i.e., infrastructure or architectural design projects). The delivery of projects on time, within scope, and on budget is a major challenge to both IT and the business function.

Process oversight establishes accountability and helps ensure deliverables meet both the needs of the organization and customer.

## Ongoing Monitoring: Quality and Compliance Needs/Activities

IT management should monitor and ensure the appropriate level of quality is delivered to its clients and the organization. This includes not only the design, delivery, and implementation of services that meet regulatory and legal compliance, but also ensuring ongoing operational requirements.

IT management must monitor the delivery of quality and compliance needs on an overall basis and ensure continuous improvement and flexibility as business requirements change. While quality and compliance should be built into all IT processes and projects, both should be monitored across the IT enterprise and in partnership with business service level expectations.

Monitoring of the quality and reliability of services is imperative in order for management to ensure that processes are being managed to expectations of the **board** and senior leadership. This assurance cannot be provided without ongoing monitoring and timely resolution of operational and control gaps.

## Challenges and Risks for IT Governance and the IT and Business Relationship

IT requires broad **governance**, alignment with the organization, and the need to be efficient, reliable, and timely in the delivery of effective services to its clients. Internal auditors should understand that many IT challenges and risks start at the governance and strategy level, followed by effective and competitive delivery and monitoring of overall service and quality levels. Internal auditors should also have a basic understanding of the common IT challenges and risks when assessing, evaluating, or reviewing IT governance and business relationships, which can include but are not limited to:

- **IT strategy and direction are misaligned with the business or organization's strategy.** Often, the technology road map is designed to improve the current business model and operations or is focused on IT infrastructure initiatives, but not to enable or accommodate potential future business objectives or models. If adaptability and flexibility are ignored, competitiveness and innovation may be hindered.
- **IT leadership does not have a "seat at the table" when business strategy is being developed, or is not part of the decision-making process on business direction and options under consideration.** IT may be excluded in business strategy development. Failure to engage information security and IT early in planning stages may result in an increased risk for adverse consequences, such as additional costs, reduced performance, regulatory fines and penalties, and even increased threat of inappropriate data/information exposure.
- **The use of "rogue IT."** The concept of rogue IT, also known as "shadow IT," occurs when anyone in the organization uses technology that is not sanctioned or even known to IT. This is a significant risk when an organization has multiple business units, locations, campuses, or subsidiaries.

Common instances might include a business unit purchasing and/or using applications or programs (e.g., an Excel macro), platforms, or infrastructure as a service to better meet their perceived needs but failing to consult IT leadership and/or follow appropriate governance protocols prior to proceeding with implementation. Whether or not the proper protocol is deliberately avoided, this indicates poor IT governance and a less than optimal relationship between the business function and IT. Business units within an organization should work together with IT to ensure the entire organization follows an established process for assessing, onboarding, and managing hardware and software.

- **The organization perceives IT as an impediment to selecting the best solution or optimizing the sourcing of an IT service.** The potential tension between the IT function and business function as to what is best delivered internally versus externally can be a major challenge. One method to overcome this challenge is for IT to indicate the cost or assign fees and an ROI (cost savings potential) for their services and consultation. Granting the internal IT organization the ability to complete a request for proposal (RFP), just as an external vendor, allows the organization to have a side-by-side comparison for their choice of working with an external provider's solution or service versus choosing an in-house solution or service.
- **The technology solutions in use are obsolete or poorly maintained.** Ensuring that software and infrastructure components are up to date and supported are essential for reliable IT operations. Business and IT functions should cooperate to establish adequate maintenance windows to ensure updates, patching, and other critical refresh activities are funded and performed in a timely manner. Failure to keep technology up to date can result in "technology debt": a lack of IT investment, either financial or in upgrades, that contributes to inefficiencies, risks (particularly around information security), or lost opportunities that can build up over time. Unrecognized levels of technology debt can lead to uninformed decisions, and is often the root cause of operational or strategic issues. It is possible for technology debt to be accepted, planned, or even built, but when doing so, the risks and impacts should be formally understood and accepted by appropriate management.
- **Lack of clarity and/or ownership of formal IT risk.** Organizations may view IT-related risks as the responsibility of the CIO or IT function. However, most IT-related risks ultimately are owned and should be accepted by the appropriate business function. With the proper understanding of who owns and takes responsibility for risks, the business function is more apt to fund IT risk mitigation efforts and partner with IT in creating value and optimizing decisions.
- **Inefficient or ineffective project governance or management.** Business-critical IT projects should be completed on time, in scope, and on budget. Project governance is critical to ensure all projects are appropriately prioritized and resourced, and delivered timely and effectively. Project management helps ensure critical project aspects are transparent to all stakeholders, giving those responsible a clear and accurate understanding of project status, issues, risks, and deliverables. It also means that "scope creep," or the tendency for a project's requirements to increase over time, is effectively managed.

From an internal audit perspective, involvement in the entirety of key projects – from business case development through project monitoring and final delivery — can be a critical success factor

and **add value**. However, when involved in a project from start to finish, the internal audit function must maintain its conformance with Standard 1100 – Independence and Objectivity, understanding that management is ultimately responsible for decision-making and delivery. This standard states that “The internal audit activity must be independent, and internal auditors must be objective in performing their work.”

# IT Infrastructure

**IT infrastructure refers to the hardware and software** that supports the management of an organization's information and data. Major components of IT infrastructure include hardware, software, storage/databases (DBs), and a network. From an organization's IT standpoint, it is important to look at the infrastructure as a whole as well as each element as a component. This section covers some of the in-depth infrastructure topics and offers a high-level overview of the main components.

## Main Components

### *IT Hardware*

Hardware consists of physical servers, mainframe machines, and peripherals, which are usually housed in enterprise server rooms or data centers. These may be housed on premise, off premise, outsourced to a third party, in the cloud, or a combination of these. IT hardware also includes end-user devices (e.g., laptops and desktops) used to access enterprise information and data, printers, network components, and storage devices, among others. An organization's hardware is usually connected to an IT network.

### *Operating Systems (OS)*

An operating system (OS) is a collection of programs (source code) that manage the computer's components and computing operations to deliver a result for the user. Operating system software provides a means to manage and access IT hardware resources and acts as an interface or platform between the end-user and the IT hardware on the network. Some types include:

- Server operating systems, which are designed to process the requests of multiple end-user computers on the enterprise's IT network. Examples include IBM AS/400, Windows Server, or Red Hat Linux.
- Client operating systems, which generally support a single user and are designed for end-user devices. Examples include Windows and Mac OS, but also include portable or mobile operating systems.
- Firmware, unlike standard operating systems, has the code embedded into the hardware. It is common to see firmware in devices and such as household appliances, medical devices, or open-source routers and firewalls.

### *Enterprise and Application Software*

Enterprise software, sometimes called enterprise resource planning (ERP) software, allows an organization to capture and connect the information and content of its various business processes and promotes efficient management decisions by the organization. Enterprise-level software includes SAP, Oracle ERP, Microsoft Dynamics, JD Edwards ERP, and others.

Application software is use-case specific software and usually performs a single function and includes word processing programs, spreadsheets, and graphics processing software.

### *Storage and Databases*

Repositories of an organization's business information frequently managed by specialized software allow users on the network to access, and where necessary, amend and append enterprise information.

### *Network*

A network is two or more IT hardware components connected for the purposes of sharing information.

### *Servers*

A server is a computer program or device that provides functionality for other programs or devices, called clients. Different types of servers include web servers, database servers, file servers, print servers, and application servers, among others. Also commonly referred to as a server is the actual hardware (physical computer), which is generally a powerful computer with the capabilities of processing large amounts of data and often dedicated to a specific business function, such as the organization's email, files, applications, and/or website. In the general business context, a server may describe the software or the hardware, but more likely it describes the combination of the two as both are needed to provide functionality.

### *Server Operating Systems*

The most common servers today either run Microsoft's proprietary Windows Operating System, IBM AS/400, or Linux, a modifiable open source operating system. Figure 2 describes various characteristics of the two operating systems.

**Figure 2: Comparison of Windows and Linux Operating Systems**

| | Windows OS | Linux OS |
|---|---|---|
| **Licensing** | **All proprietary Windows operating systems instances are required to be licensed.** | **Some Linux-based operating systems sold by vendors may have an associated license fee.** |
| **User experience** | **Text user interfaces (TUI) and graphical user interfaces (GUI).** | **Text user interfaces (TUI) and graphical user interfaces (GUI).** |
| **Source code access** | **Microsoft Windows is a proprietary operating system. This arrangement gives Microsoft a competitive advantage in the market. The general public does not have access to the source code of the Microsoft operating system.** | **The Linux operating system is built using open source technologies. This means the source code can be inspected, studied, modified, enhanced, and distributed by anyone.** |

| | | |
|---|---|---|
| **Security** | **Windows operating system security is focused on three areas:**<br>**Identity and Access Management: permissions, ownership of objects, inheritance of permissions, user rights, and object auditing.**<br>**Threat Protection: protects endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture.**<br>**Information Protection: addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.** | **Due to its open source nature, users are able to review source code and identify any security weaknesses.**<br>**Compared to Windows OS, Linux OS typically have fewer security vulnerabilities and have fewer unprotected structures.** |

### *Mainframes*

A mainframe is a computer (hardware) designed to host the commercial databases, transaction servers, and applications that require a greater degree of security and availability than is commonly found on smaller-scale machines. These machines remain in popular use by large organizations due to their reliability and stability.

Mainframes process large amounts of data, such as country and industry statistics, and tasks similar to bulk and high-volume transaction processing. Industries such as banking and insurance rely on mainframes to process the enormous transaction volume generated by the financial industry. In sectors such as health care, transportation, and public services, mainframes assist with processing large data volumes and provide support for strict compliance requirements.

Mainframes are usually the preferred infrastructure type when there is a requirement for large volumes of concurrent users. The aviation and airline travel industry is a good example because online and travel agent bookings, flight simulations, and navigation systems require high bandwidth applications and are heavily reliant on the capabilities of mainframes.

There are two main transaction-processing concepts for mainframes: batch job processing and online transaction processing:

- Batch jobs are processed without user intervention, where large volumes of information are processed in bulk rather than as individual inputs. Batches, which can sometimes include hundreds or thousands of transactions, are typically presequenced to execute at a specified time window during off-peak periods. Outputs from batch-processed jobs are typically summaries of information such as daily sales, order processing, and inventory updates.
- Online Transaction Processing (OLTP) processes data typically requiring an immediate and real-time response, and the user interaction with the mainframe is usually very short and concurrent with processing. OLTP is beneficial for services that must be continuously available and where data and information integrity are of high importance. This concept applies to ATM transactions and credit or debit card purchases.

Some major manufacturers of mainframes are IBM and Fujitsu.

### *Mainframe Operating Systems*

Due to the large amounts of data that a mainframe processes, its internal components, including internal memory, processing capability, internal and external peripherals, storage, and operating

system should be adequately efficient and complex enough to deliver the relied-upon performance standard.

Each manufacturer has its version of an operating system, which is configured and customized to suit the manufacturer's hardware and interfaces (e.g., z/OS is the operating system for IBM mainframes).

### *Virtualization*

Virtualization is the process of configuring a computer system in an environment that is separate from the actual hardware. Prior to the concept of virtualization, all operating systems were installed on the actual computer hardware, and that computer could only run one operating system. With the concept of virtualization, the virtual machine (VM) operating system runs on the computer hardware, and multiple virtualized operating systems can run under the control of that virtual machine. Common computer resources such as servers, desktops, operating systems, files, storage, or networks can all be virtualized. VMs can be used for targeted purposes and discarded once that use has been fulfilled.

This virtualized environment is usually accomplished by installing and using specialized software (called a hypervisor) on the host machine that emulates a virtualized environment. A hypervisor is a specific software set that creates and runs VMs and is also known as a virtual machine monitor /manager or VMM. There are two types of hypervisors: Type 1, which runs directly as the operating system on the host machine hardware, also known as a "bare metal" type, and Type 2, which runs in an already established operating system environment, known as a "hosted" type.

### *Directory Services*

All computer networks have IT resources associated with them, such as users, printers, storage devices, files and folders, fax machines, and more. Therefore, it makes sense that each of these resources is associated with a unique network address.

A directory service is an operating system service that provides a list of names of the associated network IT resources (e.g., users, printers, storage devices, files, and folders) and the unique network address of each. Maintaining these directories is important from an access and security standpoint.

A standard (or protocol) for directory services was initially developed to manage information on a global network of resources. This protocol was called X.500 protocol. Based on the X.500 standard, software vendors developed proprietary solutions to manage network devices related to their corresponding operating systems. A common directory service solution is Microsoft's Active Directory (AD), for use with the Windows operating system. AD has additional functionality bundled with the X.500 standard, and administrators can add new users, remove, or modify network elements, specify usage and security privileges, manage password policies, and other tasks.

An example of an open source directory protocol is the lightweight directory access protocol (LDAP), which is derived from the X.500 standard. LDAP is used to access centrally stored network information, but is simpler and less resource-intensive. When using LDAP, network resource information for an organization can be stored and managed in a centralized location.

In a Linux environment where flexibility and customization are required, open source LDAP solutions such as OpenLDAP are frequently used. There are, however, some drawbacks to using open source solutions in a Linux environment, including the need for specifically skilled staff; slowed authentication when large LDAP repositories are in use; and potential system incompatibility with some devices, applications, and web applications.

### *Data Storage*

Three primary forms of data storage are commonly used, databases, data warehouses, and data lakes. Databases are the most common and will be discussed in detail below. The difference between the three types of storage can be described by the source and type of data:

- **Database –** single source repository; can be structured or unstructured data.
- **Data warehouse –** multiple sources of data stored in a single repository. Typically, structured data that is easily retrievable for a defined purpose.
- **Data lake –** multiple sources of data stored in a single repository. Data is unstructured and not easily retrievable.

### *Databases*

A database is an organization of data in a manner that allows for easy retrieval and updates. There are two main types of databases: relational and nonrelational databases.

Relational databases have these characteristics:

- Multiple datasets arranged in a table-based schema of rows and columns.
- Clearly defined relationships among the tables.
- Useful for managing large stores of transactional and related data.
- Data security models allow users to see only what they are authorized to see.
- Can be queried (analyzed) using a simple Structured Query Language (SQL) and in tabular format, usually using proprietary database software.

Nonrelational or Not Only SQL (NoSQL) databases feature these characteristics:

- Datasets arranged in clusters and nontabular format.
- Accommodates unstructured data in a modern big data environment.
- Simple design for different types of data (e.g., time series, contacts, media).

Relational database management systems (RDBMS) are platforms that allow users to update, create, append, and delete table data within a relational database. RDBMS platforms are typically proprietary, requiring licensed use of the platform. Typical RDBMS platforms include Microsoft SQL Server, IBM DB2, Oracle Database, MySQL, and Microsoft Access.

SQL is a database language used by the RDBMS platforms to interact with (query) data in tables. An example is shown in Figure 3.

**Figure 3: Example of an SQL Query**

```
SELECT * FROM Members WHERE Age > 30
```

In this example, all entries from a table called “Members” are selected in which their age, denoted by entries in the “Age” column, is greater than 30.

A NoSQL database is a category of non-relational database management systems. These databases do not conform to the “relational” model of a database, in which there is a significant increase in the database workload and where a typical approach would be to upgrade hardware to meet performance expectations. There is a time and cost impact of this approach, which is referred to as “scaling up.” “Scaling out” refers to distributing large database workloads to multiple hosts as workloads increase. NoSQL databases are popular with entities that deal with enormous and varied data elements and wish to “scale out” in a more efficient manner.

A comparison of SQL and NoSQL databases is provided in Appendix G.

### *Messaging*

Messaging in the context of this guide refers to the creating, sharing, using, and managing the transfer of enterprise information over an IT network. Modern organizations use a variety of internally and externally supported messaging tools to communicate internally, with business partners, and with customers.

One of the most common forms of computer messaging is email, which at its core is a message sent from one computer and received by another over a network. Email and the concept of messaging in general has evolved over time to include elements such as text, images, and attachments, and many organizations open their networks for public messaging tools, such as Skype or Zoom.

### *Messaging Protocols*

A number of protocols (message transfer rules) have been developed to administer and govern the transfer of messages among computers on a network. There are a number of message-related protocols that govern how messages are sent, received, and queued. An easy way to think of a protocol is to consider it similar to a language. For two devices to communicate, they must establish rules of the language they will follow.

As mentioned in the Routers and Switches portion of the Network Components and Concepts section, TCP/IP defines the rules for how data is sent and received over a network. TCP/IP is the baseline protocol that supports internet communication, and all other protocols leverage TCP/IP.

Simple Mail Transfer Protocol (SMTP) governs how email messages are sent and received. Messages must be queued because users are not necessarily immediately available to consume them.

Messages are consumed using one of two queuing protocols: Post Office Protocol (POP) and Internet Message Access Protocol (IMAP):

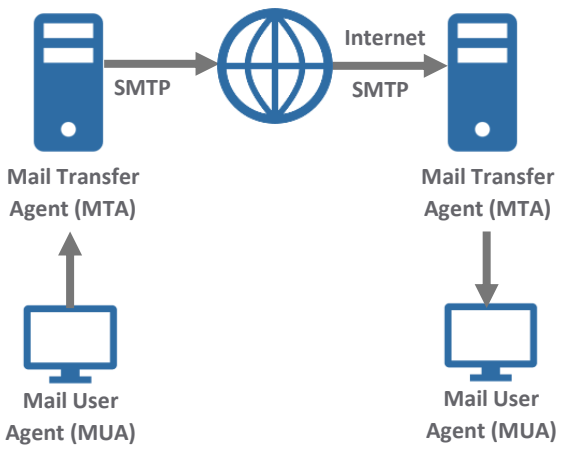
- POP messages are received and stored on an email server. When these messages are consumed, they are downloaded to the consumer's device. Messages are not retained on the server once consumed.
- IMAP messages are received and retained on an email server. When these messages are consumed, they can be organized into various folders rather than being downloaded to the consumer's device. Messages are retained on the server once consumed, thus IMAP can be thought of as a file server for messages.

### *Email Domains and Participants*

Virtually all organizations have a unique email domain (the content that comes after the @ symbol in an email address), which is considered a local domain. This local domain is managed through a mail server, also known as a mail (or message) transfer agent (MTA). This server can be administered by the organization or through a third party or cloud service (Figure 4).

Email is composed and delivered using an email client, which is either a web-based application, such as Gmail, or by using a dedicated application on a user's computer, such as Microsoft Outlook. The email client is also called the Mail User Agent (MUA).

**Figure 4: Typical Email Delivery Process**




Source: The Institute of Internal Auditors.

When a user sends an email, it transmits to the MTA, which collates and distributes internal email (messages within the same domain). It also distributes outgoing email to external users (outside the domain).

Each mail user (MU) is assigned a unique email address, with the format of **user@domain.com.** This corresponds to a "mailbox" to which the MTA will deliver all incoming messages. The MTA will also label all outgoing mail from the mailbox with the user's unique email address.

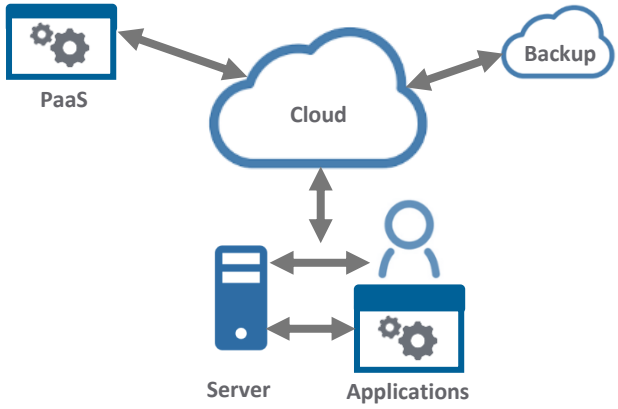
### *Spam Filters*

MTAs use spam filters, or mail monitors for unwanted communication. Spam filters attempt to identify and redirect unwanted or unsolicited email. Spam filters require near constant maintenance due to the nature of the filtering method. Frequently, false positives allowing unwanted email to arrive at a user's mailbox and legitimate email is sometimes redirected to a spam or junk mail folder. Reputable spam filters have sophisticated anti-virus capabilities to limit the threat of viruses. Mail monitors notify the user of new email and allow users to identify legitimate and suspicious messages.

### *File Sharing*

Before the internet and networked devices, users would share files using floppy disks. With the advent of protocols such as File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP) (mentioned in the Protocols portion of the IT Network section), file sharing became easier, but not necessarily user friendly. File sharing allows users to easily share files such as books, music, photos, or anything in an electronic format, either publicly or privately, over the internet (Figure 5).

**Figure 5: Typical Commercial File Sharing Platform Example**




Source: The Institute of Internal Auditors.

Commercial file sharing platforms, such as Dropbox, Microsoft One Drive, Google Drive, Microsoft SharePoint, Apple iCloud, and others usually have parameters or restrictions over the type of sharing (i.e., permissions) of files. Shared files can be created, read, updated, or deleted, depending on the type of permissions allocated to the shared file. Organizations should be aware that many of these tools require little or no licensing, and when it comes to data retention and destruction, an organization may have little control over where their data is located (typically in the cloud) or how long it is retained.

However, commercial file sharing platforms have invested resources in user and file security at each step of the process. Security features can include two-factor authentication, user permissions, file encryption, and in some cases, compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) for health care and Financial Industry Regulatory Authority (FINRA) for the financial services industry in the United States and European Securities and Market Authorities (ESMA) in Europe. However, organizations should be aware of any legal, regulatory, or security concerns in relation to the use of any of these services. As such, a file share policy is recommended.

### *Mobile Devices*

Many organizations allow their employees to connect a personal device to the company's network, which affords the employee an opportunity to carry fewer devices. It also provides the organization a potential cost savings by not having to purchase additional devices. While this practice, referred to as "bring your own device" (BYOD) or "bring your own technology" (BYOT),

offers efficiencies, it can introduce potential security concerns. (For purposes of this guidance, we will refer to both concepts of BYOD and BYOT as BYOD.)

### *Mobile Operating Systems*

Mobile operating systems are the primary level software that allows mobile devices to manage their own internal components and interact with the device user. The mobile OS controls input on the mobile device from various sources (e.g., touchscreen, microphone, camera, GPS) and allows users to interact with the device via applications loaded onto it.

The most common mobile OSs are Apple iOS and Android, but there are others, such as Microsoft's Windows Mobile, Symbian, and Blackberry OS. Though these may not be as prevalent as iOS or Android, organizations should be aware of the use of these other OSs if they allow their employees to bring their own devices, as any device connected to an organization's network can pose security risks.

The open source nature of the Android OS implies that device manufacturers and network providers can make changes to the OS for many reasons, including device and network optimization. This layered approach can have a significant impact on the security and features of the Android OS. On the other hand, Apple strictly controls the iOS environment. Source code is not shared with network providers and Apple pushes updates to their devices.

### *Mobile Device Management and Mobile Application Management*

Mobile device management (MDM) is software that allows an organization to control the features of a device (e.g., smartphones, tablets, eReaders, wearables) to secure and enforce policies. This enables organizations to manage large numbers of their mobile devices in a consistent and scalable manner. MDM also allows the organization to remotely wipe clean any device that is lost or compromised. The drawback to this is the resultant limited user flexibility on the corporate mobile device.

Mobile application management (MAM) describes the software and services responsible for provisioning and managing access to mobile applications (developed in-house or commercially available) whether applied to organization-owned mobile devices or BYOD. MAM also has the added benefit of being able to limit the sharing of corporate data among applications.

The main focus of MDM and MAM is to control exposure of corporate applications, mail, and confidential documents, and to maintain integration with other corporate technology assets (e.g., laptops, printers). In addition, security policies can be embedded and enforced at the corporate application level and may not rely on device-level security or OS patches. This implies that constant testing of MAM applications is required to ensure compatibility with device-level OS upgrades.

Organizations should consider an appropriate mobile device management policy and BYOD policy.

## Infrastructure Challenges and Risks

An organization's infrastructure is the backbone of its IT operations. When set up well, it can help maximize efficiency. When not optimized, it can introduce unnecessary risks and challenges.

Infrastructure is a key component for an internal auditor to understand for all IT-related engagements. There are numerous challenges/risks related to an organization's IT infrastructure that can include but are not limited to:

- **Configuration –** where the operating systems and the associated applications (enterprise and end-user) are not configured securely, vulnerabilities can exist.
- **Security –**
    - Inadequate development or management of security exceptions can allow for device obsolescence.
    - Poor or fragmented encryption or access management can allow excessive access, especially when the key does not change after the individual being assigned the key is no longer in a position to need access. Additionally, there is a risk of data exposure when the key expires and a new key is not assigned in a timely manner.
    - Devices added to the network without proper hardening (securing) can increase the risk of compromise due to open protocols, default passwords, and lack of monitoring.
    - Stale or generic security training increases the risk that users will succumb to social engineering tactics.
    - BYOD can lead to data leakage of devices on the network when internal processes are not followed properly.
    - Missing, outdated, or improperly placed rules can allow bad actors to circumvent controls such as access control lists (ACLs) and firewall rules.
- **Conformity –** industry recognized frameworks, standards, or methodologies may not be followed, introducing potential regulatory or compliance risk.
- **Patches –** if patches are not applied to critical systems, it can introduce the IT infrastructure to vulnerabilities and security issues.

### Resource

For more information on patch management, see IIA GTAG, "IT Change Management: Critical for Organizational Success, 3rd Edition."

# IT Network

## Defining a Network

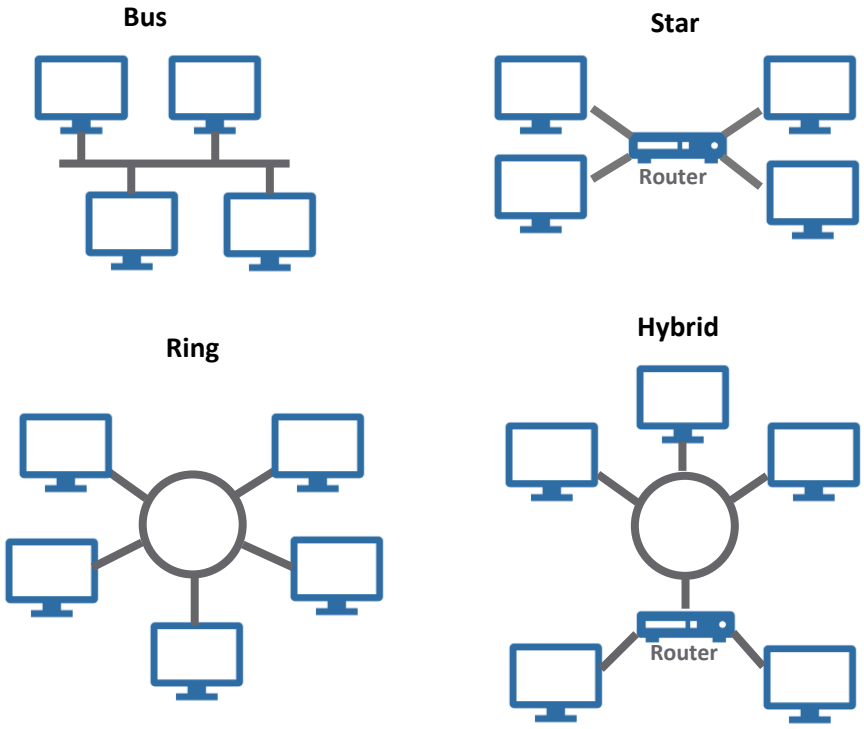
**The simplest definition of a network in the IT context** is a means of connecting two or more computers for the purposes of sharing information. A network generally has three key characteristics: topology, architecture, and protocols. This section explains each and offers examples. It also introduces concepts including the layered service mode, remote network access, and network defense.

There are three main types of networks: local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). An organization's size and geographical footprint will typically determine which type is most suitable. LANs are utilized to communicate within or between floors of a building; MANs are intended to communicate within buildings within a campus or city; and a WAN enables communication within multiple cities, states, or even countries. Any system or device, such as a PC, a laptop, or a mobile device, connected to a network is referred to as a node.

### *Topology*

The topology of a network depicts how it is physically and logically arranged. Bus, star, ring, or hybrid topologies, as shown in Figure 6, are common examples.

Figure 6: Network Topology Examples




Source: The Institute of Internal Auditors.

### *Network Architecture*

Network architecture provides context to understand an organization's IT structure, and there are multiple architecture types from which to choose.

#### Peer-to-peer

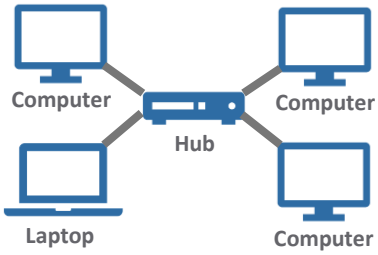
Peer-to-peer, or P2P, architecture is typically used for networking servers or smaller end-user systems, and is sometimes referred to as a distributed application file sharing network. Distributed application refers to software or applications that are executed or run on multiple nodes within the network.

A P2P architecture indicates there is no network hierarchy. Tasks are performed and data is shared among a network's members (nodes) via a hub. While some nodes may be more powerful due to hardware differences or contain different data due to their purpose, the P2P network design offers the same privileges or levels of authority among all nodes.

In a P2P network, nodes can communicate directly with one another, giving this architecture greater flexibility in designing distributed applications. This architecture offers resiliency to change and disruption as dependencies among peer nodes are low. A P2P structure simplifies service layering (see The OSI Seven-Layer Model in Figure 11) by simplifying connection designs between nodes.

A LAN, for example, could be configured as a P2P architecture, as shown in Figure 7.

**Figure 7: Peer-to-peer Network Model**

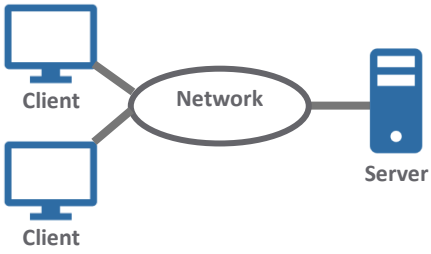



Source: The Institute of Internal Auditors.

### *Client-server*

Client-server architecture is a model based on a hierarchy of service. Individual clients or nodes (i.e., computer on a network) request services from servers. The server(s) then provide the service(s) to the client. This method is beneficial for its security aspects. For example, authentication (i.e., logon) servers use a hierarchy to provide secure access to network resources. A client provides credentials to a logon server and receives an access token or key.

**Figure 8: Client-server Network Model**

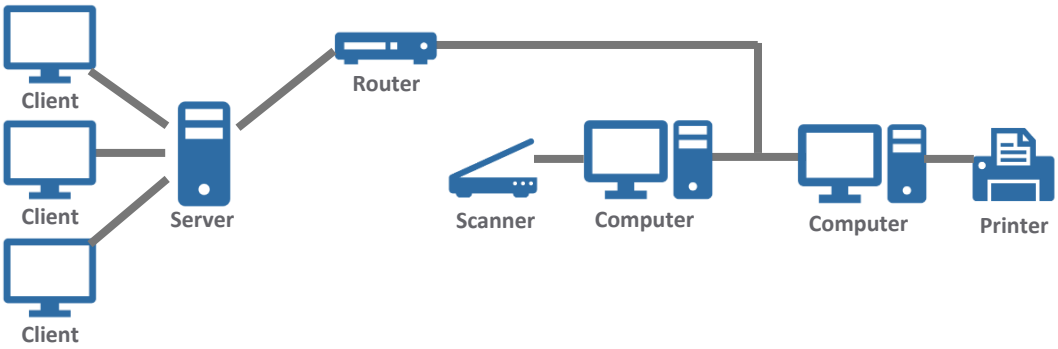



Source: The Institute of Internal Auditors.

For example, a LAN can be configured as a client-server architecture, as shown in Figure 8.

A single node can be both client and server, which can offer ease of planning and understanding on small-scale or location-based network implementations.

**Figure 9: Hybrid Network Architecture**




Source: The Institute of Internal Auditors.

### *Hybrid*

Hybrid network architecture, as shown in Figure 9, as the name would imply, is a combination of peer-to-peer and client-server types. Except for the smallest of networks, there is rarely a pure P2P or client-server network, and functionally, all networks offer hybrid service models, depending on needed services. A single node can use services from a server on the network while participating with a peer in a distributed file system also on the network and serving information to a client, all on the same network.

Functionally, network architecture is more than a system of connections among nodes. Modern computing demands have advanced rapidly, and networks require the centralized control of a client-service architecture for some demands, but also need the flexibility of open P2P relationships for other demands.

### *Cloud-based*

In a traditional "on-premise" model, the organization is responsible for all aspects of the network, including owning and maintaining all servers, storage, operating systems, developing, and maintaining applications. Cloud-based services offer an alternative to this model.

According to National Institute of Standards and Technology (NIST), "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" through the internet.[1]

In this model, an organization engages a third-party provider to offer cloud-based services. A cloud-based architecture can combine or simplify some of the network relationships and offers flexibility for the cloud service recipient.

There are three general cloud service types in which the service type may be referred to as "'X' as a service," abbreviated XaaS. XaaS means "delivery or anything as a service: products, services, and technologies." The three general cloud service types include Infrastructure (IaaS), Platform (PaaS), or Software (SaaS). Details on each of these models, compared with the traditional on-premise model include:

- **On-premise –** the organization is responsible for all aspects of the network, including maintaining all servers, storage, operating systems, and developing and maintaining applications.
- **Infrastructure as a Service (IaaS) –** the organization owns the maintenance of servers within the cloud. This is a pay-as-you-go model for network, servers, storage, applications, etc., where the size can be modified on an as-needed basis. The recipient organization is responsible for all logical configurations and maintenance, though they typically do not have access to the hardware. Organizations that desire their own features and functionalities often use IaaS to develop customized applications without the necessity of housing the infrastructure. In this case, the IaaS provider, such as Amazon Web Services (AWS),

1. Peter Mell, Tim Grance, "The NIST Definition of Cloud Computing," NIST Information Technology Laboratory, Computer Security Resource Center, SP 800-145, September 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final.

Microsoft, Google, or IBM, provides a platform on which organizations can quickly develop their applications.

- **Platform as a Service (PaaS) –** provides hardware and software tools (platform) for creating software and applications. This structure is suitable for organizations that want to host and run applications in the cloud without having to manage the infrastructure (i.e., storage, updates, O/S). Providers of PaaS include, among others, Microsoft Google and AWS.
- **Software as a Service (SaaS) –** an application delivered through the cloud available over the internet, usually for a set fee. This model allows the greatest flexibility to the recipient organization. Providers of SaaS include Google Apps, Netsuite, Salesforce.com, ServiceNow, Workday, Dropbox, and DocuSign, among others.

Although external providers use these terms to market and explain their services and approaches, an organization's IT department may also use the terms if they offer such services.

The term "cloud" describes how data and information is stored and accessed over the internet, but simplistically, it is the use of someone else's computer network. The use of the term cloud is a recognition that network architecture is largely irrelevant to most consumers of IT services, from organizational IT systems to individual users. Figure 10 depicts the on-premise and cloud models and the typical corresponding responsibilities. However, some of these responsibilities may vary on a case-by-case basis, and the organization is almost always responsible for user provisioning, access, and authentication.

In general from a responsibility standpoint, an organization is typically responsible for security "in" the cloud, while the cloud provider is responsible for security "of" the cloud.

**Figure 10: Typical Cloud Architecture by Type and Responsibility**

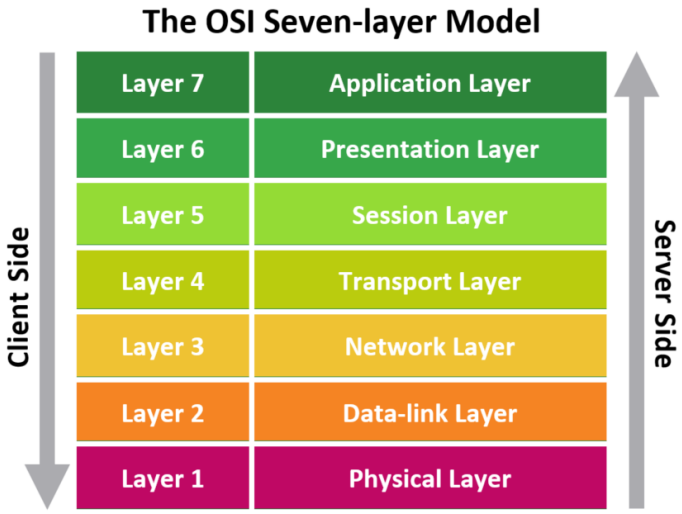
| On Premise | IaaS | PaaS | SaaS |
|---|---|---|---|
| Applications | Applications | Applications | Applications |
| Security | Security | Security | Security |
| Database | Database | Database | Database |
| Operating systems | Operating systems | Operating systems | Operating systems |
| Virtualization | Virtualization | Virtualization | Virtualization |
| Servers | Servers | Servers | Servers |
| Storage | Storage | Storage | Storage |
| Network | Network | Network | Network |
| Data centers | Data centers | Data centers | Data centers |
| Key: | Managed by Company | Managed by Cloud Provider | |

Source: The Institute of Internal Auditors.

### *Layered Service Network Model*

When referencing networks, it helps to conceptualize the different network "layers" using a model. Sometimes collectively referred to as the network stack, the most commonly used network-layered model is the Open Systems Interconnection (OSI) Seven-Layer model, as shown in Figure 11.

Figure 11: The Open Systems Interconnection Model




For more details on the specifics of the OSI Seven-layer Model, see Appendix D and Appendix E.

Like many IT concepts, this model is not universal, but it may be helpful when thinking about services provided by a network stack. Most operating systems provide a network stack that contains a series of applications allowing for remote connections and sending/receiving of data to remote devices. Each layer has a responsibility and operates independently of other layers. Additionally, each layer accepts data from the higher level and performs its required functions before passing it to a lower level. This is referred to as passing information down the "network stack" and allows developers to assume that necessary services will have been provided by lower layers. It also requires that the services they develop provide stable interoperation "up the stack."

Information passed down from a higher layer is most often intact. It can be divided or combined as needed at the new layer because all data from the higher level is simply a field of data. Control information called metadata (data about data) is added; this metadata is usually called a header.

Portions of this guide will reference the different layers.

### *Network Protocols*

The protocol of a network is an agreed-upon format for exchanging or transmitting data between systems (or up and down the network stack). Protocols define a number of agreed-upon parameters, such as the method to compress data, the type of error checking to use, and mechanisms for systems to signal when they have finished either receiving or transmitting data. A simple analogy is a telephone conversation in which the recipient of the call says "hello" when answering the call, and the caller responds, "hello," establishing a voice protocol (speaking in an agreed-upon language).

Some common network protocols include Ethernet, Transmission Control Protocol/Internet Protocol (TCP/IP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Secure Sockets Layer (SSL) Protocol. Simple descriptions of each are available in Appendix F.

Some versions of these protocols have an additional security or encryption, signified by the letter "S," such as SFTP, FTP via Secure Shell connection (SSH), or HTTPS. It is important for an organization to understand the applicable secure protocol requirements in relation to regulations, policies, and governing standards (e.g., NIST, Payment Card Industry [PCI] Data Security Standard [DSS]).

Many IT professionals often speak in terms of the protocols implementing the functions required by the layer. A list of some of the protocols used at each layer is also offered as "protocols (or media) implementing this layer." The example protocols are not exhaustive, but may help identify information resources or equivalencies and provide context. Figure 12 shows some of the common protocols used at each layer.

For example, web services are performed at the HTTP layer (layer 7). In addition, when network components (described in the next section) are discussed, they are often identified as "performing" at a specific layer.

**Figure 12: OSI Model with Example Protocols**

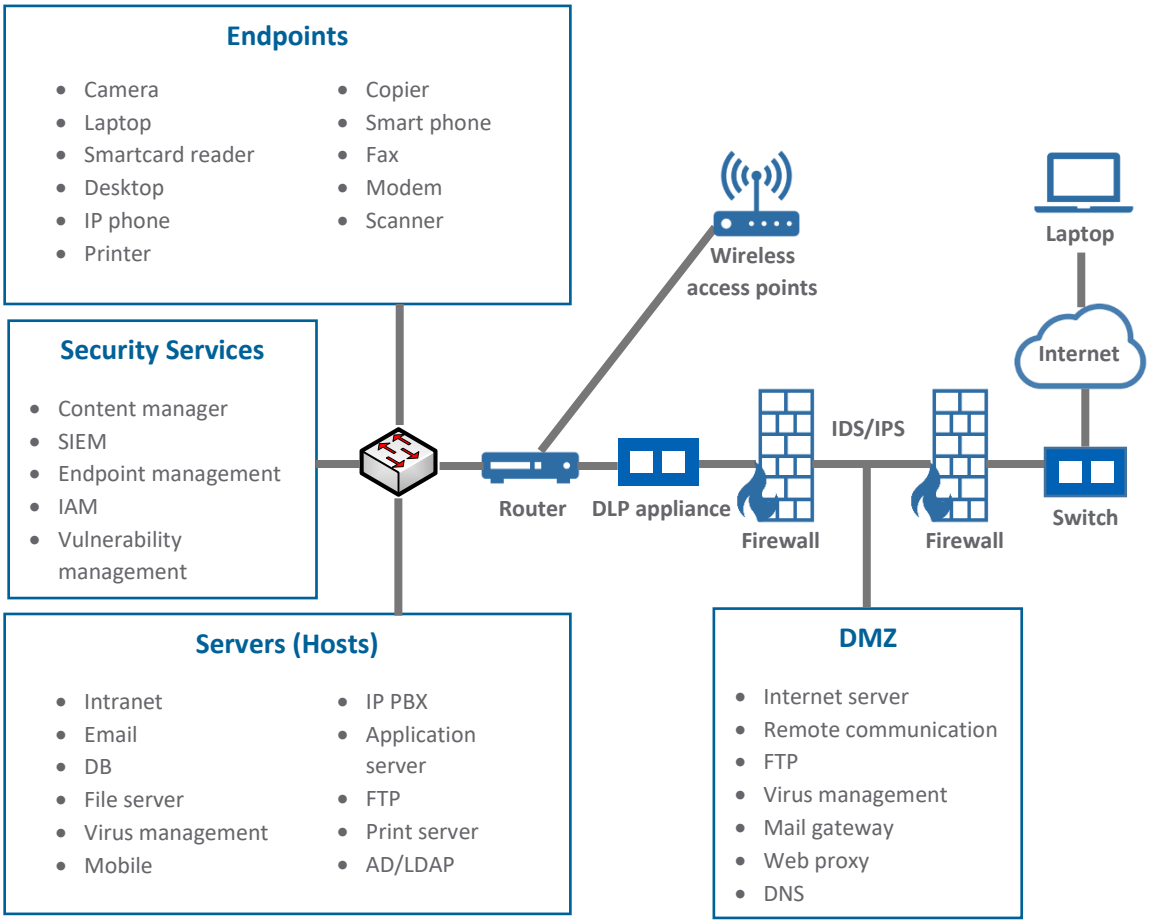
**The OSI Seven-layer Model**

| Layer | Name | Example protocols |
|---|---|---|
| Layer 7 | Application Layer | HTTP, SMTP, POP3, FTP, Telnet, Email |
| Layer 6 | Presentation Layer | SSL, TSL, JPEG, GIF |
| Layer 5 | Session Layer | NetBIOS, SAP |
| Layer 4 | Transport Layer | TCP, UDP |
| Layer 3 | Network Layer | IPv4, IPv6, IPsec, IP |
| Layer 2 | Data Link Layer | Ethernet, PPP, ATM, Fiber, MAC Address, VLAN |
| Layer 1 | Physical Layer | Cables, Connectors, Hubs (T1, ISDN), USB, Bluetooth |

## Network Components and Concepts

A typical network architecture in most organizations would have several of the components featured in Figure 13.

**Figure 13: Typical Network Architecture Components**




Source: Sajay Rai.

## Network Hosts and Nodes

A host or "network host" is a computer or other device connected to the network able to communicate with other hosts. It can be a client or server and may exist as a peer or hybrid architecture, but it will always have an internet protocol (IP) address. As mentioned, a node is defined as any system or device connected to the network, including routers and switches, but a node does not necessarily need an IP address. The host's network software implements various protocols that perform the functions of each layer of the OSI Seven-layer Model. The complete "stack" of network services is available in a host.

### *Routers and Switches*

A router is a Layer 3 (Network Layer) device that transmits data among networks. The data is sent in the form of packets (data packaged to be transferred within a network). Services such as virtual LAN (vLAN), packet filtering firewalls, and other network services can be built into routers.

A switch is a Layer 2 (Data Link) network device that connects nodes within a network with physical media such as copper wires. A switch receives, processes, and transmits data to specific destination devices through frames, which are groups of data similar to packets used in transmission control protocol/internet protocol (TCP/IP) at higher layers. Switches only send messages to the intended nodes. Switch functionality can be included in routers, so the device can be called a switch or router depending on what function is being discussed. Although confusing to some, it is actually helpful because independent switches and routers can have overlapping functions.

Layer 3 switches, or “multi-layer switches," create virtual circuits for transmitting data between nodes. Using a Layer 3 switch reduces network latency because the packet flows through the switch versus having the additional step of going through a router. IT will normally deploy a Layer 3 switch for the corporate internet or to establish a vLAN whereas they would use a router if they need traffic to traverse the WAN. Layer 7 switches integrate routing and switching capabilities, typically used for load balancing among a group of servers. These switches are also referred to as content, web, or application switches.

### *Firewalls*

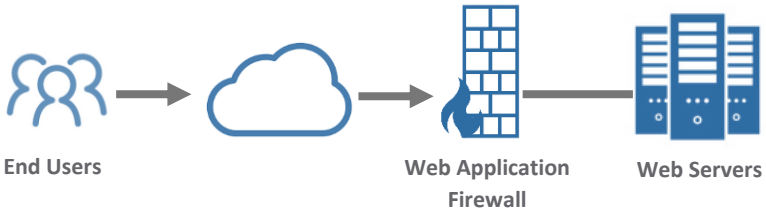
A firewall is a network security system that monitors and controls incoming and outgoing traffic based on predetermined security rules and configuration, and is designed to prevent unauthorized access to and from a private network. Organizations should ensure that firewall access is restricted, and rule sets and configuration of firewalls should be reviewed periodically. Each rule set should have proper documentation for its purpose and identification of its owner/requester.

There are many types of firewalls, each having a specific purpose, and organizations may have several types based on their unique needs. Basic firewalls inspect header information from the network layer (Layer 3) and the transport layer (Layer 4). They are sometimes called packet filters as they remove data coming from forbidden IP addresses (network layer) or destined for forbidden ports (transport layer). If the packet is not blocked, it passes to its destination within the network protected by the firewall.

Stateful firewalls inspect packets and can block potentially malicious ones that are not part of an established connection or fail to fit the rules for initiating a legitimate connection. Application layer firewalls, or next generation (NG) firewalls, intercept packet traffic and decode data all the way up the stack to the application layer (Layer 7).

Mobile firewalls provide secure communications when network access is initiated via a mobile device. Web application firewalls (WAF) analyze traffic moving in and out of an application, and can be placed between web servers and the internet to detect and protect web applications from known web application attacks, as shown in Figure 14.

**Figure 14: Web Application Firewall Placement Example**




Source: The Institute of Internal Auditors.

Additional security can be implemented through configuration to reject destinations with questionable reputations. Security tools, such as firewalls, can intercept packets, inspect header information, or even reconstruct the original data from up the stack to inspect it for security threats.

### *IDS/IPS*

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are devices or software applications that monitor network traffic for indications of compromise or attempted compromise of a system. IDS and IPS rule sets can be very large and each rule may require calibration and threshold setting to ensure system integrity, such as preventing false positives. Well-calibrated and well-monitored IDS and IPS applications can greatly increase an organization's ability to detect and stop attacks.

Alerts generated by an IDS are usually collected in a security information and event management (SIEM) system. Alerts can be correlated with network traffic flow information (net flows) and perimeter security tools such as firewalls. IDS alerts are compared against IPS rules; if there is a match, the IPS and/or the data/information leakage prevention (DLP/ILP), software designed to detect potential data breaches will execute a rule to stop an activity from taking place.

#### ***Wireless Access Points (APs)***

A wireless access point (AP) provides wireless access to a network. Modern APs provide options for encryption, or scrambling and securing data transmitted, but because the technological world is advancing so rapidly, systems often fail to keep up with bad actors who attempt to override encryption features for their own – usually (or often) criminal or malicious – purposes.

Corporate environments achieve wireless network access by broadcasting radio signals between hosts and access points. An AP provides a range of options for the Layer 1 architecture of wireless service. Depending on the age of equipment used, several types of encryption may be used, or an organization may choose not to use encryption. However, this can expose the organization to additional risk, and it is a relatively inexpensive cost to upgrade wireless network components, in order to increase security.

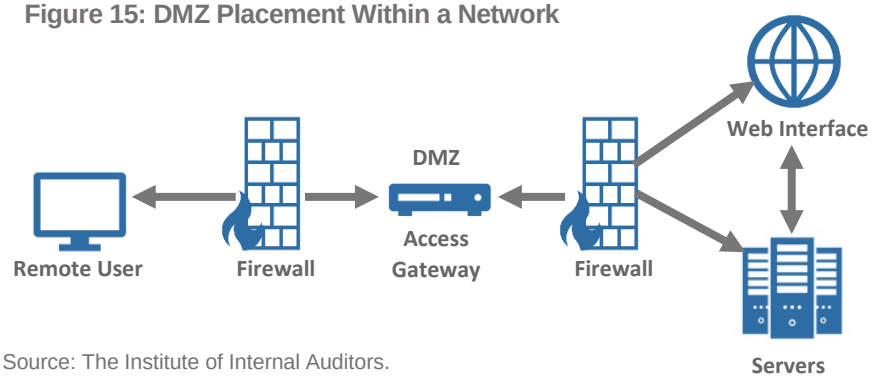
Upgrading equipment or configuration of the entire user base to use newer encryption protocols can be a very large task. Here is a brief list of various wireless encryption protocols, from least encryption to most.

- **WEP (Wired Equivalent Privacy) –** an outdated security protocol that offers basic encryption. This protocol is typically used because it may be the only option for older infrastructures. From a security standpoint, given sufficient traffic and even marginal computing power on a laptop or mobile device, WEP is easily penetrated and was superseded by the WPA protocol by the Wi-Fi Alliance in 2003.
- **WPA (Wi-Fi Protected Access) –** replaced WEP as a more secure security protocol for wireless networks. Like WEP, WPA should only be used if required by older infrastructure because it is vulnerable and provides less encryption than its successors.
- **WPA2 (Wi-Fi Protected Access 2) –** security protocol currently required on all devices considered Wi-Fi CERTIFIED by the Wi-Fi Alliance, providing stronger encryption algorithms than predecessors. It provides a degree of security from unauthorized access.
- **WPA3 (Wi-Fi Protected Access 3) –** provides individual data encryption, secures some "internet of things" (IoT) devices, protects against brute force (trial and error approach), dictionary attacks (using dictionary words to guess passwords), and offers the highest current level of encryption.

### *DMZ: A Security Application*

A demilitarized zone (DMZ) is a portion of network contained between two firewalls and protects the organization's external-facing servers. The first firewall is "outward facing" or subject to the internet, and protects the DMZ systems. The outward facing firewall has more exposure than the second firewall, which protects the interior network. Figure 15 shows an example of DMZ and its placement.

**Figure 15: DMZ Placement Within a Network**




Source: The Institute of Internal Auditors.

### *Remote Network Access*

Numerous remote access options are available to organizations, determined by factors such as security requirements, user expectations, technical capabilities, and business needs. The need to access corporate networks is a result of today's workforce becoming more mobile; to remain productive, users require constant network access. This may even require connection from an unsecure public network, such as a public access point.

A majority of solutions deployed by organizations require some form of security to ensure that remote connections are secure. The security controls are usually in the form of multi-factor authentication (MFA) (sometimes referred to as two-factor authentication (2FA)) or encryption, or

both. MFA/2FA means that in addition to entering a password, a user must enter a token or a passkey that refreshes periodically (e.g., a one-time multi-digit number or "token" is sent to a remote user's mobile phone that must be used to complete a user's access to an organization's system).

### *Remote Access: Virtual Private Network (VPN)*

A VPN extends a private network across a public network and enables users to send and receive data as if they were connected over a private network. It provides the benefits of functionality, security, and management characteristics of a private network. Organizations should ensure that all VPN access is verified and authenticated to prevent unauthorized remote access to the organization's network (e.g., MFA).

Remote access inherently presumes an insecure Layer 2 through 4 connection. When using a VPN, before data is sent, the session layer (Layer 5) provides an encrypted "tunnel" to transfer data. This is an important security measure for the organization, in the event a non-employee gains access to the data, the entire encapsulated contents, and in some cases even the transmission information, are encrypted. The internal system receiving these connections and decrypting the contents are called point of presence (PoP). Due to their role, PoP servers should never be attached to the internet. The most common way to achieve PoP service is by using a VPN to encrypt traffic between the host and the internal network point of presence.

### *Remote Access: Virtual Desktop*

Virtual desktop protocols such as Microsoft's Remote Desktop Protocol (RDP) give users a graphical interface to connect one system (computer) to another over a network connection. The primary use of virtual desktop protocols is to provide technical support and to administer servers that do not have a keyboard/video monitor/mouse attached to them, allowing administrators to operate and maintain servers in a data center.

Both computers must have the same virtual desktop protocol software installed to use this function. To access another computer, a remote user must have both the IP address and the ability to authenticate (e.g., login, offer a security token). For security purposes, virtual desktop protocol software connections are often blocked at the perimeter firewall or in the DMZ.

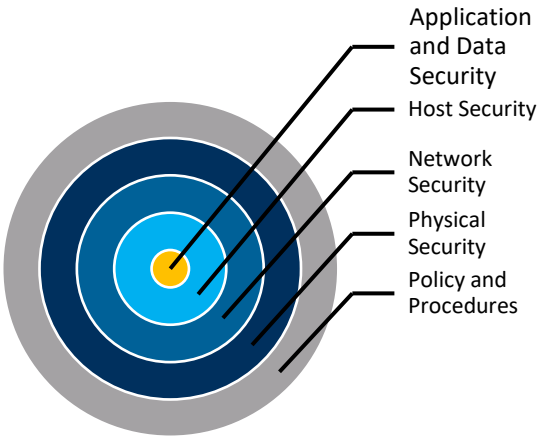
## Network Defense

To fully comprehend network security as it relates to a network's components and architecture, the concept of layered defense or defense-in-depth must be understood (Figure 16). This concept focuses on the premise that no single point of failure should cause the total compromise of security.

### *Layered Defense or Defense-in-depth*

This concept ensures there are multiple layers of controls before a potential intruder can access sensitive information. Usually, these layers of controls exist across a network, servers, applications, and databases. This concept also ensures that appropriate physical controls are in place. The overall concept is governed by appropriate policies and procedures.

**Figure 16: Layered Defense-in-depth Model**




Source: The Institute of Internal Auditors.

The concept of defense-in-depth is similar to how castles were protected during medieval times, when multiple controls or barriers protected the crown jewels as well as the inhabitants. A similar philosophy exists today to define cyber controls across various layers of the cyber environment.

- The internet is outside of the castle gate.
- The castle gate is the firewall rule (outward facing).
- The walls, moat, and courtyard are the DMZ.
- Watchtowers are security IDS/IPS, DLP, email, and web gateways.
- The inner door to the castle is the internal-facing firewall.
- The rooms of the castle are the segmented network.

## Network Challenges and Risks

Networks have many components and each organization will have a unique network structure. Having an effective network can significantly impact an organization's operations. An internal auditor's understanding of the network architecture is key to understanding the risks and challenges associated with the networks.

There are numerous challenges/risks related to an organization's network that internal auditors should be aware of, which can include but are not limited to:

- Ensuring proper identification of all external-facing services provided by the organization.
- Ensuring sufficient network security.

    - Ensuring that network components are secured and configured according to organizational policies that are aligned to applicable regulations and industry best practices.
    - Monitoring the dark web for compromised emails/passwords and verifying that passwords are changed frequently.
    - Ensuring appropriate anti-malware and anti-phishing software are deployed.
    - Conducting mandatory employee awareness training for anti-malware and anti-phishing software.
- Ensuring appropriate access.
    - Ensuring that access to switches is restricted and that technicians routinely maintain and update them for functionality.
    - Ensuring that physical access to routers is restricted. Routers almost always have remote access capabilities for the devices themselves. These should be secured with strong passwords and monitored for failed login attempts.
    - Verifying that remote users are required to use two-factor authentication.
- **Ensuring patch maintenance.** Ensuring the latest security patches and firmware updates are installed on network components (e.g., firewalls, routers, printers, and Voice over Internet Protocol (VoIP) phones).
- **Ensuring appropriate management of third-party network risks.** This is applicable if network management is outsourced and if so, ensuring the vendor's security programs are robust, efficient, effective, and accessible.

# Applications

## Application Architecture

**Application architecture involves the design and behavior** of an organization's applications and focuses on their interaction with other applications and with data and users in support of business cycles and functions. An organization's architecture should be designed in alignment with its requirements and business strategy, and have proper controls to ensure completeness, accuracy, and authorization.

### Resources

For more information on IT general controls, see IIA GTAG "Information Technology Risk and Controls, 2nd Edition."

For more information on application controls, see IIA GTAG "Auditing Application Controls."he cover, logo, and references in this guide have been updated. The content has not changed.

Considerations should include interaction among application packages and users, data integration, and how systems are designed to work together with the network and infrastructure. Within architecture, the scalability and capacity of applications should be a consideration because of potential business growth, change in organizational priorities, and other factors. Consideration for the extent of business fluctuation raises potential integration problems or gaps in functional coverage. For planning purposes, strategies can be developed to identify systems that may be functional now but at-risk to sustain the pace of change and the need for data integrity, reliability, or availability.

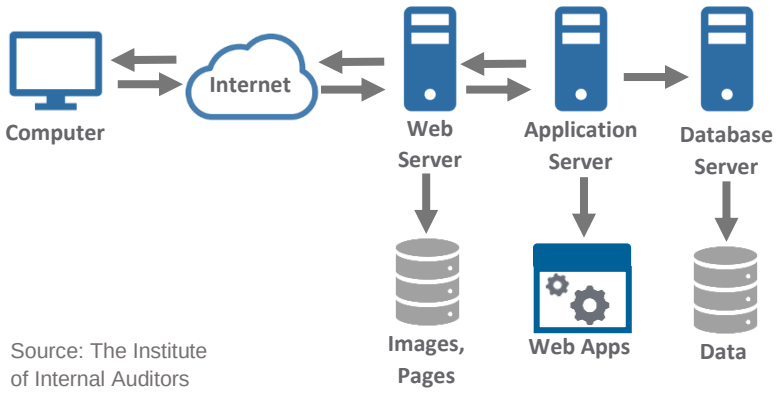
Understanding an organization's application architecture allows internal auditors to appreciate how multiple applications are strategically aligned to accomplish a business operation. For example, a cloud-based platform may combine multiple technologies and SaaS-provided applications to deliver a specific business process. Management would then design a combination of application controls, IT general controls, and ongoing monitoring sufficient to address applications managed both on premise and off premise (potentially by third-party service providers).

#### *Web or Internet Applications*

Application architecture for web applications usually requires a web server that is accessible from the internet, and which usually resides in the DMZ. Scripting languages used to write application source code include Java, C, Python, Ruby, PHP, and others. Examples of web applications includes sites such as www.amazon.com or www.rakuten.co.jp. Any user with internet access can reach these applications. The web server usually only handles the interface with the user over the internet.

From the architecture perspective, the web server usually "talks" to an application server that performs the application's major functions. The application server interfaces with the database where information is stored, which is usually housed in a database server. Based on the application, database servers may contain sensitive or critical information related to the application (e.g., credit card information, health information, or a user's personal information), and therefore must be secure and appropriately access-controlled. This database resides in the inside network, inaccessible from the internet for control and security purposes. Only the application server can connect to the database, and only the web server can connect to the application server through a secure connection, as shown in Figure 17.

**Figure 17: Typical Web Application Architecture**




Source: The Institute of Internal Auditors

In many organizations, the web application architecture will also include a web application firewall (WAF, as shown in Figure 14), to identify, detect, and prevent web application attacks such as SQL injection or cross-site scripting (XSS). Such attacks may be successful if a web application running on a web server is not coded securely. Rather than reviewing all web applications, an organization can deploy a WAF to prevent the web application attacks.

### *Application Program Interfaces (APIs) and Web Services*

APIs and web services are pieces of code designed to interface with other pieces of code and describe how two applications communicate. These allows an organization's applications to interact with other applications within or outside the organization. Accordingly, web and mobile applications rely heavily on both web services and APIs. One main differentiator between an API and a web service is that APIs work with a variety of communication protocols. Because these interfaces can be critical to an organization's business functions, the organization should inventory all APIs and web services in use. The uses should be a part of API documentation, and APIs should be included in an organization's patch management process.

### *Internal Applications*

Internal-facing applications are primarily accessed through an organization's internal network or via their VPN. Only users signed on to the internal network can access these applications. In this case, the typical architecture comprises an application server, a database server, and a database. The architecture is usually less complex compared to a web application.

### *Cloud Applications*

Due to potential cost and time savings, as well as ease of implementation, many organizations are willing to forego some application features and adapt to the features provided by different cloud applications (see the Network Architecture section for details on the different types of cloud service models). This allows organizations to forego developing applications in-house or purchasing off-the-shelf software from vendors. In many cases, the cloud application cost is cheaper than developing an application in-house, but each organization should determine if selected cloud applications can fulfill the organizational and regulatory requirements.

Due to their focus on specific services, cloud applications often put an organization in a better position to reduce internal hardware and network resource costs versus maintaining their current IT infrastructure. Utilizing the cloud can also provide the organization with a competitive advantage over their competition when it comes to deploying emerging technologies.

## Application Development and Maintenance

For some organizations, application development may be a core competency that helps them meet their strategic objectives. Application development involves creating and integrating programs that can facilitate business processes, automate control activities, and advance efficiency. Applications connect with the organization's network and infrastructure and carry out the business logic intended by the process. Software programs can have embedded application controls to address risk related to accuracy, completeness, and authorization.

Applications and software have been traditionally developed using the waterfall project management method. A simple way to think of the waterfall method is to consider the way housing is developed. A house is designed, built, and inspected before a certificate of occupancy is granted. This can sometimes be inefficient.

Application and software development can take a more incremental approach, which can address the potential delay in deliverables. Rather than delivering an entire product at once, a method known as Agile (or adaptive software development) is now often used. With this method, there is still a blueprint and a known final outcome — as there is for a house — but one deliverable at a time can be developed or built, in what are referred to as sprints. Using the analogy of building a house, the Agile method of software development would be like following the blueprint, building, inspecting, and granting of a home's occupancy one room at a time, but instead for delivering a unit or section of an entire application or project.

The Agile method can be effective in application development, given the waterfall approach requires all the in-between steps to be completed before delivering the final product.

Agile, properly implemented, has created a new software development and testing process referred to as DevOps (a combination of the words development and operations) or DevSecOps (development, security, and operations). Using this method, an organization does not need to know the final product because it is based on program vs. project management. The focus is more customer-centric, building one feature at a time. This may address frustrations that come with waiting for complete project deliverables.

Regardless of which project management methodology is followed, three activities must be accomplished to develop a reliable application:

1. Strategic planning and design.
2. Development and testing.
3. Implementation and maintenance.

Practicing a disciplined application development approach strengthens an organization's capability maturity from an ad hoc manual activity to optimized systematic practices. Done well, application development can have a positive impact by:

- Enhancing ongoing engagement with external (e.g., customer and supplier) and internal (e.g., direct report and cross organizational) relationships.
- Determining data integrity, through logic and business rules that ensure data is authorized, complete, and accurate.
- Ensuring information is available and communicated timely to take decisive action.

A structured approach will help accelerate transformative change in a controlled way:

- Access controls safeguard the transition from strategic design through code development and implementation.
- Protecting source code advances the application changes as approved by management.
- Robust testing gives assurance that the design functions with reliability, and operates with interdependent technologies, according to management's expectations.
- Documentation and training provide for the suitable and consistent use of the application.

Ongoing maintenance keeps applications fit-for-purpose and ensures system availability, security, and integrity.

***Changes to applications and controls***

Whether computer programs are developed internally or by others to the organization's specifications, controls are necessary to ensure that application changes are designed appropriately and implemented effectively. This protects an application's production (live) environment.

## Resources

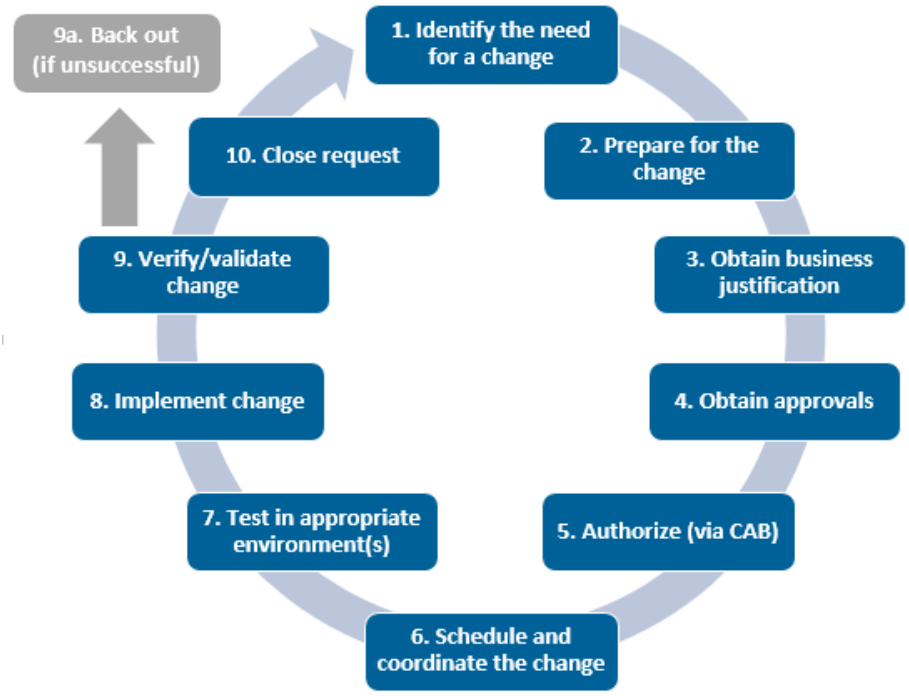
For more information on change management in relation to applications, please see IIA GTAG "IT Change Management: Critical for Organizational Success, 3rd Edition."

Changes should follow management's change protocols. Each should be requested, scoped, and approved by the appropriate business function. Change initiatives should be evaluated for benefit and priority and tracked with a service order or ticket number. The impact and risk posed by the change should be considered when scoping the effort and timing of the project, and appropriate resources with expertise should be assigned to carry out the change.

Change requests should be designed based on documented requirements directed by the appropriate business unit, and proper segregation of duties controls should exist throughout the

process. Sequential steps should be followed in the evolution of a needed change, as shown in the example in Figure 18.

**Figure 18: Sample Steps in a Change Process**




Source: The Institute of Internal Auditors.

Robust testing ensures the quality of the information affected by the change. Changes should be developed and tested in nonproduction environments, such as a development or test (DEV and TEST) environment first by IT then provided to the business unit for acceptance testing. A user acceptance test plan is developed by end-users who have experience with the process being tested, and should identify key business activities or functions affected by the change. These factors can contribute to developing an effective user acceptance test plan:

- Participation by the application and business unit representatives with direct knowledge of the application and data to be tested.
- Clearly stated objectives and event-driven test scenarios based on the business activity cycle, including high-risk activities (e.g., potential revenue loss/interruption or legal issues).
- A set of required test conditions for the business scenario, rather than conditions based on variations of a software program.
- A set of predetermined test results for the test plan.
- Defect tracking and resolution.
- Diligence monitoring techniques to follow subsequent to the production (PROD) move.
- Interrelationships and impacts with other applications.

Ultimately the organization's management ensures the appropriate level of documentation and authorizes the change that affects the application's production environment on the basis of test results. The approved source code then moves into production by an independent function from a staging environment that mimics production activity. The change should be formally accepted by the business unit requester subject to their due diligence (i.e., diligence monitoring might include validating a series of consecutive processing cycles without error).

A simple depiction of the migration of a proposed change through the appropriate environments is shown in Figure 19.

**Figure 19: Example of an IT Change Migration**


*Note:* The migration through each of these environments should be properly segregated.
Source: The Institute of Internal Auditors.

Business users are usually restricted to their online production environment; programmers and developers are restricted to their test environment. Movement into production environments should be performed independently to ensure version control.

Emergency changes should be few and still require the same level of documentation and testing. In some instances, the approval to run an emergency change in production may be obtained after the fact, but within a reasonable and formally established timeframe (e.g., two business days).

## Applications Challenges and Risks

Functioning and efficient applications are key to every organization's success. The design and maintenance of application architecture, development of new applications, and changes to existing applications should be efficient and effective processes owned by management and understood by internal auditors. Appropriately operating controls across these functions can be the difference between an effective or ineffective process.

Regarding application architecture, internal auditors should have an enterprisewide view of third-party service providers, cloud technology risk, and suitable controls that are significant to business process operations and delivery.

There are numerous challenges/risks related to an organization's applications that internal auditors should be aware of, which can include but are not limited to:

- **Unclear planning/accelerated timeframes.** When application development efforts fail, it is often due to unclear planning and/or an accelerated timeframe that leads to insufficient design. If the frequency of change increases, development teams may accelerate implementation outside of documented protocols and without giving priority to strategic architecture and planning.

- **Multiple service providers.** Working with multiple software service providers may further complicate data management as information flows from one application to another.

The following risk factors, related to application changes, are categorized by three root causes: informal methodology, incorrect logic, and increasing volatility. Addressing the root cause may correct symptomatic exceptions and promote remediation:

***Informal Methodology/Ad Hoc Changes***

- Unrealistic ROI expectations inhibit submission of emerging ideas.
- Ambiguous system requirements.
- Changes applied to the wrong version of source code.
- Recurring changes to the same program/application.
- Delays in delivery of the solution.
- Unconsidered inter-relationships during an emergency change.
- Lack of user involvement during testing.
- Lack of user review and diligence subsequent to applying the change.

***Incorrect/Poor Logic Designed into Programs***

- Business-critical applications that are changed in-house as an interim fix.
- Errors introduced as a result of delivering a change based on an incomplete understanding of the solution.
- Unrestricted access to source code.
- Lack of change control and monitoring tools.
- Insufficient testing.

***Increasing Volatility of the Application***

- Growing frequency of changes and interruptions in service due to maintenance (applications that change every week).
- Growing volume of changes (applications that draw the most maintenance).
- Increasing the quantity of key reports, and the changes made to key reports.
- The number of emergency changes that occur.

# Additional and Emerging IT Topics

**This section will discuss some additional fundamental and emerging IT topics** at a high level. It is important to understand that these additional topics are dynamic, not static, and the list is not exhaustive. The topics covered in the previous sections were once considered as emerging IT topics and have over time become ubiquitous and essential to organizations. The same applies to the several topics in this section; they may one day become commonplace processes for all organizations.

As new IT topics surface and existing topics evolve, keeping informed and applying professional skepticism remains crucial for internal auditors who strive to stay relevant and in conformance with The IIA's *International Standards for the Professional Practice of Internal Auditing*.

## Data Management

In many organizations, applications are developed or obtained/used in silos, and it can be difficult to verify the integrity of data used and produced by the applications. Data integrity relies on many variables, such as the source(s) of data input into the application, the logic used by the application to produce the data, and the accuracy of the data produced by the application.

One reason data quality may be insufficient is that organizations often gather or acquire data from various sources. As this data is input to an organization's various applications over time, due to the sheer volume, the quality can deteriorate. In addition, if the format of data collected is different for each collection method, the resulting data may be compromised. It is important to have front-end controls to ensure uniform formatting.

Examples of data input issues include:

- Data entry mistakes.
- Data inaccurately stored within applications.
- Data formatting is incorrect.

Once applications (which may have been developed in silos) are incorporated in key business processes, users become dependent on these applications and data, even though in some cases, this data may not be reliable.

The potential poor quality, lack of integrity, and inability for organizations to rely on their data may cost millions of dollars. Recent estimates indicate an average organization may suffer losses of

$15 million a year based on poor data quality, and the U.S. economy may suffer losses exceeding $3 trillion annually.[2]

The challenges and risks associated with enterprise data management can also depend on the culture of the organization and its structure (factors such as if it is decentralized vs. centralized). The more the organization's individual divisions operate in silos, the more difficult it is to have an effective enterprise data management strategy.

Other factors that could potentially affect data management include but are not limited to:

- Inaccurate or incomplete data and information asset inventory.
- Lack of enterprise data management policies.
- No one individual responsible for or capable of handling the organization's enterprise data architecture.
- Poor sources of data.
- Lack of procedures to identify the applications and systems that have data quality issues and
- lack of procedures to initiate projects addressing the issues.

Potential adverse outcomes from poor data management include:

- Customer displeasure when their data is inaccurately reflected in organization's systems and applications.
- Regulatory fines and/or penalties.
- Data breaches.
- Potential impact on an organization's profitability.

## Data Analytics

Data analytics can be used to identify trending key indicators to help management see how well processes and controls are operating. More importantly, analytics may show ongoing degradation of processes and controls that may prompt expedited corrective action. As organizations mature, data analytics strongly impacts the way they can assess and compile relevant information for decision making and monitoring key risks.

### Resource

The IIA GTAG "Data Analytics Technologies" provides insight on assessing the maturity level of data analysis usage, with a focus on increasing the levels of assurance and other value-added services.

At the same time, data analytics has also increased in importance as a technique that the internal audit activity may apply when executing audits. A formal data analytics program can be useful in supporting an audit function in becoming more effective, more efficient, easily scalable, and significantly reducing auditing errors while providing greater audit and **fraud** risk coverage. Data

2. Kaerrie Hall, "Customer Data Quality: The Good, the Bad, and the Ugly," Validity, September 5, 2019. https://www.validity.com/blog/customer-data-quality/.

analytics programs can provide long-term continuous auditing or monitoring around legal and compliance issues as well as the ability to perform ad hoc audit testing, business review, and assist with potential fraud investigations.

For both business and internal audit, data quality can remain a challenge. While applying analytics to structured data sets (e.g., SQL tables) may be advanced in some organizations, applying data analytics to unstructured data sets (e.g., spreadsheets or emails) can be of special interest to organizations as it may provide additional key insights.

## Social Media

Social media comprises a set of technologies and channels targeted at forming and enabling a potentially massive community of participants to productively collaborate. Examples of social media platforms and channels around the world include Facebook, LinkedIn, YouTube, Twitter, Instagram, QQ, Wechat, WhatsApp, and many more.

Risks organizations face in this realm range from not adopting social media (e.g., brand/image, missing out on customer interaction), reputational damage from misleading or incorrect information postings, security risk, violation of privacy/confidentiality regulations, loss/theft of intellectual property, and exposure of trade secrets. For example, a disparaging statement made about a competitor by an employee could result in a potential lawsuit against the organization, or a comment made by an employee related to another employee could be construed as harassment resulting in a lawsuit. Accordingly, organizations should understand their social presence and monitor each channel in which they are present.

Organizations should have a social (digital) presence policy and procedures regarding the manner in which social media sites are managed. Policies should also address employee behavior in regard to social media. Organizations should ensure employees are aware of these policies, as misuse of social media could have a drastic effect on the entity's reputation.

## Robotic Process Automation

Robotic process automation (RPA) refers to software that can be programmed to perform tasks across applications, similar to the way that humans would. A software robot (bot) can be taught a workflow with multiple steps and applications, such as evaluating received forms, sending a receipt message, checking forms for completeness, filing forms in folders, and updating spreadsheets with the name of the form, the date filed, and so on. RPA software is designed to reduce or automate repetitive, simple tasks.

Use of RPA differs greatly depending on desired outcomes. Organizations may differ by strategic use (automation at the core vs. automation using RPA), numbers of platforms in use (one platform vs. multiple platforms), types of bots in use (attended bots are initiated by a dialogue user whereas unattended bots are scheduled to run automatically), and more.

Like any new technological innovation, there are benefits and risks of RPA. Organizations should weigh each individually before embarking on an RPA strategy. Benefits may include but are not limited to:

- **Improved employee morale –** employees may be freed from conducting repetitive tasks.
- **Productivity –** automating simple tasks allows employees to increase productivity in other areas.
- **Reliability –** with proper programming, RPA may produce more dependable results.
- **Consistency –** bots can be programmed to work nonstop and perform repeatable processes, ensuring consistent results over time.
- **Non-invasive technology –** disruption to existing systems isn't an issue.
- **Compliance –** audit trails can be documented to satisfy regulatory requirements.
- **Low technical barrier –** configuration is relatively simple.
- **Accuracy –** bots are less prone to human error.

Risks may include, but are not limited to:

- **Segregation of duties issues –** bots may have excessive authority.
- **Poorly scripted processes –** as with any computer program, attention must be paid to what the bot is being requested to do.
- **Existing process not improved before being automated –** if a process was flawed before automation, simply transferring the same rule set to an automated program will continue to produce flawed results.
- **Poor monitoring of bots and administrators –** though automated, bots need occasional maintenance, and administrators should be kept apprised of new processes, compromised output, etc.
- **Cyberattacks –** anything in the IT environment is subject to cyber issues. Bots are no exception.

## Machine Learning and Artificial Intelligence

Cognitive automation combines advanced technologies such as natural language processing (NLP), artificial intelligence (AI), machine learning (ML), and data analytics to mimic human activities such as inferring, reading emotional cues, reasoning, hypothesizing, and communicating with humans.

The value goes beyond the ability to automate business processes; cognitive automation may also serve to augment what humans do, making employees both more informed and more productive. Within cognitive automation, there is an important difference between learning and reasoning. Learning is about recognizing patterns from unstructured data and the correlated automation is based on accuracy ratings. In contrast, hypothesis-based reasoning is based on confidence ratings.

Risks related to cognitive automation include but are not limited to:

- Bad practices can be interpreted as acceptable by AI.
- Poor understanding by designers is reflected in systems.

- Systems being compromised and taken over by bad actors.
- Potential for malware to be embedded in learning engines, which could skew the results of machine learning and potentially impact processes.

## Internet of Things (IoT)

Growing pressure to increase the efficiency and quality of operational processing continues to drive efforts to advance digitalization and automation. From these efforts, the internet of things (Figure 20, sometimes referred to as “connected devices”) has emerged, which extends internet connectivity into physical devices and everyday objects, such as TVs, wristwatches, refrigerators, doorbells, thermostats, cars, and so many more.

**Figure 20: Internet of Things**


Source: The Institute of Internal Auditors.

While devices communicate and interact with each other over the internet, they can be monitored and controlled remotely. The ability of machines and systems to interface and exchange information without human intervention expedites efforts around digitalization and automation.

Alongside the perceived significant benefits, challenges will inherently arise due to the rapid pace of change. From a risk perspective, due to the sheer prevalence of devices and their connectivity, the underlying security component is imperative. Organizations must have an understanding of all connected devices, both company-owned and employee-owned, and understand the unique risks associated with each.

## Challenges for Additional and Emerging IT Topics

Technologies are emerging and evolving faster than ever. Regardless of an organization’s maturity level using the technologies reviewed in this section, internal audit’s knowledge of them

and early involvement in their implementation is imperative. This could identify potential risks that may occur and better equip the organization to address them. Numerous risks must be considered including operational, compliance, and reporting. Other challenges and risks may include but are not limited to:

- Lack of understanding the technology/concept/tool.
- Lack of understand changes in the process associated with the technology/concept/tool.
- Insufficient planning for implementation, maintenance, or changes to the technology/-concept/tool.
- Lack of inclusion of the new technology/concept/tool in the risk assessment.

What is audited typically does not change with new technology, tools, automation, etc.; rather, how the audit is performed based on the change in inherent and residual risk must be considered. For example, IT general controls (e.g., access, change, backups) still exist, so existing control frameworks are all still applicable (e.g. Center of Internet Security [CIS], Cloud Security Alliance [CSA], or NIST 800-53). Audits of emerging areas still face operational risks, reporting risks, as well as compliance risks. A holistic view on risks is fundamental.

In addition to understanding technologies an organization is using, internal audit may leverage some emerging technologies for their own uses (e.g. using data analytics or RPA to assist in their sampling process, or to implement continuous auditing).

# Conclusion

Technology drives every organization in today's world. Internal auditors will need more tools, talents, and skills than ever before to remain relevant, to continue providing assurance to their organizations that systems are running as they should and controls are in place. The fundamentals of internal auditing – risk-based assessments, planning, communicating, and continual learning – are as important as ever.

Internal auditors should remain agile and ready for changes in business models as organizations adopt advances in technology. They should be nimble enough to grow along with the organization and foster good working relationships with their fellow business units and departments to be progressive in partnering to face challenges that lie ahead. To remain relevant, to add value, and to offer protection to their organizations, it will be crucial for internal audit to keep up with change.

# Appendix A. Relevant IIA Standards and Guidance

The following resources were referenced throughout this practice guide. For more information about applying The IIA's *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

| Code of Ethics |
| --- |
| **Principle 4 – Competency** |
| **Standards** |
| **Standard 1100 – Independence and Objectivity** |
| **Standard 1200 – Proficiency and Due Professional Care** |
| **Standard 1210 – Proficiency** |
| **Standard 2230 – Engagement Resource Allocation** |
| **Standard 2340 – Engagement Supervision** |
| **Guidance** |
| **GTAG "Auditing Application Controls," 2009.** |
| **GTAG "Auditing IT Governance," 2018.** |
| **GTAG "Data Analysis Technologies," 2011.** |
| **GTAG "IT Change Management: Critical for Organizational Success, 3rd edition," 2020.** |
| **GTAG "Information Technology Risk and Controls, 2nd Edition," 2012.** |

# Appendix B. Glossary

All terms identified here are taken from The IIA's *International Professional Practices Framework* "Glossary," 2017 edition.

**add value** – the internal audit activity adds values to the organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management, and control processes.

**board** – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

**chief audit executive** – describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

**engagement** – a specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

**fraud** – any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

**governance** – the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

**information technology governance –** consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.

**internal audit activity** – a department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

**risk** – the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

**risk management** – a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

# Appendix C. Acronym Guide

These are acronyms commonly used in the IT industry and appear throughout this guidance.

| Common IT Acronyms | |
|---|---|
| **Acronym** | **What it stands for** |
| **2FA** | **Two Factor Authentication** |
| **ACL** | **Access control list** |
| **AD** | **(Microsoft's) Active Directory** |
| **AI** | **Artificial intelligence** |
| **AP** | **Access point** |
| **API** | **Application program interface** |
| **ARP** | **Address Resolution Protocol** |
| **ATM** | **Asynchronous Transfer Mode** |
| **AWS** | **Amazon Web Services** |
| **B2B** | **Business to business** |
| **B2C** | **Business to consumer** |
| BYOD | **Bring your own device** |
| **BYOT** | **Bring your own technology** |
| **CDO** | **Chief data officer** |
| **CIO** | **Chief information officer** |
| **CIS** | **Center for Internet Security** |
| **CISO** | **Chief information security officer** |
| **CPO** | **Chief privacy officer** |
| **CTO** | **Chief technology officer** |
| **DB** | **Database** |
| **DLP** | **Data leakage prevention** |
| **DMZ** | **Demilitarized zone** |
| **DPO** | **Data protection officer** |
| **DNS** | **Domain name system** |
| ERP | Enterprise resource planning |
| **FTP** | **File Transfer Protocol** |
| **GUI** | **Graphical user interface** |
| **HTTP** | **Hypertext Transfer Protocol** |
| **HTTPS** | **Hypertext Transfer Protocol Secure** |
| **IaaS** | **Infrastructure as a Service** |
| **IAM** | **Identity and Access Management** |
| **ICMP** | **Internet Control Message Protocol** |
| **IDS** | **Intrusion detection systems** |
| **(The) IIA** | **The Institute of Internal Auditors** |
| **ILP** | **Information leakage prevention** |
| **IMAP** | **Internet Message Access Protocol** |
| **IoT** | **Internet of Things** |

| | |
|---|---|
| **IP** | **Internet Protocol** |
| **IP PBX** | **Internet Protocol private branch exchange** |
| **IPS** | **Intrusion prevention system** |
| **IPSec** | **Internet Protocol Security** |
| **IS** | **Information Security** |
| **IT** | **Information Technology** |
| **KPI** | **Key performance indicator** |
| **KRI** | **Key risk indicator** |
| **LAN** | **Local area network** |
| **LDAP** | **Lightweight direct access protocol** |
| **MAM** | **Mobile application management** |
| **MAN** | **Metropolitan area network** |
| **MDM** | Mobile device **management** |
| **MFA** | **Multi-factor authentication** |
| **ML** | **Machine learning** |
| **MTA** | **Mail (or Message) Transfer Agent** |
| **MU** | **Mail User** |
| **MUA** | **Mail User Agent** |
| **NG** | **Next Generation** |
| **NIST** | **National Institute of Standards and Technology** |
| **NLP** | **Natural language processing** |
| **NoSQL** | **Not Only SQL** |
| **OLTP** | **Online transaction processing** |
| **OS** | **Operating system** |
| **OSI** | **Open Systems Interconnection** |
| **OSS** | **Operating systems software** |
| **P2P** | **Peer-to-peer** |
| **PaaS** | **Platform as a Service** |
| **PHP** | **Personal Home Page (Hypertext Processor)** |
| **PoP** | **Point of presence** |
| **POP** | **Post Office Protocol** |
| **PPP** | **Point-to-point Protocol** |
| **PPTP** | **Point-to-point Tunneling Protocol** |
| **RDBMS** | **Relational database management systems** |
| **RDP** | **Remote Desktop Protocol** |
| **RFP** | **Request for proposal** |
| **ROI** | **Return on investment** |
| **RPA** | **Robotic process automation** |
| **SaaS** | **Software as a Service** |
| **SFTP** | **Secure File Transfer Protocol** |
| **SIEM** | **Security information and event management** |
| **SLA** | **Service level agreement** |
| **SMTP** | **Simple Mail Transfer Protocol** |
| **SNMP** | **Simple Network Management Protocol** |
| **SQL** | **Structured Query Language** |
| **SSH** | **Secure Shell** |
| **SSL** | **Secure Socket Layer** |
| **TCP** | **Transmission Control Protocol** |
| **TLS** | **Transport Layer Security** |

| | |
|---|---|
| **TUI** | **Text user interfaces** |
| **UDP** | **User Datagram Protocol** |
| **USB** | **Universal Serial Bus** |
| **vLAN** | **Virtual Local Area Network** |
| **VM** | **Virtual machine** |
| **VMM** | **Virtual machine monitor/ manager** |
| **VoIP** | **Voice over Internet Protocol** |
| **VPN** | **Virtual private network** |
| **WAF** | **Web application firewall** |
| **WAN** | **Wide area network** |
| **WEP** | **Wired Equivalent Privacy** |
| **WPA** | **Wi-Fi Protected Access** |
| **WPA2** | **Wi-Fi Protected Access 2** |
| **WPA3** | **Wi-Fi Protected Access 3** |
| **XaaS** | **“X” as a Service** |
| **XSS** | **Cross-site scripting** |

# Appendix D. OSI Seven-layer Network

The appendix provides the details of each of the seven layers of OSI Seven-layer Network model, as shown in Figure 11 of this guidance.

## Description of the OSI Seven-layer Network

### Layer 1 — Physical

**Function: The job of the physical layer is to provide a path for data transmission.**

**Media implementing this layer: Copper wire, fiber optic cable, radio waves, or any other method capable of transmitting data.**

**Professional working at this level: Telecommunications Engineer or Telecommunications Technician.**

**The physical layer can be very expensive to update. Many legacy network methods are maintained to prevent replacement of Layer 1 infrastructure. The physical layer exists in all network spans and in the nodes themselves. Older routers and switching equipment can provide limited function even with software updates because of their Layer 1 limitations. Older network interface cards (NIC's) can have similar limitations. Newer equipment maintains backward compatibility to allow network operation on older infrastructure.**

### Layer 2 — Data Link

**Function: The data link layer controls the transmission of data over a given path. In network terms, this is node to node transmission.**

**Protocols implementing this layer: Ethernet, Wi-Fi, Address Resolution Protocol (ARP), and others.**

**Professional working at this level: Network Engineer or Network Technician.**

**The data link layer is concerned with organizing Layer 1 transmissions into usable data. Different Layer 2 protocols use different methods to do this. Ethernet (defined by the Institute of Electrical and Electronics Engineers standard 802.3 e.g. IEEE 802.3) divides electrical pulses into "frames" that can be sent and received down a Layer 1 link. If frames are not received intact, Layer 2 protocols can correct this by requesting a retransmission or accept faults. Layer 2 also controls the speed of transmission to ensure reliable service; this is often called flow control.**

### Layer 3 — Network

**Function: The network layer is concerned with addressing individual computers (also called hosts) and routing connections on different local networks. In common usage, a node is a point in a network, but a host is a fully functional system (not a network device like a router or printer) with a network layer address.**

**Protocols implementing this layer: Internet Protocol (IP), Internet Control Message Protocol (ICMP), Internet Protocol Security (IPsec), Internetwork Packet Exchange (IPX), and others.**

**Professional working at this level: Network Engineer, Network Administrator, Cryptographer, or Network Infrastructure Team.**

**The network layer is often associated with IP addresses, but is properly understood for the way it allows routing across networks (i.e. internetworking). Numerous methods to achieve more efficient routing have been proposed and revised. Various local architectures depend on the routing characteristics of protocols used at Layer3. Multi-protocol Label Switching (MPLS) backbones connect geographically divided offices and data resources. VLAN segregation helps virtually and flexibly divide different systems on a network to secure data and to balance infrastructure usage.**

**Data Quality, Management, and Reporting Risks: "Garbage in, garbage out" refers to inputting bad data into a system will result in bad data output from the system. Poor data or data quality issues may lead to inaccurate management reporting and flawed decision making. Databases that are not designed to ensure the integrity of the data can result in incomplete or invalid data. Analytics that rely on invalid data will most likely yield flawed results. Therefore, big data analytics must account for these data quality risks.**

**Additionally, data that is not obtained and analyzed in a timely manner may also result in incorrect analytic outputs, flawed management decisions, and loss of revenue. Data sourced from third parties should be timely, accurate, complete, and from a reputable source. Third-party data that is in an inappropriate format may not be suitable for analysis and may delay management decision-making.**

**After data has been received and analyzed, it may be challenging to ensure that end users manage and protect the data. A lack of end-user computing controls may lead to inaccurate reports and data leaks. End-user production reports, ad hoc reports, and predictive analytic outputs must all be reviewed and approved to limit flawed management decisions. Big data reports should also adhere to an organization's data classification policies to ensure only appropriate data is shared, both internally and externally. Report options and distribution channels may be appropriate only for data of specific sizes and formats. Organizations may face obstacles when determining the appropriate report options and channels for each analytic result.**

## Layer 4 — Transport

**Function: The transport layer is concerned with transmitting data from host to host on a network or across networks with a specified quality of service.**

**Protocols implementing this layer: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and others.**

**Professional working at this level: Network Engineer, Network Administrator, Cryptographer, or Network Infrastructure Team.**

**The transport layer is primarily known for allowing network hosts to use and/or provide multiple service. Using a TCP example, a client makes a request to a server. The server is listening with an open connection on a well-known port number. Specifying the port number in the request allows the server to identify which service is being requested. The server then replies to the appropriate client port, which can be assigned in any number of ways depending on the protocol. Layer 4 specifies other services like flow control to ensure speed without overwhelming the host, error correction to identify and resend bad packets, and others.**

## Layer 5 — Session

**Function: The session layer provides services for management of remote connections at very basic levels of interaction. Layer 5 is responsible for enabling the interaction of local and remote processes.**

**Protocols implementing this layer: Remote Procedure Calls (RPC), AppleTalk Session Protocol (ASP), parts of TCP, and others.**

**Professional working at this level: Network Administrator, Application Developer, Cryptographer, or Network Application Team.**

**The session layer includes some of TCP's functions that provide connections. In contrast, UDP provides "connectionless" service by treating each UDP "datagram" (equivalent to a TCP packet) as independent of other datagrams. TCP packet streams can be placed in order and retransmitted if one is damaged or lost. Layer 5 services also establish and track multiple connections between hosts using the same application (e.g. downloading multiple files simultaneously using File Transfer Protocol [FTP]). Some connections are sensitive to start and stop or combine multiple data streams; the session layer controls start and stop services for applications needing a controlled data stream. This feature also allows recovery of interrupted sessions.**

## Layer 6 — Presentation

**Function: The presentation layer is concerned with taking data form a wide variety of application layer sources and making the data available to other applications and network standard protocols. The presentation layer represents a departure from the layers associated with data in motion. Presentation applies to data at rest as well as data in motion. The presentation layer also coordinates the encapsulation of data at rest in compressed files, encrypted files, and compound files (i.e., files containing other files like email attachments).**

**Protocols implementing this layer: MIME, ASCII, Zip.**

**Professional working at this level: Application Developer, Network Application Team, Cryptographer, Telecommunications Architect, Network Architect, Forensic Analyst, Network Engineer.**

**The presentation layer is primarily concerned with data conversion. Numerous standardization protocols are used to ensure interoperability between systems and applications like ASCII and UNICODE. If conversion is possible between two such standards, the presentation layer performs this function, but it also performs compression, decompression, encryption, and decryption, although all such tasks are not exclusively part of this layer.**

### Layer 7 — Application

**Function: Various other applications generate and consume data at this level. This layer is the most diverse, but also the most familiar to users. The applications that generate and modify user data implement the application layer of the stack. It is a subtle difference, but this layer is not the applications themselves; rather, it is the formatted data product of those applications.**

**Protocols implementing this layer: File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and many others.**

**Professional working at this level: Application Developer, Network Application Team, Cryptographer, Telecommunications Architect, Network Architect, Forensic Analyst, Network Engineer.**

**The application layer and the presentation layer function together in most cases. Applications that organize data into standard formats for interoperation use presentation layer file formats. Those formats are opened to the user by applications with awareness of that file type. For example, most users automatically associate the application, MS Word, with the file type ".docx." These two layers have distinct functions, but differ from the strictly data-in-motion layers: 2, 3, 4, and 5.**

# Appendix E. The Seven-layer Model in Action

This example represents two hosts communicating across two LANs. (Note: this example ignores the complexities of internet routing.)

| Example of Two Hosts Communicating Across Two Local Area Networks (LANs) |
| --- |
| **Layer 7 — Application** |
| **User data (a graphic).** |
| **Layer 6 — Presentation** |
| **The graphic is formatted as a JPG. No encapsulation occurs; this is a transformation of a displayed bitmap to a storage format. It can be stored in a file system or transferred via network connection.** |
| **Layer 5 — Session** |
| **Secure Socket Layer (SSL) encryption is applied. No encapsulation occurs; this is a transformation within a session. The other end knows how to decrypt it. This layer begins the data-in-motion layers.**<br><br>**Visually, the content can be presented as <DATA>. For visual reinforcement, brackets surround the content at this level. The next level shows how metadata from higher levels is treated as content.** |
| **Layer 4 — Transport** |
| **TCP header information is added to identify the receiving host's connected port to receive the encrypted data. The encrypted session layer data become the payload data of layer 4 encapsulation.**<br><br>**Visually, this can be abbreviated as 4+<DATA>, where the brackets define DATA at this level.** |
| **Layer 3 — Network** |
| **IP header information is added to the data received down the stack from layer 4. The combined session layer data and transport layer metadata become the payload data of layer 3 encapsulation.**<br><br>**Visually, this can be abbreviated as 3+<4 DATA>. Layer 4 metadata is now inside the brackets meaning that it is treated as DATA by layer 3.** |
| **Layer 2 — Data Link** |
| **The IP packets are broken into frames for transmission across the Local Area Network to the switch which also serves as a router. Similar to the transport and network layers, both the original data and the metadata from the higher layers are treated the same when forming data link layer frames.**<br><br>**Visually, this can be abbreviated as 2+<3 4 DATA>. All previous data and metadata are encapsulated by layer 2 headers.** |
| **Layer 1 — Physical** |
| **The frames are encoded as a wave form in the copper wires. No encapsulation takes place because layer one simply transforms the data into a carrier signal. Since all data from higher levels is treated the same, metadata from higher levels is considered to be part of the data coming down the stack.**<br><br>**Once the metadata relevant to the current layer is removed, the remaining data is pushed up the stack where the higher-level metadata is recognized as metadata again. Network devices often only go back up the stack through layer 4; session layer data is rarely modified at intermediate stops between the hosts.** |

# Appendix F. Common Network Protocol Descriptions

These definitions are from Barron's Business Guide's *Dictionary of Computer and Internet Terms*, Twelfth Edition, 2017.

**domain name server** – a server responsible for translating domain addresses, such as www.example.com into IP (internet protocol) numbers, such as 127.192.92.95.

**ethernet** – a type of local-area network originally developed by Xerox Corporation. Communication takes place by means of radio-frequency signals carried by a cable.

**File Transfer Protocol (FTP)** – a standard way of transferring files from one computer to another on the Internet and on other TCP/IP networks.

**Hypertext Transfer Protocol (HTTP)** – a standard method of publishing information as hypertext in HTML format on the Internet. HTTPS is a variation of HTTP that uses SSL encryption for security.

**Internet Mail Access Protocol (IMAP)** – a protocol for viewing email on a personal computer while leaving it in place on the host system.

**Post Office Protocol (POP)** – a standard protocol for delivering email to personal computers.

**Secure Sockets Layer (SSL) Protocol** – designed for securing connections between web clients and web servers over an insecure network, such as the internet.

**Simple Mail Transfer Protocol (SMTP)** – a protocol used to transfer electronic mail between computers on the Internet and other TCP/IP networks.

**Transmission Control Protocol/Internet Protocol (TCP/ IP)** – a standard format for transmitting data packets from one computer to another. The two parts of TCP/IP are TCP, which deals with construction of data packets, and IP, which routes them from machine to machine.

# Appendix G. Comparison of SQL and NoSQL Databases

| | SQL Databases | NoSQL Databases |
|---|---|---|
| Types | One type (SQL database) with minor variations. | Many different types including key-value stores, document databases, wide-column stores, and graph databases. |
| Development History | Developed in 1970s to deal with first wave of data storage applications. | Developed in 2000s to deal with limitations of SQL databases, particularly concerning scale, replication and unstructured data |
| Examples | MySQL, Postgres, Oracle Database. | MongoDB, Cassandra, HBase, Neo4j. |
| Data Storage Model | Individual records (e.g., "employees") are stored as rows in tables, with each column storing a specific piece of data about that record (e.g., "manager," "date hired"), much like a spreadsheet. Separate data types are stored in separate tables, and then joined together when more complex queries are executed. For example, "offices" might be stored in one table, and "employees" in another. When a user wants to find the work address of an employee, the database engine joins the "employee" and "office" tables together to get all the information necessary. | Varies based on NoSQL database type. For example, key-value stores function similarly to SQL databases, but have only two columns ("key" and "value"), with more complex information sometimes stored within the "value" columns. Document databases do away with the table-and-row model altogether, storing all relevant data together in single "document" in JSON, XML, or another format, which can nest values hierarchically. |
| Schemas | Structure and data types are fixed in advance. To store information about a new data item, the entire database must be altered, during which time the database must be taken offline. | Typically dynamic. Records can add new information on the fly, and unlike SQL table rows, dissimilar data can be stored together as necessary. For some databases (e.g., wide-column stores), it is somewhat more challenging to add new fields dynamically. |
| Scaling | Vertically, meaning a single server must be made increasingly powerful to deal with increased demand. It is possible to spread SQL databases over many servers, but significant additional engineering is generally required. | Horizontally, meaning that to add capacity, a database administrator can simply add more commodity servers or cloud instances. The NoSQL database automatically spreads data across servers as necessary. |
| Development Model | Mix of open-source (e.g., Postgres, MySQL) and closed source (e.g., Oracle Database). | Open-source. |

| | | |
|---|---|---|
| **Supports Transactions** | **Yes, updates can be configured to complete entirely or not at all.** | **In certain circumstances and at certain levels (e.g., document level vs. database level).** |
| **Data Manipulation** | **Specific language using Select, Insert, and Update statements, e.g. SELECT fields FROM table WHERE [enter specific criteria]** | **Through object-oriented APIs.** |
| **Consistency** | **Can be configured for strong consistency.** | **Depends on product.** |

Source: Mongo DB website, https://www.mongodb.com/nosql-explained/nosql-vs-sql.

# Appendix H. References and Additional Reading

## References


Hall, Kaerrie. “Customer Data Quality: The Good, the Bad, and the Ugly.” Validity. September 5, 2019. https://www.validity.com/blog/customer-data-quality/.

Mell, Peter and Tim Grance, “The NIST Definition of Cloud Computing,” NIST Information Technology Laboratory, Computer Security Resource Center, SP 800-145, September 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final.


## Additional Reading


Center for Internet Security, https://www.cisecurity.org.

Cloud Security Alliance, https://cloudsecurityalliance.org.

Downing, Douglas, Michael Covington, Ph.D., Melody Covington, Catherine Anne Barrett, and Sharon Covington. *Dictionary of Computer and Internet Terms, Twelfth Edition*. Hauppauge, NY: B.E.S. Publishing, 2017. https://www.simonandschuster.com/books/-Dictionary-of-Computer-and-Internet-Terms/Douglas-Downing/Barrons-Business-Dictionaries/9781438008783.

Gibbs, Nelson, Divakar Jain, Amitesh Joshi, Surekha Muddamsetti, and Sarabjot Singh. *A New Auditor's Guide to Planning, Performing, and Presenting IT Audits*. Altamonte Springs, FL: The Interal Audit Foundation, 2010. https://bookstore.theiia.org/a-new-auditors-guide-to-planning-performing-and-presenting-it-audits.

ISACA, https://www.isaca.org.

National Institute of Standards and Technology (NIST), https://www.nist.gov.

Rai, Sajay, Philip Chukwuma, and Richard Cozart. *Security and Auditing of Smart Devices: Managing Proliferation of Confidential Data on Corporate and BYOD Devices*. Boca Raton, FL: CRC Press, 2016. https://bookstore.theiia.org/security-and-auditing-of-smart-devices-managing-proliferation-of-confidential-data-on-corporate-and-byod-devices.

Sigler, Ken and Dr. James L. Rainey III. *Securing an IT Organization through Governance, Risk Management, and Audit*. Boca Raton, FL: CRC Press, 2015.

# Acknowledgements


## Guidance Development Team

Susan Haseley, CIA, USA (Chairman)

Sajay Rai, CISM, CISSP, USA (Project Lead)

Brad Ames, USA

Michael Lynn, CIA, CRMA, USA

Avin Mansookram, South Africa

Gerard Morisseau, USA

Justin Pawlowski, CIA, CRMA, Germany

## Contributors

Lee Keng “Joyce” Chua, CIA, Singapore

James Enstrom, CIA, USA

Scott Moore, CIA, USA

Shawna Flanders, Director of IT Curriculum, IIA Staff Contributor

## IIA Global Standards and Guidance

P. Michael Padilla, CIA, Director (Project Lead)

Jim Pelletier, Vice President

Anne Mercer, CIA, CFSA, Director

Chris Polke, CGAP, PS Director

Jeanette York, CCSA, FS Director

Shelli Browning, Technical Editor

Lauressa Nelson, Technical Editor

Geoffrey Nordhoff, Content Developer and Technical Writer

Christine Janesko, Content Developer and Writer

Vanessa Van Natta, Standards and Guidance Specialist

The IIA would like to thank the following oversight bodies for their support: Information Technology Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and the International Professional Practices Framework Oversight Council

## About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves 200,000 members from nearly 200 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.theiia.org.

## Disclaimer



## Copyright



June 2020

Note: The cover, logo, and certain references were updated November 2021. There were no changes to the original content. Questions may be directed to guidance@theiia.org.

The Institute of Internal Auditors

**Global Headquarters**
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101