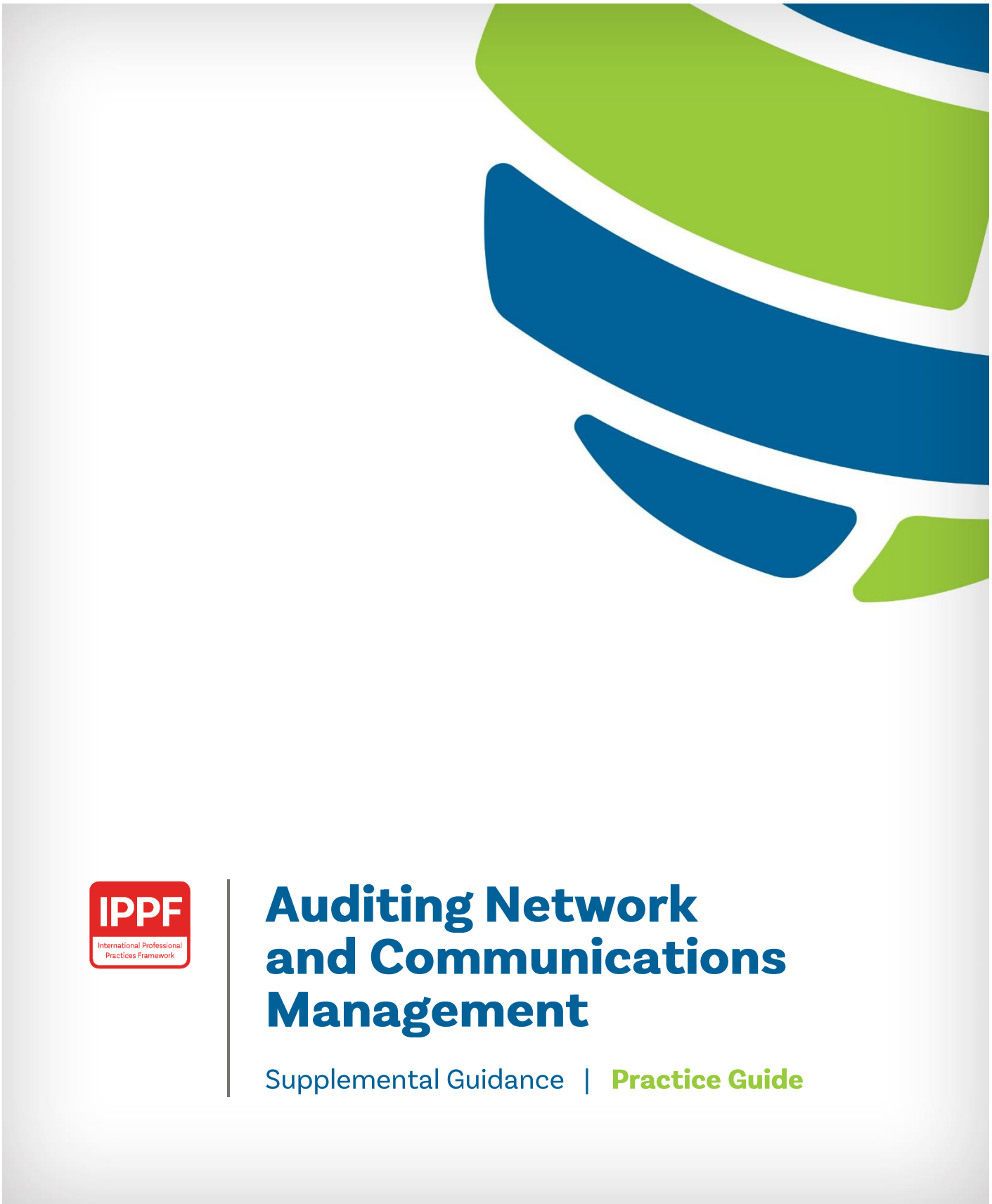


IPPF
International Professional Practices Framework

Auditing Network and Communications Management

Supplemental Guidance | **Practice Guide**

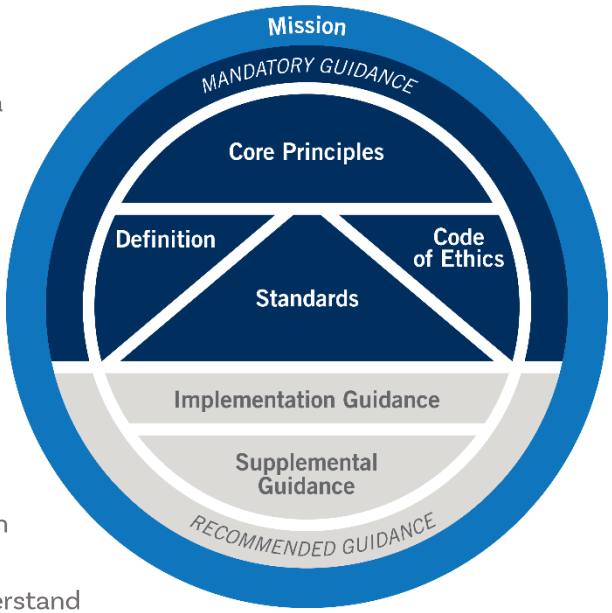
GLOBAL TECHNOLOGY AUDIT GUIDE

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.

IPPF | International Professional Practices Framework



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.theiia.org.

About GTAGs

Within the IPPF's Supplemental Guidance, Global Technology Audit Guides (GTAGs) provide auditors with the knowledge to perform assurance or consulting services related to an organization's information technology (IT) and information security (IS) risks and controls. The *Standards* that give rise to the GTAGs are listed below.

- **1210.A3** – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.
- **2110.A2** – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- **2120.A1** – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
    - Achievement of the organization's strategic objectives.
    - Reliability and integrity of financial and operational information.
    - Effectiveness and efficiency of operations and programs.
    - Safeguarding of assets.
    - Compliance with laws, regulations, policies, procedures, and contracts.
- **2130.A1** – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:
    - Achievement of the organization's strategic objectives.
    - Reliability and integrity of financial and operational information.
    - Effectiveness and efficiency of operations and programs.
    - Safeguarding of assets.
    - Compliance with laws, regulations, policies, procedures, and contracts.
- **2220.A1** – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

Contents

Executive Summary

An organization's data network enables communications with customers, vendors, and other stakeholders, powering e-commerce and the delivery of services, among other benefits. Due to the inherent security risks associated with operating a data network, "zero-trust" design principles, which increase the granularity of identity verification controls, are often implemented by management.

In their assessments of organizational risks, internal auditors are likely to identify the availability and security of the enterprise data network, including its connections to external systems, as significant inherent risks. Therefore, to provide relevant, valuable assurance and consulting services, it is helpful to understand some basic network management techniques and terms.

Engagement planning efforts typically focus on the organization's governance, risk management, and control processes over common technologies and connections to ensure various objectives are met. Control objectives for network and communications management can be grouped in the following high-level categories:

1. Governance, Risk Management, and Administration – Ensuring network and communications objectives, risks, and controls are aligned with organizational strategies and objectives. Requirements, expectations, and the resources to meet them are formalized in policies, procedures, budgets, and technical plans.
2. Domain Management – Utilizing an inventory of Internet Protocol (IP) addresses effectively and efficiently. An environment of subnetworks, also known as security domains, to meet operational and security objectives is established.
3. Communications Management – Implementing services from qualified providers to meet the organization's collaboration needs. Such services typically include email, video conferencing, Voice over IP, programmed data exchanges, and cloud-based services.
4. Boundary Defense – Ensuring that only authorized accounts and services are accessing and traversing the network, and that adequate event logging and log monitoring promote accountability. Connections to external networks are properly authorized and secured.
5. Network Operations – Monitoring and ensuring data network service availability, often referred to as resiliency, throughout the organization. Network managers work with cybersecurity operations teams to investigate and resolve issues or anomalous activity.

Other relevant, high-level control objectives, such as identity and access management, cybersecurity, and secure remote access, are covered briefly in this guide and discussed more extensively in other GTAGs. Broadly applicable risk and control groupings are discussed in this guide as they relate specifically to network and communications management.

Introduction

Put simply, modern organizations run on computers connected to communications **networks**, primarily the internet. Therefore, each organization has **inherent risks** related to managing the **confidentiality**, **integrity**, and **availability** of its enterprise data network, due to threats that may arise from inside or outside the network. Some organizations have multiple, separately managed networks, for example when certain business units, subsidiaries, or other affiliated entities maintain separate virtual **domains** and physical networks.

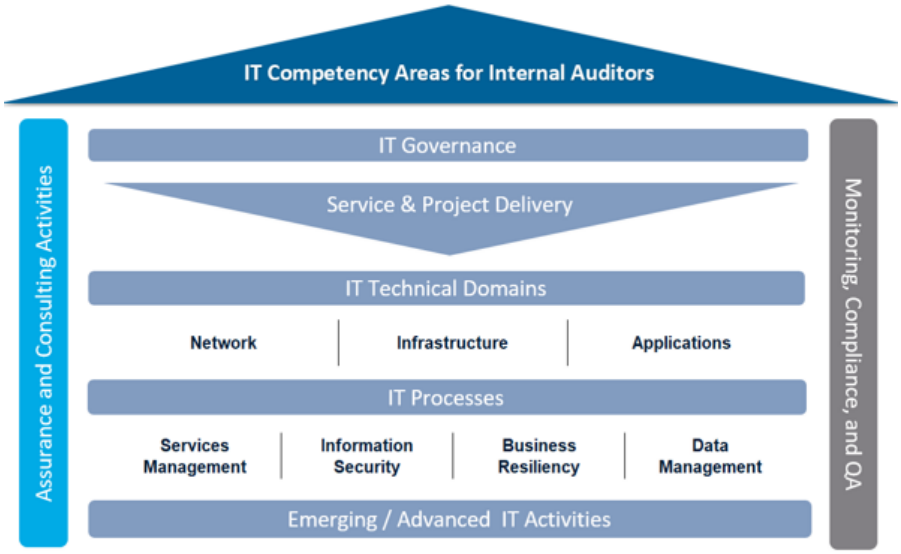
> **Note**
>
> Appendix A lists other IIA resources relevant to this guide. Terms in bold are defined in the Glossary in Appendix B.

Organizations design and implement **information technology controls** to ensure that **information security**, service availability, and system functionality **objectives** are met effectively and efficiently.

For the **internal audit activity** to provide valuable **assurance** and **consulting services**, the auditors should have a reasonable understanding of the **controls** relevant to meeting an organization's communications needs.

This GTAG includes **risks** and controls relevant to the "Network" technical domain, as depicted in Figure 1 below, which was introduced in the GTAG "IT Essentials for Internal Auditors."

Figure 1: The IIA's IT Competency Areas for Internal Auditors



Source: The Institute of Internal Auditors

While each organization's needs may be unique, the processes to establish and operate an enterprise communications ecosystem can be grouped into high-level objectives that are essentially common to all. The five high-level objectives for network and communications management can be summarized as:

- **Governance**, **Risk Management**, and Administration.
- Domain Management.
- Communications Management.
- Boundary Defense.
- Network Operations.

These objectives and their respective risks and controls are described in greater detail in the sections below, along with references to relevant guidance in widely used external **control frameworks** to help an internal audit team plan an **engagement**.

The chief audit executive (CAE) is responsible, per Standard 2030 – Resource Management, for ensuring "that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan." For organizations where network and communications risks are assessed, as required in Standard 2010 – Planning, as relatively significant, this GTAG helps the CAE by providing a systematic approach that can be adopted by auditors of all backgrounds and adapted to all organizations.

This guide will help the reader:

- Describe the importance of network and communications management to achieving an organization's operating objectives.
- Identify the typical components — or groupings of related objectives, risks, and controls — that go into managing an enterprise communications ecosystem.
- Identify certain external frameworks' relevant **control processes**, for further research into best practices to aid engagement planning.
- Perform assurance and consulting services over network and communications management.

Audit Planning

An audit engagement that examines an organization's network and communications management involves a **risk assessment** and specified **engagement objectives**. It also includes tests to evaluate the adequacy and effectiveness of relevant control processes to determine whether any significant risk **exposures** exist. Ideally, the internal audit activity, technology management teams, and other personnel will collaborate to provide valuable insight into inherent risks, the strength of controls, and **residual risks**.

The risks and controls relevant to network and communications management are also relevant to other IT and information security (IS, collectively IT-IS) auditable subject areas. This guide will focus on controls central to planning, implementing, and monitoring the organization's data and

communications networks and services to meet operational objectives. Some risk-control groups discussed briefly in this guide are covered more extensively in other GTAGs, primarily:

- "Auditing Business Applications."
- "Auditing Identity and Access Management."
- "Auditing Mobile Computing."
- "Auditing Cybersecurity Operations: Prevention and Detection."
- "Auditing Cyber Incident Response and Recovery."

An audit engagement covering network and communications management risks and controls may help the internal audit activity provide assurance on whether the organization's **information technology governance** supports its **strategies** and objectives, as required by Standard 2110.A2. Following this approach helps internal auditors demonstrate conformance to Standard 1200, which states: "Engagements must be performed with proficiency and due professional care."

Internet Overview

Before discussing network and communications management risks and controls, it is helpful to understand how the internet works, including what **Internet Protocol (IP) addresses** and registered **domain names** are. The following descriptions are intended to be understandable by an audience of internal auditors who may not specialize in technology auditing. Further information on the concepts presented in this guide can be found in the sources in Appendix C.

IP Addresses and Registered Domain Names

The internet is based on a numbering system that provides a unique value, known as an address, to each **server** properly registered as a **host** on the network. The most familiar address format is written as four values, each consisting of a number from 0 to 255, separated by periods — for example, 192.0.34.163. This format is used in IP version 4 (IPv4), which is described in greater detail below.

Internet addresses function similarly to physical addresses, in that each unique identifier has an "owner" (actually a lessee, as described below) documented in a public database of record. In addition, the owner can restrict access to the host server and services associated with the address.

The Internet Protocol is a language that network hosts and telecommunications providers use to enable "source" IP addresses to communicate with "destination" addresses, much like completing an old-fashioned telephone call. In fact, data communications are mainly carried on the infrastructure originally built for telephone calls or cable television, which is why many **internet service providers (ISPs)** are owners of vast fiber-optic, copper wire, and wireless communications networks.

The Internet Corporation for Assigned Names and Numbers (ICANN). a global public benefit corporation, allocates portions of the available IP addresses to five Regional Internet Registries (RIRs), each of which covers a different part of the world. The RIRs, in turn, allocate smaller

groups of addresses to ISPs and other network operators in their region, who then license the exclusive right to use specified addresses to individual and enterprise customers.

Enterprise customers typically obtain licenses for a range of IP addresses, known as a "block," which can be obtained in various sizes. The licensing process also includes domain name registration, where the licensee assigns a domain name to at least one of their addresses. A domain name is a set of characters (such as "icann.org") associated with a licensed IP address (such as 192.0.34.163). People can use either the numeric or the character (domain) name to contact the destination address.

Each domain name must be unique to ensure that all communications are routed properly, so new domain name requests are checked against a worldwide **Domain Name System (DNS)** to determine whether a name has already been taken. A domain name is not required for an IP address, so some addresses are only accessible via the numeric identifier. Additionally, the IP address with which a domain name is associated can be changed to another IP address licensed by the registrant.

Once an organization has licensed some number of IP addresses and registered its domain names, it then typically implements website, email, and other servers and services that are assigned to its virtual resources — the IP addresses. The risks and controls related to the communications infrastructure are described in the Network and Communications Control Groups section below, while similar audit guidance for the computing infrastructure (such as **application** servers and databases) is covered in other GTAGs.

Ports

In addition to the numeric or domain name address, a "call" to an IP address is also directed to a designated **port** (depending on the type of service or **protocol** making the call), which the host uses to manage various types of requests and responses. Port numbers theoretically range from 0 to 65535, but certain ones are designated for commonly used protocols. For example, port 53 is used for DNS services, and port 80 is used for the hypertext transfer protocol (HTTP) that the World Wide Web uses.

IPv4 Versus IPv6

The IPv4 protocol has about 4.3 billion addresses, which were effectively completely distributed by the RIRs by November 2019.[1] However, technologies such as **network address translation** (NAT) enabled organizations to associate multiple devices with a single address, extending the protocol's usable life. The use of NAT also deferred a transition to exclusive use of the next generation of IP numbering, known as IPv6.

IPv6 addresses consist of eight groups, each a four-character combination of hexadecimal characters (0-9, then A-F representing 10-15), separated by colons. For example, an IPv6 address might look like: 123A:4B5C:D6E7:89F0:0000:1A23:45B6:7C8D. This format theoretically allows 2^{128} total addresses (an essentially unlimited number), compared to IPv4's total of 2^{32} (about 4.3

1. Wikipedia "IPv4 address exhaustion." https://en.wikipedia.org/wiki/IPv4_address_exhaustion.

billion addresses). IPv6 eliminates the problems posed by the complete distribution of IPv4 addresses and enables other engineering and security improvements. However, even though the DNS has supported IPv6 addresses since 2008, a considerable amount of internet traffic still uses IPv4. To promote accessibility, nearly all hardware is programmed to support both protocols.

Network Design Terms and Tools

Communications networks serve a critical function in modern societies and organizations, so their use is subject to laws, regulations, and standardized engineering protocols, as well as organizational policies, procedures, and various objectives. Before reviewing network and communications management controls, it may be helpful to introduce some network design terms and tools.

Networks are managed within administrative business applications (see Business Applications sidebar) that define the elements such as host servers, **routers**, digital **identities**, IP addresses, and communication protocols. The applications also define how the elements relate to each other as a network in domains, subnetworks, and **security domains** (also called security zones). The network administration application associates the internal network elements with the organization's IP addresses and registered hosts. This facilitates management of the assets, including the related hardware, software, and service inventory **metadata**.

Business Applications

Network management tools are software-based; thus, they have the inherent governance, risk management, and control concerns described in the GTAG "Auditing Business Applications." That guide groups relevant objectives, risks, and controls into the following high-level objectives:

- Technology planning.
- System development life cycle.
- Production support.
- Application security.
- Records and information management.
- Vendor management.
- Software asset management.
- Database administration and business intelligence.

Planners define the **enterprise architecture**, then **network administrators** apply best practices and **business rules** to manage communications with adequate security, capacity, and availability, among other objectives. Dividing the network into subnetworks, known as **network segmentation**, is one way to apply varying business rules, such as access restrictions and **authentication** controls, to different parts of the network. One overarching objective of network design is to ensure that the strength of security controls is proportionate to the criticality of the resources to which they are applied.

The devices used to establish a network and properly handle data communications traffic include routers, border **gateways**, **firewalls**, **policy enforcement points**, and a multitude of software-based services, some of which mimic or virtualize the hardware-based services. Physical and software-based devices manage outbound, inbound, and internal communications

according to authorized business rules. Personnel who manage the tools should be adequate in number and have the necessary skills to realize the benefits from such investments.

Monitoring tools, often centrally managed in a network operations center (NOC), provide alerts and outage notifications to help manage issues and reasonably ensure service availability. NOC teams are also often responsible for contributing to or leading resiliency planning efforts, for example by procuring communications services from multiple providers, establishing provisions for **failover** or short-term **bandwidth** needs.

The responsibility for managing the ecosystem of network and communications management hardware and software is often delegated by the chief information officer (CIO) or chief technology officer (CTO) to one or more individuals, depending on the organization's size and other factors. Responsibility for the relevant operating and capital budgets is usually aligned with operational oversight and administration hierarchies. Additionally, one of the typical risk management decisions made by the CIO or CTO is to align the organization's technology policies, procedures, and controls with one or more external control frameworks.

IT-IS Control Frameworks

This guide references specific controls described in three external IT-IS control frameworks of standards, guidance, and best practices (although there are many others). Each framework provides more information about the specific controls than is discussed here. Internal auditors are encouraged to review frameworks used by their organizations and other authoritative IT-IS control guidance. This will help them understand common risks and controls in business processes relevant to their environment. Appendix C provides links to these sources.

This GTAG refers to controls described in the following publications:

- *COBIT 2019 Framework: Governance and Management Objectives* from ISACA (also referred to as COBIT 2019).
- *NIST Special Publication (SP) 800-53, Revision 5: Security and* ***Privacy*** *Controls for Information Systems and Organizations* from the National Institute of Standards and Technology (also referred to as NIST SP 800-53r5).
- *CIS Controls Version 8 (CIS v.8)* from the Center for Internet Security.

IT-IS personnel frequently benchmark operational and security controls against one or more of these frameworks; although each framework uses its own groupings of controls, there are substantial commonalities among them in terminology and categorization. However, one of the significant challenges in grouping "controls" from these frameworks into an audit guide is that each one contains multiple levels of aggregation, as follows:

- *COBIT 2019* consists of 40 Objectives, which contain 231 Practices, which are further broken-down into 1,202 Activities.
- *NIST SP 800-53r5* consists of 20 Families, which contain 298 Controls, which are further broken-down into 709 Subcontrols.

- *CIS v.8* consists of 18 Controls, which contain 153 Safeguards.

This guide mainly references COBIT 2019 Practices, NIST SP 800-53r5 Controls, and CIS v.8 Safeguards, balancing the detailed level of information presented in the frameworks against the usability of this document. However, some Activities and Subcontrols would be grouped differently than their respective Practices and Controls and there are some differences in how the frameworks present similar processes. Nevertheless, this guide's approach provides a means for identifying relevant guidance in each framework for additional consideration in developing an audit program and tests of control adequacy and effectiveness.

Readers of this guide are assumed to have a general knowledge of IT-IS risks and controls, as described in the GTAG "IT Essentials for Internal Auditors." They are encouraged to incorporate a review of the relevant portions of one or more IT-IS control frameworks into their engagement planning and test programs. In addition, when planning a network and communications management engagement, internal auditors generally review relevant policies and procedures to understand control requirements established by the organization. These actions demonstrate the essence of Standard 2201 – Planning Considerations:

> In planning the engagement, internal auditors must consider:
>
> - The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.
> - The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
> - The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.
> - The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

Network and Communications Control Groups

This section describes significant components of an organization's data network and communications ecosystem. In each group, references are made to three external IT-IS control frameworks, where doing so would provide helpful guidance to the reader for additional details. Internal auditors can review the detailed control guidance and other related information in the frameworks for help with building an audit program.

In general, the following sections associate controls within a process or control objective likely to be managed as an aggregated concern. Naturally, this can vary from one organization to the next, so internal auditors are encouraged to structure their engagements as appropriate.

Governance, Risk Management, and Administration

In the *Standards*, governance is defined as: "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." This is separate from risk management, which is described in Standard 2120 – Risk Management as having the following criteria for effectiveness:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

In this context, and in accordance with The IIA's Three Lines Model (see Three Lines Model sidebar), governance includes actions for which the board is responsible, while risk management encompasses management's responsibilities, including:

Three Lines Model

The IIA's Three Lines Model describes the respective roles of the organization's governing body, management, and independent assurance providers. The three lines referenced in the title refer to: reasonably ensuring the achievement of objectives by establishing controls (first line management); reviewing controls and providing risk management assistance (second line management); and providing independent assurance (third-line auditors) to senior management and the organization's oversight authority (the governing body, which is not counted as a line).

- Setting strategies and objectives.
- Determining appropriate risk responses to reasonably ensure the achievement of objectives.
- Allocating capital and expense budgets to various projects and functions to implement the organization's mission, achieve objectives, and manage risks.

One response to risk is to reduce, or mitigate, exposure by designing and implementing controls. Internal controls over the data network and communications typically require a combination of technology and personnel. A mature **control environment** includes monitoring and reporting on the overall effectiveness of the **enterprise risk management (ERM)** program.

Controls are grouped in this guide as administrative or operational, with the latter group divided into the following high-level objectives: domain management; communications management; boundary defense; and network operations.

Governance and Risk Management

As described above, governance pertains to the board's processes for representing the stakeholders' interests, which includes directing and authorizing certain strategies and priorities. The board needs timely, relevant, and decision-useful information, as well as constructive communications with management, to exercise its oversight function. Governance-related controls should be assessed for their utility in helping the board achieve its objectives.

Entity-level strategies and objectives for network and communications management may include **compliance** with applicable regulations and control frameworks, as well as decisions to outsource network infrastructure or otherwise engage critical service partners.

To achieve network and communications objectives, ERM processes typically result in the establishment of policies, procedures, teams, and tools. Enterprise architects use available resources to design a data network that meets the organization's requirements and constraints. Competing objectives of performance, security, and cost factor into designs and standards, which ultimately aim for a reasonable level of residual risk.

An auditor may review the ownership of relevant capital and expense budgets to determine the management teams responsible for designing, implementing, and supporting the data network. Management reports are also typically reviewed to identify and evaluate significant performance metrics, trends, and other relevant data.

Controls that contribute most directly to governance and risk management objectives for a data communications network are described in more detail in:

- *COBIT 2019 Framework: Governance and Management Objectives* in practices:
    - APO01.04 Define and Implement the Organizational Structures.
    - APO01.09 Define and Communicate Policies and Procedures.
    - APO03.01 Develop the Enterprise Architecture Vision.
    - APO06.02 Prioritize Resource Allocation.

- APO08.02 Align I&T [information and technology] Strategy With Business Expectations and Identify Opportunities for IT to Enhance the Business.
- APO09.04 Monitor and Report Service Levels.
- APO10.01 Identify and Evaluate Vendor Relationships and Contracts.
- APO10.04 Manage Vendor Risk.
- APO11.04 Perform Quality Monitoring, Control and Reviews.
- BAI08.01 Identify and Classify Sources of Information for Governance and Management of I&T.
- EDM04.01 Evaluate Resource Management.
- EDM04.02 Direct Resource Management.
- EDM04.03 Monitor Resource Management.
- MEA01.02 Set Performance and Conformance Targets.
- MEA01.04 Analyze and Report Performance.
- MEA03.01 Identify External Compliance Requirements.
- MEA03.02 Optimize Response to External Requirements.

- *NIST SP 800-53r5* in controls:
  - AC-1 Access Control Policy and Procedures.
  - CA-1 Assessment, Authorization, and Monitoring Policies and Procedures.
  - CA-2 Control Assessments.
  - CA-6 Authorization.
  - CM-1 **Configuration** Management Policy and Procedures.
  - CM-4 Impact Analyses.
  - CP-1 Contingency Planning Policy and Procedures.
  - IA-1 Identification and Authentication Policy and Procedures.
  - IR-1 Incident Response Policy and Procedures.
  - PM-1 Information Security Program Plan.
  - PM-6 Measures of Performance.
  - PM-8 Critical Infrastructure Plan.
  - PM-10 Authorization Process.
  - PM-12 Insider Threat Program.
  - PM-14 Testing, Training, and Monitoring.
  - PM-31 Continuous Monitoring Strategy.
  - PT-7 Specific Categories of Personally Identifiable Information.
  - SA-2 Allocation of Resources.
  - SC-1 System and Communications Protection Policy and Procedures.

- SC-38 Operations Security.
- SC-43 Usage Restrictions.
- SI-1 System and Information Integrity Policy and Procedures.
- SI-12 Information Management and Retention.
- SR-3 Supply Chain Controls and Processes.
- SR-6 Supplier Assessments and Reviews.
- SR-8 Notification Agreements.

- *CIS Controls* in safeguards:
  - 4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure.
  - 4.6 Securely Manage Enterprise Assets and Software.
  - 8.1 Establish and Maintain an Audit Log Management Process.
  - 12.3 Securely Manage Network Infrastructure.
  - 15.2 Establish and Maintain a Service Provider Management Policy.
  - 15.4 Ensure Service Provider Contracts Include Security Requirements.
  - 15.5 Assess Service Providers.
  - 17.4 Establish and Maintain an Incident Response Process.

Administration

Controls in this group often serve a combination of risk management, administrative, and operational objectives. Network and communications services consist of processes, tools, and personnel working together to achieve multiple high-level objectives determined by governance and risk management processes. Technical planning, asset management, human resource management, and financial management controls provide resources and more granular direction to the operations.

Technical planning controls typically produce an overall design, or architecture, for the data network, as well as **baseline configurations** to guide the installation of approved technologies. Such controls also produce a timeline, often referred to as a roadmap, for the introduction and retiring of relevant technologies used throughout the organization. For example, a network and communications roadmap might include plans for taking advantage of the benefits of IPv6 routing and security while reducing significant technology resources' exposure to IPv4.

Zero Trust

In SP 800-207 "Zero Trust Architecture," NIST describes zero trust as "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, **least privilege** per-request access decisions." For network and communications management, such principles generally lead technical planning processes to segment the network into security zones and place access controls strategically throughout the organization's network.

Zero trust principles emphasize granular **identity** verification and authentication controls (see Zero Trust sidebar). Deciding how and where to implement those principles to manage confidentiality and integrity risks is a significant concern for network and communications technical planning.

The risks and controls related to managing access to technology resources, including the enterprise data network, in accordance with the least privilege principle are covered more extensively in the GTAG "Auditing Identity and Access Management." However, an audit of network and communications management processes would typically include a review of the management of network administrator accounts and authentication services.

Asset management processes ensure relevant software and hardware are properly procured and recorded. Periodic reconciliations are performed between operational, physical, and financial records to maintain agreement and resolve discrepancies. Bandwidth capacity planning and location-specific connectivity decisions are also intertwined with technical planning and asset management controls to address service availability objectives.

Human resource controls determine the number, types, and levels of personnel engaged to perform network and communications management functions. To gain optimal benefits (otherwise known as achieving effectiveness objectives) from the communication and collaboration services, designated personnel are trained to administer and use the tools effectively and securely. Additionally, training on how to properly use the organization's communication services is usually provided to end users.

Financial administration controls ensure proper accounting treatment of transactions and enable management objectives related to efficiency, such as performance monitoring, resource allocation, and cost modeling. Various analyses of network and communications expenditures can identify significant vendors, recurring liabilities that may need lease accounting treatment, or **rogue IT**. Reporting and analyses also may be used to monitor the progress of relevant projects, such as network equipment upgrades or adding an outsourced cloud-based infrastructure-as-a-service (IaaS) environment to the organization's data and communications ecosystem.

Controls that enable the administration of network and communications processes are described in more detail in:

- *COBIT 2019 Framework: Governance and Management Objectives* in practices:
    - APO01.08 Define Target Skills and Competencies.
    - APO01.10 Define and Implement Infrastructure, Services and Applications to Support the Governance and Management System.
    - APO02.03 Define Target Digital Capabilities.
    - APO02.05 Define the Strategic Plan and Road Map.
    - APO03.02 Define Reference Architecture.
    - APO03.03 Select Opportunities and Solutions.

- APO03.04 Define Architecture Implementation.
- APO03.05 Provide Enterprise Architecture Services.
- APO04.04 Assess the Potential of Emerging Technologies and Innovative Ideas.
- APO06.01 Manage Finance and Accounting.
- APO06.04 Model and Allocate Costs.
- APO06.05 Manage Costs.
- APO07.01 Acquire and Maintain Adequate and Appropriate Staffing.
- APO07.03 Maintain the Skills and Competencies of Personnel.
- APO09.05 Review Service Agreements and Contracts.
- BAI02.01 Define and Maintain Business Functional and Technical Requirements.
- BAI03.01 Design High-Level Solutions.
- BAI03.04 Procure Solution Components.
- BAI03.09 Manage Changes to Requirements.
- BAI04.01 Assess Current Availability, Performance and Capacity and Create a Baseline.
- BAI04.03 Plan for New or Changed Service Requirements.
- BAI09.01 Identify and Record Current Assets.
- BAI10.01 Establish and Maintain a Configuration Model.
- BAI10.02 Establish and Maintain a Configuration Repository and Baseline.
- BAI10.05 Verify and Review Integrity of the Configuration Repository.
- BAI11.07 Monitor and Control Projects.
- DSS05.04 Manage User Identity and Logical Access.
- MEA01.03 Collect and Process Performance and Conformance Data.

- *NIST SP 800-53r5* in controls:
  - AC-2 Account Management.
  - AC-3 Access Enforcement.
  - AC-6 Least Privilege.
  - AC-7 Unsuccessful Login Attempts.
  - AC-16 Security and Privacy Attributes.
  - AC-25 Reference Monitor.
  - AT-2 Literacy Training and Awareness.
  - AT-3 Role-Based Training.
  - AU-10 Non-Repudiation.
  - CM-8 System Component Inventory.

- CM-9 Configuration Management Plan.
- IA-2 Identification and Authentication (Organizational Users).
- IA-3 Device Identification and Authentication.
- IA-5 Authenticator Management.
- IA-7 Cryptographic Module Authentication.
- IA-9 Identification and Authentication (Non-Organizational Users).
- IA-10 Adaptive Authentication.
- IA-11 Re-Authentication.
- PL-4 Rules of Behavior.
- PM-4 Plan of Action and Milestones Process.
- PM-5 System Inventory.
- PM-13 Security and Privacy Workforce.
- PM-32 Purposing.
- PS-6 Access Agreements.
- PS-7 External Personnel Security.
- RA-9 Criticality Analysis.
- SA-4 Acquisition Process.
- SA-5 System Documentation.
- SA-8 Security and Privacy Engineering Principles.
- SA-9 External System Services.
- SA-17 Developer Security and Privacy Architecture and Design.
- SA-22 Unsupported System Components.
- SA-23 Specialization.
- SC-11 Trusted Path.
- SC-16 Transmission of Security and Privacy Attributes.
- SR-11 Component Authenticity.

- *CIS Controls* in safeguards:
  - 1.1 Establish and Maintain Detailed Enterprise Asset Inventory.
  - 1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory.
  - 1.5 Use a Passive Asset Discovery Tool.
  - 3.8 Document Data Flows.
  - 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software.
  - 5.1 Establish and Maintain an Inventory of Accounts.

- 5.5 Establish and Maintain an Inventory of Service Accounts.
- 5.6 Centralize Account Management.
- 6.3 Require MFA (**multi-factor authentication**) for Externally-Exposed Applications.
- 6.4 Require MFA for Remote Network Access.
- 6.5 Require MFA for Administrative Access.
- 6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems.
- 6.7 Centralize Access Control.
- 12.1 Ensure Network Infrastructure is Up-to-Date.
- 12.2 Establish and Maintain a Secure Network Architecture.
- 12.5 Centralize Network Authentication, Authorization, and Auditing (AAA).
- 14.3 Train Workforce Members on Authentication Best Practices.
- 14.8 Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks.
- 14.9 Conduct Role-Specific Security Awareness and Skills Training.

Domain Management

When an organization obtains a block of IP addresses and registers its domain names (including assigning specific IPv4 and IPv6 addresses to the domain names), it also assigns or retains the excess IP addresses for additional uses. Enterprise architects apply best practices, requirements, and the outputs of ERM processes to determine the components and necessary business rules to provide effective, efficient communications services.

To manage data traffic between the organization's network and external systems, including the communications transport networks, a border gateway protocol (BGP) language has become a global standard. Dedicated servers use the BGP to recognize telecommunications transport networks and other organizations' internal data networks, and apply programmed business rules to properly route traffic.

Misconfigurations and some cyberattacks can cause traffic to be misrouted, often to websites that mimic legitimate sites to trick the end user into divulging sensitive information. Misconfigurations and cyberattacks on the border gateway servers can overload routing services with false requests, causing a **denial of service** to legitimate requests.

COBIT 2019 does not include Practices or Activities specifically related to managing an organization's IP addresses or domains. However, the generalized controls for solution development and implementation, covered in Objectives "BAI03 Managed Solutions Identification and Build" and "BAI07 Managed IT Change Acceptance and Transitioning," offer a high-level model.

In NIST SP 800-53r5, control "AC-4 Information Flow Enforcement" has 32 subcontrols (only "SA-8 Security and Privacy Engineering Principles" has more, with 33). It is grouped here with other network design controls. Internal auditors can review the subcontrols for more details on how network designs and devices contribute to efficient, secure communications. Such details may be helpful for designing tests of domain management controls.

Controls to define and manage an organization's digital domain can be grouped as relating to network design and device administration.

Network Design

To help manage the complexity of an organization's data network, enterprise architects designate segments of the network — a set of IP addresses — to support specified groups of resources. The designations are usually determined by a combination of organizational **data classification** policies and each resource's function and **security categorization** (see Principles of Modularity and Layering sidebar). Associating IP addresses with elements in the ecosystem enables network administration controls and the writing of traffic-routing business rules. **Microsegmentation** facilitates a zero-trust approach by decreasing the number of addresses in each segment, which helps increase the granularity of access controls.

Principles of Modularity and Layering

In NIST SP 800-53r5, a subcontrol of "SA-8 Security and Privacy Engineering Principles" describes modularity as isolating "functions and related data structures into well-defined logical units." Layering (for example, organizing a network into security zones) is described as aiding the identification and management of dependencies and relationships between systems.

Security zones are groups of network segments with similar security categorizations; typically, the data transmission rules, and necessary strength of **encryption** and authentication controls, are determined by a system's security categorization. For example, a security zone may be created for system testing, where developers and end users can test new versions of software for functionality, compatibility, and security without impacting or interfacing with the production (the in-service) security zone.

Data loss prevention and privacy-related controls are also facilitated by security zones, for example by enabling firewall rules to disallow transmissions of certain file types or communication protocols from a more-restricted to a less-restricted zone.

Often, systems within a security zone can share (trust) a user authentication within a single **session**; however, zero-trust principles encourage a new authentication before accessing each system, which may have a negative impact on the user experience.

Controls that implement network designs into segments and security zones are described in more detail in:

- *COBIT 2019 Framework: Governance and Management Objectives* in practices:
    - BAI03.02 Design Detailed Solution Components.
    - BAI03.08 Execute Solution Testing.
    - BAI07.01 Establish an Implementation Plan.
    - BAI07.04 Establish a Test Environment.
    - DSS06.06 Secure Information Assets.
- *NIST SP 800-53r5* in controls:
    - AC-4 Information Flow Enforcement.
    - AC-21 Information Sharing.
    - CA-9 Internal System Connections.
    - CM-12 Information Location.
    - PL-8 Security and Privacy Architectures.
    - RA-2 Security Categorization.
    - SC-2 Separation of System and User Functionality.
    - SC-20 Secure Name/Address Resolution Service (Authoritative Source).
    - SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver).
    - SC-22 Architecture and Provisioning for Name/Address Resolution Service.
    - SC-32 System Partitioning.
    - SC-39 Process Isolation.
    - SC-44 Detonation Chambers.
    - SC-46 Cross Domain Policy Enforcement.
    - SC-49 Hardware-enforced Separation and Policy Enforcement.
    - SC-50 Software-enforced Separation and Policy Enforcement.
- *CIS Controls* in safeguards:
    - 3.7 Establish and Maintain a Data Classification Scheme.
    - 3.12 Segment Data Processing and Storage Based on Sensitivity.
    - 3.13 Deploy a Data Loss Prevention Solution.
    - 4.4 Implement and Manage a Firewall on Servers.
    - 4.9 Configure Trusted DNS Servers on Enterprise Assets.
    - 12.4 Establish and Maintain Architecture Diagram(s).
    - 16.8 Separate Production and Non-Production Systems.
    - 16.10 Apply Secure Design Principles in Application Architectures.

Network Device Administration

Devices that act as intermediaries between the organization's computing and communications capabilities include hardware and related software applications. These devices are programmed to facilitate communications according to engineering best practices and internal business rules (see Transport Layer Security sidebar).

There are significant inherent risks related to the administrator accounts that manage the network devices. These accounts are often targeted by hackers and malware to create a means (such as unauthorized administrator accounts or escalated privileges, bypassed or suppressed controls, and covert communication channels) for further exploits.

Examples of network devices include routers, border gateway servers, domain name servers, network administration applications, web application firewalls (WAF), other firewalls, policy servers, and various virtualization technologies. An analysis of expenditures in certain finance and accounting categories can reveal the significant vendors, tools, and services employed in network administration.

Transport Layer Security (TLS)

Communications between devices assigned to IP addresses are mainly secured by TLS, which uses encryption and digital certificates to ensure the confidentiality and non-repudiability (verifying the identity of the sender), respectively, of the messages. In SP 1800-16 "Securing Web Transactions – TLS Server Certificate Management," NIST recommends centralizing the management of an organization's digital certificates as a best practice to mitigate the operational and security risks of communications traversing the network with expired, missing, or untrusted digital certificates.

A review of network device administration controls would typically determine the strength of controls to achieve the following objectives:

- Network management hardware and software are properly installed and connected to monitoring systems, in accordance with internal requirements.
- Security **event logs** are programmed to capture an audit trail for significant actions, such as creating new administrator accounts or modifying any configuration items.
- Baseline configurations are managed to optimize controls for network performance and security.
- Changes to network and communications technologies or configurations, including security **patches** for relevant applications, are effectively implemented.
- Access to technology resources, both physical and logical, is sufficiently secured, with system administrator accounts authorized according to the least privilege principle.

Relevant controls over network device administration are described in:

- *COBIT 2019 Framework: Governance and Management Objectives* in practices:
    - BAI03.05 Build Solutions.

- BAI03.10 Maintain Solutions.
- BAI07.05 Perform Acceptance Tests.
- BAI07.06 Promote to Production and Manage Releases.
- BAI10.03 Maintain and Control Configuration Items.
- BAI10.04 Produce Status and Configuration Reports.
- DSS05.05 Manage Physical Access to I&T Assets.
- DSS06.03 Manage Roles, Responsibilities, Access Privileges and Levels of Authority.

- *NIST SP 800-53r5* controls:
  - AU-2 Event Logging.
  - AU-3 Content of Audit Records.
  - AU-4 Audit Log Storage Capacity.
  - AU-8 Time Stamps.
  - AU-11 Audit Record Retention.
  - AU-12 Audit Record Generation.
  - CM-2 Baseline Configuration.
  - CM-3 Configuration Change Control.
  - CM-5 Access Restrictions for Change.
  - CM-6 Configuration Settings.
  - CM-7 Least Functionality.
  - CM-14 Signed Components.
  - MA-2 Controlled Maintenance.
  - MA-3 Maintenance Tools.
  - MA-6 Timely Maintenance.
  - MA-7 Field Maintenance.
  - SC-3 Isolate Security Functions From Nonsecurity Functions.
  - SC-41 Port and I/O Device Access.
  - SC-45 System Time Synchronization.
- *CIS Controls* safeguards:
  - .5 Allowlist Authorized Software.
  - 2.6 Allowlist Authorized Libraries.
  - 2.7 Allowlist Authorized Scripts.
  - 4.7 Manage Default Accounts on Enterprise Assets and Software.
  - 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts.
  - 6.8 Define and Maintain Role-Based Access Control.

- 7.4 Perform Automated Application Patch Management.
- 8.4 Standardize Time Synchronization.
- 8.5 Collect Detailed Audit Logs.
- 8.10 Retain Audit Logs.
- 12.6 Use of Secure Network Management and Communication Protocols.
- 12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work.
- 13.4 Perform Traffic Filtering Between Network Segments.
- 13.9 Deploy Port-Level Access Control.
- 13.10 Perform Application Layer Filtering.

Communications Management

The processes to manage an organization's communication needs cover end user communication and collaboration tools, as well as facility infrastructure connections to telecommunications service providers. While ERM and technical planning processes establish internal guidelines for communication and collaboration services, controls in this group implement, manage, and support the usage of those services. The ubiquity, versatility, and relatively low cost of IP transmissions have transformed most enterprise communications into data communications.

Prior to mass adoption of the internet (and still in use at some organizations), enterprise networks often included dedicated communication lines to connect local area networks (LANs) in various locations, such as corporate headquarters, regional offices, and retail stores. The resulting collection of dedicated circuits and LANs is called a wide area network (WAN). When organizations associate their data network elements with their IP addresses, network management applications can control a software-defined wide area network (SD-WAN). An SD-WAN can include resources physically managed by the organization or outsourced to some degree, for example to third-party cloud service providers (CSPs).

Network and telecommunications engineers determine the connectivity (voice and data, as well as non-IP connections) and bandwidth needs for each location, including managing wireless access points. An organization's ecosystem of communication and collaboration tools is likely to include several common types. They may include email, internet browsers, Voice over IP, video conferencing, internal or external chat applications, and cloud-based file storage and sharing. An SD-WAN may be used to centrally manage various communication paths, including performing load-balancing, traffic-routing, and security monitoring functions.

Managing the operating relationships with various service providers is a significant concern for this grouping of controls. Performance, cost, and **resilience** factors all contribute to management decisions on which communication and collaboration services to provide the organization.

Controls relevant to managing communication and collaboration services are described in:

- *COBIT 2019 Framework: Governance and Management Objectives* in practices:
    - APO10.02 Select Vendors.
    - APO10.05 Monitor Vendor Performance and Compliance.
    - DSS01.02 Manage Outsourced I&T Services.
    - DSS01.05 Manage Facilities.
    - DSS06.02 Control the Processing of Information.
- *NIST SP 800-53r5* in controls:
    - AC-10 Concurrent Session Control.
    - AC-18 Wireless Access.
    - CP-8 Telecommunications Services.
    - PE-4 Access Control for Transmission.
    - PE-19 Information Leakage.
    - SC-8 Transmission Confidentiality and Integrity.
    - SC-10 Network Disconnect.
    - SC-17 Public Key Infrastructure Certificates.
    - SC-18 Mobile Code.
    - SC-23 Session Authenticity.
    - SC-37 Out-of-Band Channels.
    - SC-40 Wireless Link Protection.
    - SI-8 Spam Protection.
    - SI-14 Non-Persistence.
- *CIS Controls* safeguards:
    - 3.10 Encrypt Sensitive Data in Transit.
    - 9.1 Ensure Use of Only Fully Supported Browsers and Email Clients.
    - 9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions.

Boundary Defense

Historically, network security has been described as “perimeter” defense, based on the prevailing model of an internal network surrounded by the external environment. However, as more functions and services were either outsourced or provided over the internet, the so-called boundary distinctions became less relevant. Network management and cybersecurity (as high-level auditable subjects) have many overlapping objectives, risks, and controls. However, the respective management teams are often separated into IT and IS reporting hierarchies.

Some risks and controls related to protecting technology resources connected to the internet are covered more extensively in the GTAGs "Auditing Cybersecurity Operations: Prevention and Detection," and "Auditing Mobile Computing." However, an audit of network and communications management could include a review of controls that support the following business objectives:

- Connections to external systems — such as outsourced services, including CSPs — are properly authorized and configured.
- Remote connections are adequately **encrypted** and limited to authorized security zones.
- Network-based intrusion prevention and detection systems are implemented to promote confidentiality, data integrity, and service availability.
- The network management team contributes to cybersecurity objectives and processes.

External Connections

When the organization engages with vendors to obtain data or services, a connection between the two enterprise networks (often called an interconnection) is typically established. Like the WAN's history, such connections used to be primarily made with dedicated circuits; however, the connections are now typically made using encrypted services over the internet, such as **virtual private networks (VPNs)**.

Interconnection configuration baselines enable the necessary data exchanges and controls, such as identity verification and authentication services, to provide secure communications. Application programming interfaces (see sidebar) and other services delivered over the internet may also constitute connections to external systems. A review of the management of external connections could verify whether all types, or primarily the ones interfacing with critical systems or handling sensitive data, are covered by adequate controls.

Application Programming Interfaces (APIs)

In NIST SP 800-204 "Security for Microservices," APIs are described as "a contract between clients and services." Basically, an API establishes the details of an information exchange – for example, which fields from a specified database to extract data, perhaps for a specified identity. APIs are managed in applications referred to as **middleware**.

When end users attempt to connect a device to the enterprise network via the internet, commonly referred to as **remote access**, network controls may verify the identities of the person and the device, and ensure that the connection is adequately secured. The risks and controls relevant to remote access are covered in greater detail in the GTAG "Auditing Mobile Computing." However, a review of network and communications management could determine whether network administrators appropriately restrict remote access in the most sensitive security zones, in accordance with internal guidelines and best practices.

Controls over external connections are found mainly in:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - BAI09.02 Manage Critical Assets.
    - DSS05.02 Manage Network and Connectivity Security.
    - DSS05.03 Manage Endpoint Security.
- *NIST SP 800-53r5* controls:
    - AC-17 Remote Access.
    - AC-19 Access Control for Mobile Devices.
    - AC-20 Use of External Systems.
    - AU-16 Cross-Organizational Audit Logging.
    - CA-3 Information Exchange.
    - SC-7 Boundary Protection.
- *CIS Controls* safeguards:
    - 12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure.
    - 13.5 Manage Access Control for Remote Assets.

Network Security

Network security, broadly conceived, could include many of the controls mentioned throughout this guide. However, network security controls can be more narrowly defined as designed to achieve the following business objectives:

- Security technologies, such as network-based intrusion prevention and detection systems and anti-malware software, are implemented to protect resources in accordance with their risk-based categorizations.
- Security event logs are configured to capture data about significant actions, such as attempts to access sensitive resources or deactivate authentication or logging controls, with enough information to promote individual accountability.
- Network management personnel work with IS teams to test controls and remediate any significant vulnerabilities identified. Joint efforts also monitor for anomalous activities, including service impairments, and perform investigative and remedial actions.

Network security controls are described in the subcontrols of some of the guidance cited previously, such as COBIT 2019 Practice "DSS05.02 Manage Network and Connectivity Security," as well as in:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - APO13.02 Define and Manage an Information Security Risk Treatment Plan.
    - APO13.03 Monitor and Review the Information Security Management System (ISMS).
    - DSS05.01 Protect Against Malicious Software.

    - DSS05.07 Manage Vulnerabilities and Monitor the Infrastructure for Security-related Events.
- *NIST SP 800-53r5* controls:
    - AU-6 Audit Record Review, Analysis, and Reporting.
    - AU-14 Session Audit.
    - CA-8 Penetration Testing.
    - RA-5 Vulnerability Monitoring and Scanning.
    - SC-5 Denial-of-Service Protection.
    - SC-31 Covert Channel Analysis.
    - SC-35 External Malicious Code Identification.
    - SI-3 Malicious Code Protection.
    - SI-5 Security Alerts, Advisories, and Directives.
- *CIS Controls* safeguards:
    - 4.5 Implement and Manage a Firewall on End-User Devices.
    - 8.6 Collect DNS Query Audit Logs.
    - 8.7 Collect URL Request Audit Logs.
    - 8.11 Conduct Audit Log Reviews.
    - 8.12 Collect Service Provider Logs.
    - 9.2 Use DNS Filtering Services.
    - 9.3 Maintain and Enforce Network-Based URL Filters.
    - 9.5 Implement DMARC.
    - 9.6 Block Unnecessary File Types Attempting to Enter the Enterprise's Email Gateway.
    - 9.7 Deploy and Maintain Email Server Anti-Malware Protections.
    - 10.1 Deploy and Maintain Anti-Malware Software.
    - 10.5 Enable Anti-Exploitation Features.
    - 10.7 Use Behavior-Based Anti-Malware Software.
    - 13.3 Deploy a Network Intrusion Detection Solution.
    - 13.8 Deploy a Network Intrusion Prevention Solution.
    - 18.3 Remediate Penetration Test Findings.

Network Operations

The performance and availability of the data and communications ecosystem needs to be monitored, with issues resolved effectively and efficiently. Network operations teams typically work with system support teams to ensure computing infrastructure, databases, applications,

and other resources are monitored for various service issues. Those issues generally include power, internet connectivity, system processing and capacity utilization status, and other environmental and operational metrics.

Resolving such issues usually requires a coordinated effort between network operations and other teams, though management reporting on service issues is often one of the responsibilities of the network team. Ideally, monitoring and reporting are performed by a centralized function, such as a NOC, for greater efficiency and conformance with internal policies and procedures.

Business resilience objectives for the data network ecosystem largely consist of ensuring redundant, failover, and emergency communication capabilities, as well as developing and testing contingency plans. In some organizations, the responsibility for leading business resilience planning efforts may be assigned to network operations personnel.

Monitoring and Operations Assistance

Monitoring is often performed by a centralized function, which may or may not be physically located in a NOC. Some types of network traffic and system usage monitoring are performed by network security and IS teams; however, the monitoring usually associated with network operations contributes primarily to service availability, rather than security, objectives.

Nevertheless, some types of cyberattacks result in traffic anomalies or disruptions to network functions, including changing configuration settings. Therefore, network monitoring processes should be coordinated with security controls to identify potential cyber incidents in a timely manner.

Network operations personnel typically support — and in some cases, own — the technology change management process. While such risks and controls are described in more detail in the GTAG "IT Change Management, 3rd Edition," an audit of network and communications management could review the processes used to manage changes to the network infrastructure, including updates to hardware operating systems and other relevant network management applications.

Network monitoring and operations assistance controls are described in:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - BAI06.02 Manage Emergency Changes.
    - DSS01.03 Monitor I&T Infrastructure.
    - DSS02.04 Investigate, Diagnose and Allocate Incidents.
    - DSS02.05 Resolve and Recover From Incidents.
    - DSS03.01 Identify and Classify Problems.
    - DSS03.02 Investigate and Diagnose Problems.
    - DSS03.03 Raise Known Errors.
    - DSS03.04 Resolve and Close Problems.

- *NIST SP 800-53r5* controls:
    - AU-5 Response to Audit Logging Process Failures.
    - CA-7 Continuous Monitoring.
    - CP-10 System Recovery and Reconstitution.
    - IR-4 Incident Handling.
    - IR-7 Incident Response Assistance.
    - IR-9 Information Spillage Response.
    - MA-4 Nonlocal Maintenance.
    - SC-24 Fail in Known State.
    - SI-2 Flaw Remediation.
    - SI-4 System Monitoring.
    - SI-6 Security and Privacy Function Verification.
    - SI-7 Software, Firmware, and Information Integrity.
    - SI-11 Error Handling.
- *CIS Controls* safeguards:
    - 1.2 Address Unauthorized Assets.
    - 1.3 Utilize an Active Discovery Tool.
    - 13.6 Collect Network Traffic Flow Logs.
    - 15.6 Monitor Service Providers.
    - 17.1 Designate Personnel to Manage Incident Handling.
    - 17.7 Conduct Routine Incident Response Exercises.

Resilience

Network and communications management personnel are often prominently involved in resilience planning efforts, sometimes referred to as business continuity or **disaster recovery** planning. In some organizations, resilience program ownership may be delegated to a member of network management. Additionally, the network hardware, software, and communication services are critical infrastructure elements that typically have contingency plans, redundant or alternate paths, and geographic distribution capabilities to enhance their resilience. Technology resilience risks and controls are described in more detail in the GTAGs "Auditing Cyber Incident Response and Recovery," and "Business Continuity Management."

Resilience controls for network and communications services mainly consist of contingency planning for the relevant hardware, software, and services. The contingency plans are developed, tested, and refined in response to experience and changes in the ecosystem. The contingency plans may include procuring redundant connections to facilities or planning alternate means of communications, such as personal cell phones, in case the enterprise network is unavailable.

The CIS v.8 framework does not contain any safeguards related to network and communications contingency planning or resilience, although there are a few related to data recovery processes. The CIS v.8 focuses primarily on controls most likely to prevent, detect, or respond to the most common cyberattacks and is not presented as a comprehensive framework of IT-IS controls.

Controls over resilience for network and communications services can be found in:

- *COBIT 2019 Framework: Governance and Management Objectives* practices:
    - DSS03.05 Perform Proactive Problem Management.
    - DSS04.02 Maintain Business Resilience.
    - DSS04.03 Develop and Implement a Business Continuity Response.
    - DSS04.04 Exercise, Test and Review the **Business Continuity Plan (BCP)** and Disaster Response Plan (DRP).
- *NIST SP 800-53r5* controls:
    - CP-2 Contingency Plan.
    - CP-3 Contingency Training.
    - CP-4 Contingency Plan Testing.
    - CP-11 Alternate Communications Protocols.
    - CP-12 Safe Mode.
    - PE-18 Location of System Components.
    - SC-29 Heterogeneity.
    - SC-36 Distributed Processing and Storage.
    - SC-47 Alternate Communications Paths.
    - SI-17 Fail-safe Procedures.

Conclusion

Every organization that connects their computing infrastructure to the communications network has inherent risks related to the confidentiality, integrity, and availability of resources that constitute or travel across the network. For internal auditors to provide valuable assurance and consulting services regarding the objectives, risks, and controls over network and communications management, it is necessary to understand the key processes and controls. Network and communications management risks and controls can be conceptually organized according to the model of governance, risk management, and internal controls provided in the *Standards*. The groupings of risks and controls presented in this guide include references to detailed entries in widely used IT-IS control frameworks. These entries can help internal auditors find the additional information they need to build tailored audit programs and meaningful tests of control adequacy and effectiveness.

Appendix A. Relevant IIA Standards and Guidance

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

Code of Ethics
Principle 1: Integrity
Principle 2: Objectivity
Principle 3: Confidentiality
Principle 4: Competency
Standards
Standard 1200 – Proficiency and Due Professional Care
Standard 1210 – Proficiency
Standard 2010 – Planning
Standard 2030 – Resource Management
Standard 2110 – Governance
Standard 2120 – Risk Management
Standard 2130 – Control
Standard 2201 – Planning Considerations
Standard 2220 – Engagement Scope
Guidance and Other IIA Resources
GTAG "Auditing Business Applications," 2020
GTAG "Auditing Cyber Incident Response and Recovery," 2022
GTAG "Auditing Cybersecurity Operations: Prevention and Detection," 2022
GTAG "Auditing Identity and Access Management," 2021
GTAG "Auditing Mobile Computing," 2022
GTAG "Business Continuity Management," 2008
GTAG "IT Change Management: Critical for Organizational Success," 2020
GTAG "IT Essentials for Internal Auditors," 2020
The Institute of Internal Auditors: *The IIA's Three Lines Model: An Update of the Three Lines of Defense*, 2020.

Appendix B. Glossary

Definitions of terms marked with an asterisk are taken from the "Glossary" of The IIA's publication "*International Professional Practices Framework*® 2017 edition" (also known as the Red Book), published by the Internal Audit Foundation. Other sources are either defined for the purposes of this document or derived from the following sources:

- ISACA, Glossary, https://www.isaca.org/resources/glossary.
- NIST, Computer Security Resource Center Glossary. https://csrc.nist.gov/glossary.
- *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5*, Glossary. https://doi.org/10.6028/NIST.SP.800-53r5.
- *NIST SP 800-215: Guide to a Secure Enterprise Network Landscape.* https://doi.org/10.6028/NIST.SP.800-215.
- The IIA, Internal Auditing: Assurance and Advisory Services, 5th Edition (IIA textbook). https://www.theiia.org/en/products/bookstore/internal-auditing-assurance-and-advisory-services-5th-edition/.
- The IIA, Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value, 7th Edition (Sawyer's). https://www.theiia.org/en/products/bookstore/sawyers-internal-auditing-enhancing-and-protecting-organizational-value-7th-edition/.

application – A computer program or set of programs that performs the processing of records for a specific function. Contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort [ISACA Glossary].

assurance (services)* – An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system [NIST SP 800-53r5 Glossary].

availability – Ensuring timely and reliable access to and use of information. [NIST SP 800-53r5 Glossary].

bandwidth – The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity of an electronic line and is expressed in bytes per second or Hertz (cycles per second) [ISACA Glossary].

baseline configuration – A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures [NIST SP 800-53r5 Glossary].

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).

business continuity plan (BCP) – A plan used by an enterprise to respond to disruption of critical business processes; depends on the contingency plan for restoration of critical systems [ISACA Glossary].

business rules – Representations of business processes and constraints that are encoded into applications to fulfill user requirements.

compliance* – Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

confidentiality – Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information [ISACA Glossary].

configuration – The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged [NIST Glossary].

consulting services* – Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

control* – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient action to provide reasonable assurance that objectives and goals will be achieved.

control environment* – The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organizational structure.

- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

control framework – A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an enterprise [ISACA Glossary].

control processes* – The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

data classification – The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored, or transmitted. The classification level is an indication of the value or importance of the data to the enterprise [ISACA Glossary].

data loss prevention – A systems ability to identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of information [Adapted from NIST Glossary].

denial of service – The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) [NIST Glossary].

disaster recovery – Activities and programs designed to return the enterprise to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan (DRP) to restore an enterprise's critical business functions [ISACA Glossary].

domain – An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See Security Domain [NIST Glossary].

domain name – A label that identifies a network domain using the Domain Naming System [NIST Glossary].

Domain Name System (DNS) – A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers [ISACA Glossary].

encrypted (or encryption) – The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext). [ISACA Glossary].

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.

engagement objectives* – Broad statements developed by internal auditors that define intended engagement accomplishments.

enterprise architecture – Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support the enterprise's objectives [ISACA Glossary].

enterprise risk management (ERM) – A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives [Sawyer's].

event log – A chronological record of system activities, like access attempts, role creation, user account creation or deactivation, etc. [adapted from "audit log" entry in *NIST SP 800-53r5* Glossary].

exposure – The potential loss to an area due to the occurrence of an adverse event [ISACA Glossary].

failover – The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system [NIST Glossary].

firewall – A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the internet [ISACA Glossary].

gateway – A physical or logical device on a network that serves as an entrance to another network (e.g. router, firewall or software) [ISACA Glossary].

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.

host – A host is any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, personal electronic devices, thin clients, and multi-functional devices [NIST Glossary].

identity – The set of physical and behavioral characteristics by which an individual is uniquely recognizable. Note: This also encompasses non-person entities (NPEs) [NIST Glossary].

information security – Ensures that, within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and nonaccess when required (availability) [ISACA Glossary].

information technology controls* – Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.

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.

inherent risk – The combination of internal and external risk factors in their pure, uncontrolled state, or the gross risk that exists, assuming there are no internal controls in place [IIA textbook].

integrity [of systems or data] – The guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity [ISACA Glossary].

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.

internet protocol (IP) addresses – Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks [NIST Glossary].

internet service providers (ISPs) – A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services [ISACA Glossary].

least privilege – The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function [NIST Glossary].

metadata – Information describing the characteristics of data. This may include, for example, structural metadata describing data structures (i.e., data format, syntax, semantics) and descriptive metadata describing data contents [NIST Glossary].

microsegmentation – A security design practice where an internal network (e.g., in the data center, cloud provider region) is divided into isolated segments so that the traffic in and out of each segment can be monitored and controlled [NIST SP 800-215].

middleware – Another term for an application programmer interface (API). It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services [ISACA Glossary].

multi-factor authentication – An authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multi-factor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are [adapted from *NIST SP 800-53r5* Glossary].

network – A system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices [*NIST SP 800-53r5* Glossary].

network address translation (NAT) – A methodology of modifying network address information in IP datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another [ISACA Glossary].

network administrator – Responsible for planning, implementing and maintaining the telecommunications infrastructure; also may be responsible for voice networks. Scope Notes: For smaller enterprises, the network administrator may also maintain a local area network (LAN) and assist end users [ISACA Glossary].

network segmentation – A common technique to implement network security that segments and enterprise network into separate zones that can be separately controlled, monitored, and protected [ISACA Glossary].

objectives – What an entity desires to achieve. When referring to what an organization wants to achieve, these are called business objectives, and may be classified as strategic, operations, reporting, and compliance. When referring to what an audit wants to achieve, these are called audit objectives or engagement objectives [IIA textbook].

patch – Fixes to software programming errors and vulnerabilities [ISACA Glossary].

policy enforcement point (PEP) – Mechanism (e.g., access control mechanism of a file system or Web server) that actually protects (in terms of controlling access to) the resources exposed by Web services [NIST Glossary].

port (port number) – A process or application-specific software element serving as a communication endpoint for the transport layer IP protocols (UDP and TCP) [ISACA Glossary].

privacy – The right of an individual to trust that others will appropriately and respectfully use, store, share, and dispose of his or her associated personal and sensitive information within the context, and according to the purposes for which it was collected or derived. Scope notes: What is appropriate depends on the associated circumstances, laws, and the individual's reasonable expectations. An individual also has the right to reasonably control and be aware of the collection, use, and disclosure of his or her associated personal and sensitive information [adapted from ISACA Glossary].

protocol – The rules by which a network operates and controls the flow and priority of transmissions [ISACA Glossary].

remote access – Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network [*NIST SP 800-53r5* Glossary].

residual risk – The portion of inherent risk that remains after management executes its risk responses (sometimes referred to as net risk) [IIA textbook].

resilience – The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect [ISACA Glossary].

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 assessment – The identification and analysis (typically in terms of impact and likelihood) of relevant risks to the achievement of an organization's objectives, forming a basis for determining how the risks should be managed [IIA textbook].

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.

rogue IT – Technology resources not managed by the IT function, often indicating non-compliance with internal policies.

router – A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the open systems interconnection (OSI) model. Scope Notes: Networks connected by routers can use different or similar networking protocols. Routers usually are capable of filtering packets based on parameters, such as source addresses, destination addresses, protocol and network applications (ports) [ISACA Glossary].

security categorization – The process of determining the security category for information or an information system [adapted from NIST Glossary].

security domain – A domain within which behaviors, interactions, and outcomes occur and that is defined by a governing security policy. Note: A security domain is defined by rules for users, processes, systems, and services that apply to activity within the domain and activity with similar entities in other domains [NIST Glossary].

server – A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries) [NIST Glossary].

session – A persistent interaction between a subscriber and an endpoint, either an RP or a CSP. A session begins with an authentication event and ends with a session termination event. A session is bound by use of a session secret that the subscriber's software (a browser, application, or OS) can present to the RP or CSP in lieu of the subscriber's authentication credentials [NIST Glossary].

strategy – Refers to how management plans to achieve the organization's objectives [IIA textbook].

virtual private network (VPN) – A secure private network that uses the public telecommunications infrastructure to transmit data. Scope Notes: In contrast to a much more expensive system of owned or leased lines that can only be used by one enterprise, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two internet points, maintaining privacy and security [ISACA Glossary].

Appendix C. References

Center for Internet Security. "The 18 CIS Critical Security Controls," interactive guide to CIS Controls, Version 8. https://www.cisecurity.org/controls/cis-controls-list/.

Chandramouli, Ramaswamy. *NIST SP 800-204: Security Strategies for Microservices-based Application Systems*. Gaithersburg, MD: NIST, August 2019. https://doi.org/10.6028/NIST.SP.800-204.

Chandramouli, Ramaswamy. *NIST SP 800-215: Guide to a Secure Enterprise Network Landscape*. Gaithesburg, MD: NIST, November 2022. https://doi.org/10.6028/NIST.SP.800-215.

Chandramouli, Ramaswamy and Scott Rose. *NIST SP 800-81.-2: Secure Domain Name System (DNS) Deployment Guide*. Gaithersburg, MD: NIST, September 2013. http://dx.doi.org/10.6028/NIST.SP.800-81-2.

Dempsey, Kelley, Victoria Pillitteri, and Andrew Regenscheid. *NIST SP 800-47: Managing the Security of Information Exchanges, Revision 1*. Gaithersburg, MD: NIST, July 2021. https://doi.org/10.6028/NIST.SP.800-47r1.

ICANN. *Beginner's Guide to Domain Names*. https://www.icann.org/resources/pages/beginners-guides-2012-03-06-en.

ICANN. *Beginner's Guide to Internet Protocol (IP) Addresses*. https://www.icann.org/resources/pages/beginners-guides-2012-03-06-en.

ISACA. *COBIT: An ISACA Framework*. 2022. https://www.isaca.org/resources/cobit.

ISACA. Glossary. 2022. https://www.isaca.org/resources/glossary.

Joint Task Force. *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5*. Gaithersburg, MD: NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

McKay, Kerry A., and David A. Cooper. *NIST SP 800-52: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Revision 2*. Gaithersburg, MD: NIST, August 2019. https://doi.org/10.6028/NIST.SP.800-52r2.

Montgomery, Doug, Mark Carson, Timothy Winters, Michayla Newcombe, and Timothy Carlin. *NIST SP 500-267A: NIST IPv6 Profile, Revision 1*. Gaithersburg, MD: NIST, November 2020. https://doi.org/10.6028/NIST.SP.500-267Ar1

Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. *NIST SP 800-207: Zero Trust Architecture*. Gaithersburg, MD: NIST, August 2020. https://doi.org/10.6028/NIST.SP.800-207.

Scarfone, Karen and Paul Hoffman. *NIST SP 800-41: Guidelines on Firewalls and Firewall Policy* Revision 1. Gaithersburg, MD: NIST, September 2009. https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final.

Sedgewick, Adam, Murugiah Souppaya, and Karen Scarfone. *NIST SP 800-167: Guide to Application Whitelisting*. Gaithersburg, MD: NIST, October 2015. http://dx.doi.org/10.6028/NIST.SP.800-167.

Sriram, Kotikalapudi and Doug Montgomery. *NIST SP 800-189: Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*. Gaithersburg, MD: NIST, December 2019. https://doi.org/10.6028/NIST.SP.800-189.

The Institute of Internal Auditors. *International Professional Practices Framework*. 2017 ed. The IIA, 2017. https://www.theiia.org/en/products/bookstore/international-professional - practices-framework---ippf---2017-edition/.

Acknowledgements

IT Guidance Development Team

Jim Enstrom, CIA, United States

Uday Gulvadi, CIA, CPA, CISA, United States

Ruth Mueni Kioko, CIA, Kenya

Avin Mansookram, CISA, CGEIT, South Africa

Scott Moore, CIA, CISA, CRISC, GSLC, United States

Manoj Satnaliwala, CIA, CPA, CISA, United States

Terence Washington, CIA, CRMA, United States

Dennis Wong, CIA, CFSA, United Kingdom

Global Guidance Council Reviewers

Nur Hayati Baharuddin, CIA, CCSA, CFSA, CGAP, CRMA, Malaysia

Larry Herzog Butler, CIA, CRMA, CPA, Germany

Emmanuel Johannes, CIA, CCSA, CGAP, Tanzania

Klaus Rapp, CIA, CRMA, Switzerland

Carolyn Saint, CIA, CRMA, CPA, United States

International Internal Audit Standards Board Reviewers

Naji Fayad, CIA, Saudi Arabia

Hans-Peter Lerchner, CIA, CRMA, Austria

IIA Global Standards and Guidance

David Petrisky, CIA, CRMA, CPA, CISA, Director, (Project Lead)

Katleen Seeuws, CIA, CGAP, CRMA, Vice President

Dr. Lily Bi, CIA, QIAL, CRMA, CISA, Executive Vice President

Anne Mercer, CIA, CFSA, CFE, Senior Director

Jill Austin, Senior Manager

Shelli Browning, Associate Manager, Technical Writer

Geoffrey Nordhoff, Content Writer and Technical Editor

The IIA would like to thank the following oversight bodies for their support: Information Technology Knowledge Group, Global Guidance Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors is a nonprofit international professional association that serves more than 218,000 global members and has awarded 180,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized as the internal audit profession's leader in standards, certification, education, research, and technical guidance throughout the world. Learn more at www.theiia.org.

Disclaimer

Copyright

January 2023

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