Mastering the IT Audit

Assuring a resilient and compliant IT landscape through effective audit

Jyothi Ramaswamy

www.bpbonline.com

First Edition 2026

ISBN: 978-93-65893-274

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

To View Complete
BPB Publications Catalogue
Scan the QR Code:

www.bpbonline.com

Dedicated to

My seniors and colleagues

About the Author

Jyothi Ramaswamy is a seasoned risk, security, audit, and compliance professional with over 25 years of experience in the information security domain. Her career spans a distinguished tenure at Tata Consultancy Services Ltd., where she specialized in defining, implementing, reviewing, and auditing controls across complex IT environments. Currently operating as a freelance consultant, auditor, and trainer, Jyothi brings expertise in auditing diverse facets of organizational process management, particularly in the realms of information security and data privacy. Her consulting work is rooted in global standards, with a strong focus on ISO 27001, ISO 20000, ISO 9001, ISO 27701, and CIS controls.

Jyothi is a passionate educator and a certified trainer, known for delivering impactful sessions on cybersecurity, service and quality management, and regulations. Her audit experience spans enterprise networks, firewall-segregated infrastructures, and air-gapped systems. She has played key roles in ISO audits, SSAE assessments, third-party risk evaluations, and internal audits across various business functions. A committed member of professional bodies such as ISACA, IEEE, and GCA, Jyothi actively contributes to local chapters and has led numerous awareness programs on data privacy, cyber risk, and audit methodologies. Her credentials include ISO 27001:2022 Lead Auditor, CRISC – Certified in Risk and Information Systems Control, CISM – Certified Information Security Manager, CRISP – Certified Risk Professional, BS 7799 Lead Implementer, and APMG accredited ISACA Chapter Trainer for CISM and CRISC certifications.

Known for her collaborative spirit, sharp analytical skills, and problem-solving capabilities, Jyothi continues to contribute to the future of audit and security through her thought leadership and hands-on expertise.

About the Reviewers

- **Nikhil Deshmukh** is a senior IT auditor and a certified information system auditor (CISA). He is currently responsible for Governance, Risk, and Compliance (GRC), cybersecurity audits, and AI audits. Nikhil is also focused on infrastructure security assessment, ensuring robust protection and compliance across IT environments. An active reader, he engages with a wide range of IT-related literature and hosts podcasts on IT audits, sharing insights and developments in the field. Additionally, Nikhil has delivered seminars on IT security and information security, contributing to the broader discourse on safeguarding digital assets and systems.

- **Dinesh Kumar Budagam** is a seasoned IT professional with over 15+ years of experience across diverse domains within the technology sector. His expertise spans Microsoft technologies, Hadoop-based Big Data systems, data engineering, cloud security, privacy, and cybersecurity.

  Over the course of his career, Dinesh held key technical and leadership roles at prominent organizations, including IBM, where he was a core contributor, and served as a consultant to major tech leaders such as Microsoft and Meta. Dinesh began his professional journey as a developer and steadily progressed through roles including technical lead and senior technical manager.

  Currently, he serves as a senior manager and senior cybersecurity consultant at VISA, where he specializes in cybersecurity and functions as a security architect. In this capacity, Dinesh led strategic initiatives aimed at protecting the organization's most critical digital assets. His responsibilities include designing and implementing advanced security frameworks and strategies for Big Data and cloud environments and focusing on ensuring these platforms remain secure, compliant, and resilient to emerging cyber threats.

  Dinesh holds a bachelor of technology in electrical and electronics engineering (2005) and a master's degree in software engineering (2008), which together provide a strong foundation for his technical and analytical capabilities. Additionally, he is a certified IBM solution architect for Big Data analytics, certified cloud architect, certified system architect and is a senior IEEE member. Dinesh completed Advance CyberSecurity and Generative AI: Technology, Business, and Society Program professional certificate program from Stanford University and has published a textbook on Oracle Cloud Infrastructure Security Handbook and Journals on Cybersecurity/AI.

- **Sanyam Jain** is a globally recognized security engineering leader and cybersecurity thought leader, known for securing complex digital ecosystems and enhancing resilience across cloud-native environments. With deep expertise in cloud security, security operations, application security, compliance, and security automation, he helps enterprises and startups exceed their security goals through strategic foresight and technical depth.

  He brings a DevSecOps-first approach, designing secure architectures, embedding security in CI/CD, and automating compliance. His technical skills span threat detection, Kubernetes security, identity and access management, encryption, and network security across AWS, Azure, and Google Cloud. Sanyam is well-versed in ISO 27001, SOC 2, SOX, HITRUST, GDPR, HIPAA, PCI DSS, and NIST CSF, enabling secure-by-design implementations that meet audit requirements. His research has appeared in Forbes, TechCrunch, ZDNet, and more. He serves as a Judge for Globee® Awards, mentors through NITI Aayog, advises startups, and supports NGOs like GDI Foundation. He reviews technical books for several publishing houses and has mentored thousands via Udacity and other platforms. Sanyam holds a Master's from BITS Pilani and is a Certified Kubernetes Administrator.

Acknowledgement

I want to express my heartfelt gratitude to those who have stood by me throughout this journey, both personally and professionally.

To my family, thank you for your unwavering support, patience, and belief in me. Your encouragement has been the quiet strength behind every milestone and every chapter of this book. I want to thank my father, who taught me to keep learning throughout life, my mother and sisters who supported me relentlessly, my husband who motivated me to take all challenges that came my way, and last but not least, my daughter who lived through my *change approver* mindset.

I am also deeply thankful to my seniors from Tata Consultancy Services Ltd. Trivandrum during my early career, who instilled the habit of excelling in all activities. They provided guidance, vision, and support throughout my professional journey. My supervisors and colleagues from the information security team and the delivery excellence team require a special mention here for helping me learn to look at the bigger picture and cultivate the habit of reviewing solutions, keeping the business context in mind. I would like to acknowledge the support from the cybersecurity service delivery team, my managers, team members, and customer managers, who have helped me in strengthening the governance mindset. The lessons I learned under your direction have echoed through every stage of my growth, and I am very grateful for your support; I will always be thankful for the lessons that you taught me. This book is, in many ways, a reflection of those early lessons and the people who helped instill them.

Preface

Throughout this book, we explain why an IT audit is important in helping an organization strengthen its IT infrastructure, mitigate potential outages in operations, and identify areas for improvement. The major steps here are risk identification and mitigation; assessment of resilience; geography and industry compliance verification; data and platform protection; and last but not least, assuring governance mechanisms through proper documentation and reporting. Audit process requires understanding of the IT landscape, perimeter setup, and various upstream and downstream connectivity. The landscape covers the various appliances, firewall, IDS and IPS, servers, network devices, their configuration, and maintenance. Capacity management, incident management and change management are the main governance activities that stitch the responsibilities of the IT team of any organization. In addition to these, the auditor has to understand the security policies, the patching practices, and the segregation of networks to manage different access levels to different teams.

Once one becomes an IT auditor, they will be able to provide value to managing the backbone of the organization by ensuring security, availability, and integrity of operations and data within their organization. This helps in career growth in the IT service, operation, strategic, and project management roles. Auditors possess a deep understanding of systems, controls, and vulnerabilities. With the right mindset and skill-building, they can evolve into engineers who design secure, efficient, and compliant systems from the ground up.

Chapter 1: IT Audit and Assurance Standards Statements- Key concepts such as auditing, deciding the criteria, and risk-based approach to audits, etc., are explained. It also covers the principles of auditing, due professional care, conflict of interest, and independence.

Chapter 2: IT Audit Defined, Charter and Criteria- Highlights the benefits of the audit process, e.g., improved management system performance, enhanced credibility and trust, better risk management, and increased organizational efficiency.

Chapter 3: Planning, Scheduling, Reporting and Follow-ups for Audit- Steps of conducting an audit: entry meeting, gathering audit evidence, document review, interview techniques, and observations, site inspections are introduced here. We will learn the process of managing an audit program for the IT department and the operations of an organization.

Chapter 4: Types of Audits- Types of audits are explained herewith, like internal audits, external audits, first-party audits, second-party audits, and third-party audits.

Chapter 5: IT Policies, Processes and SOPs- How the policies, processes and operating procedures are defined for typical tasks to be managed by the IT team. We will also get the view of the roles and their responsibilities, helping us to focus on the operational aspects of the IT operations.

Chapter 6: Risk Management and Impact Analysis- The key risk areas relevant to the systems and processes are identified. We see how common risk areas are analyzed, including cybersecurity vulnerabilities, system availability, data backups, and disaster recovery capabilities. Risk management is to be carried out based on the impact on the specific industry and business requirements.

Chapter 7: Procurement, Asset, Capacity and Cloud Service Management- IT policies have to look at the complete life cycles of the equipment, starting with procurement, configuration, defining and implementing procedures, inventorising of assets by marking critical equipment and finally managing EOL for this equipment. IT policies should also focus on interconnection of equipment, access management, monitoring usage to ensure capacity management, and build-in continuity by managing backup systems.

Chapter 8: Access Management and Acceptable Usage Policy- Access management in an organization is the virtue of how well the organization functions when it comes to the authorization of assets to users. Acceptable use policy gives the dos and don'ts and outlines the expectations for how employees and other authorized users should interact with the assets.

Chapter 9: Network, Server, Storage and End Point Management- This chapter talks about process of monitoring and maintaining network devices, servers and storage devices, to optimize the performance. This has to encompass the management of hardware, software, security, and backups to minimize slowdowns and downtime.

Chapter 10: Business Continuity and Disaster Recovery Planning- BCP and DRP provides assurance of IT infrastructure being available for delivering the required services during disruptive events, such as natural disasters, cyberattacks and communication failures, etc. Planning continuity looks at critical services and also takes inputs from asset inventory for critical assets.

Chapter 11: Organization Context and IT Services- IT operation management processes are essential to ensure meeting service requirements, and to continually improve service management. Ensuring information security becomes an integral part of managing IT operations. Business context defines how IT supports the business mission and operations, and how to plan IT strategies and initiatives.

Chapter 12: Logging and Monitoring Services- Through logging of events and activities within a system or application, user actions and error messages are captured. Monitoring helps in measuring the performance and health of a system, such as resource usage, network traffic, and error rates. This helps in designing corrective and preventive actions for process improvements.

Chapter 13: KPIs and Status Reports- This chapter talks about creating guidelines for designing, planning, implementing, continuous testing, improving the processes in an ongoing manner, and governing the complete enterprise IT architecture. Criticality of the assets give inputs to KPIs and governance measures through status reports.

Chapter 14: BCP Drills, Plans and Reports- IT team conducts simulated exercises that test the effectiveness of the business's BCP. After every BCP drill, the business continuity team analyzes and reports the effectiveness of continuity measures. The learnings from drills go as feedback to the various operating procedures.

Chapter 15: Configuration and Change Management- This helps in ensuring that changes to an organization's technical environment are documented and managed in a structured manner. In change management, changes to applications and hardware are tracked, while configuration management focuses on how the physical attributes of application or systems are consistently maintained and managed.

Chapter 16: IT Audit Frameworks ISO 20000 and ITIL– This chapter focuses on how IT audits begins with deciding the audit framework, identifying the aims and benefits of framework, understand the compliance requirements, benefits of audits, etc. The difference between ITIL as a framework and ISO as a certification will also be covered here.

Chapter 17: Organizations, People, Data and Technology Processes– During an IT audit, auditors have to focus on the effectiveness, reliability, and security of an organization's IT infrastructure, systems, and processes. IT audit comprises a review of asset safeguarding practices, namely, data, application systems, technology, and people.

Chapter 18: Partners, Value Streams and Processes- Partner audit focuses on assessing the partner or vendor's past project performance, technical expertise, compliance with industry standards, and financial stability in ensuring uninterrupted services. Value stream analysis can help evaluate the current way of working, identify new requirements, and propose improvements.

Chapter 19: Scope of Audit, and Audit Plan- Audit planning should define the role and responsibilities of an auditor, and also should include all the entities in the enterprise landscape, including external stakeholders. The apex processes of the organization like information security and quality management systems, need to be included in audit process along with IT policies and operation processes, to ensure IT processes are in alignment. Data at rest and in transit has to be checked for the sensitivity, to see whether the processes around them are adequate.

Chapter 20: Review of Policy and Controls- Purpose of the audit function is to evaluate and test the design (ToD) and execution of controls implemented for effectiveness (ToE) by processes surrounding the business operations. Scope of the audit has to be defined either to the entire enterprise or to a specific entity within the enterprise ad all relevant policies surrounding the operations of IT team has to be reviewed along with the governance mechanism in place.

Chapter 21: Interviews, Site Visits and Technical Testing- Status reports and actions on any deviation from threshold has to be given adequate importance as this provides inputs to ToE. Site visits to data centre, support systems like UPS, power backup, access control and CCTV monitoring area etc give inputs to effectiveness of processes put in place. Conflict of interest is another area to be checked thoroughly for ensuring ToE.

Chapter 22: Audit Findings and Actionable Audit Report- An audit report must be well-written to effectively stand out, capture interest, and promote changes. Audit report should illustrate non-conformities, outline positives, call out opportunities for improvement, and should be translatable to actions to close non-conformities.

Chapter 23: Evolving with the Audit Landscape- This chapter provides a conclusion to all areas that have been covered in the book, along with some guidelines on how to plan the audit and prepare a proper audit report with actionable observations. This will also mention how the remediation can be planned on audit observations, and verification audit has to be conducted to cross check the reediation measures taken as a result of audit.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/32e9bb

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at:

errata@bpbonline.com

Your support, suggestions and feedback are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our Discord space

Join our Discord workspace for latest updates, offers, tech happenings around the world, new releases, and sessions with the authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
IT Audit and Assurance Standards Statements

Introduction

In this chapter, key concepts such as auditing, deciding the criteria, and a risk-based approach to audits are explained. It also covers the principles of auditing, due professional care, conflict of interest, independence, etc. IT audits and assurance statements are vital tools for ensuring that IT systems are secure, reliable, and compliant. They empower organizations to build a resilient IT infrastructure, safeguard their data, and earn the trust of their stakeholders in an increasingly digital world.

In today's interconnected world, **information technology** (**IT**) is the backbone of almost every business operation. However, with its benefits come risks, such as data breaches, system failures, and compliance challenges. This is where IT audits and assurance statements play a critical role. By prioritizing IT audits, organizations can navigate the complex IT landscape with confidence and turn potential risks into opportunities for growth and improvement.

An IT audit is a detailed evaluation of an organization's IT systems, infrastructure, policies, and operations. Its purpose is to ensure alignment with business goals while complying with relevant regulations. These audits are essential for identifying vulnerabilities, managing risks, and maintaining data security.

Through IT audit learning, one gains skills in various process frameworks, the ability to assess risks systematically, and expertise in tools used for auditing IT environments. Staying updated on compliance requirements and developing actionable solutions for audit findings are also critical outcomes. IT auditing is vital in today's rapidly evolving digital landscape to ensure efficiency, security, and regulatory adherence.

Structure

The chapter covers the following topics:

- Key concepts
- Components of IT management
- Core standards for IT audits
- Assurance statements
- Regulatory compliance requirements

Objectives

This chapter aims to introduce the readers to the concept of the IT audit process and take them through the basic components of IT management, core standards for IT audits, and regulatory compliance requirements. The components of IT management will help the auditor to have a critical look at how the organization's structure is set up, and the standards allow the auditor to decide the applicable controls that need to be checked during the audit. The regulatory compliance requirements are the driving factor for setting up controls and the periodicity of the audit process. Together, all these will create an environment which functions well, is managed well and is subjected to periodic reviews. We will see how these will help in addressing the credibility requirements for an organization.

This chapter contains an introduction to the audit process for first-time auditors and helps them to visualize the audit being conducted. We will also see the outcome of audits, i.e., the assurance statements obtained from different types of audits. By the end of this chapter, we will have obtained an introduction to what an audit is, why an audit is required, who is audited, and what the outcome of an audit is.

Key concepts

The main areas of focus in an IT audit include IT governance, which examines how the organization aligns its IT strategy with business objectives, and risk management, which evaluates safeguards against cybersecurity threats and ensures the effectiveness of disaster recovery plans. Compliance plays a significant role in ensuring adherence to related regulations. Technical infrastructure is reviewed for performance, while access controls are assessed to prevent unauthorized use of sensitive systems.

An audit for IT audits focuses on evaluating whether an organization's IT processes, systems, and controls align with international standards, for information security management or for IT service management. These audits are conducted to ensure compliance, enhance operational efficiency, and build stakeholder trust in the organization's ability to manage risks and protect sensitive information. Audits assess the organization's adherence to policies, procedures, and controls outlined in the relevant standards.

The audit process typically involves a detailed review of documentation, interviews with staff, and inspection of IT systems to verify compliance and identify areas for improvement. The ultimate goal is to demonstrate the organization's commitment to best practices in IT management, security, and compliance.

Auditing is a systematic process of examining, evaluating, and verifying an organization's financial records, operational processes, or IT systems to ensure accuracy, compliance, and effectiveness. It plays a critical role in governance, accountability, and risk management across industries and domains. The IT department is the core that connects your company's networks, systems, applications and data in one central spot to ensure they are functioning properly. It is through an IT system that a business, whether large or small, is able to remain competitive. Different areas of IT include sales, invoicing, accounting, taxes, marketing, HR, customer development and retention, and product development. It supports all the departments of every business. IT service management involves overseeing an organization's IT operations, resources, and infrastructure to ensure technology is effectively leveraged and aligned with the overall business strategy. Professionals in IT implement policies, practices, and procedures essential for managing the maintenance and utilization of hardware, software, and networks, regardless of the industry or business environment. IT management is a salient feature in every organization, and is evident in the following areas:

- **Proper IT management supports business operations**: IT lies at the core of almost all business activities.
- **Brings efficiency and productivity**: IT management ensures that a business's information technologies are secure, optimized, and performing efficiently.
- **Manages risks**: IT systems are to be subjected to business impact assessments and risk analysis, which will help in identifying controls to minimize the impact due to any outages and risks caused by the impact.
- **Improves data management**: IT management improves data management by implementing mechanisms for all users to collaborate, transfer data as required, and store and protect confidential and sensitive data.
- **Plays a strategic role in business growth**: IT management needs a shift in the placeholder from BAU maintenance/management activities to strategic/tactical activities by aligning with the organization's strategic goals, fostering innovation, managing risks, and allocating resources.

Components of IT management

Depending on the business needs and organizational structure, IT management can be broken down into several key components. Typical components are given as follows:

- **IT governance**: Aligning the IT investments and operations with the organization's strategies, followed by the required risk management practices. This leads to the establishment of a framework for decision-making, risk management, and accountability.
- **IT financial management**: Embedding strategic planning, budgeting, tracking, and managing the costs, benefits, and risks of IT investments, in a way to keep the performance metrics at an acceptable level. It includes costing, ROI analysis, accounting, and cost-tracking activities.
- **IT service management** (**ITSM**): Focuses on delivering IT support to end-users to meet the needs of the business. ITSM includes service support along with service delivery.
- **IT operations management**: Involves overseeing and managing daily activities, processes, and infrastructure needs of a typical organization, by being responsible for delivering value to the business through technology support.
- **IT project management**: Defines project scopes, budgets, timelines, and resources. It ensures all IT initiatives reach their designated goals in a timely manner and within budget.
- **IT security management**: Protects the organization's data assets and systems from threats and ensures compliance with relevant regulations and standards by implementing security measures and monitoring vulnerabilities to ensure business continuity.

The general responsibilities of the IT managers and the IT team are as follows:

- Managing IT procurement budget and configuration/monitoring costs.
- Determining IT systems/controls that are required for achieving company goals.
- Monitor compliance and integrity of the complete landscape.
- Control network security and ensure zero breach in the organization with proper **operating level agreements** (**OLAs**).
- Roll out and administer new software, hardware, and relevant data systems.
- Provide technical or service desk support to employees with proper **service level agreements** (**SLAs**).

It is clear that IT managers and professionals within the IT management field need to have subject matter expertise on all things technical, and also have a solid understanding of what goes into business operations. It is up to the IT team to ensure that business operations are using technology to support all aspects of the company strategy and its goals. At the end of the day, the IT leaders at your business will be the problem solvers as your business implements new technologies and systems within its network.

Auditing is an essential process in verifying that organizations comply with **International Organization for Standardization** (**ISO**) standards. ISO auditors must follow specific guidelines to ensure audits are thorough, objective, and aligned with the requirements of the relevant ISO standard.

Core standards for IT audits

IT audits play a critical role in ensuring the security, efficiency, and compliance of IT systems, which form the backbone of any organization. The IT audit and assurance process involves conducting specific procedures to provide reasonable assurance regarding the subject matter. Practitioners undertake assignments that deliver varying levels of assurance, ranging from reviews to attestations or examinations.

Each IT audit or assurance assignment must comply with established standards, ensuring that individuals are qualified to perform the work, the procedures are appropriately executed, the scope of work is clear, and findings are reported accurately based on the assignment's nature and results.

For engagements carried out by a single individual, they must have the necessary skills and knowledge to complete the assignment. In cases where a team is involved, the collective expertise and knowledge of the team must meet the requirements to effectively execute the work.

ISO/IEC 20000 and **Information Technology Infrastructure Library** (**ITIL**) are closely related frameworks that provide best practices and standards for **IT service management** (**ITSM**). Organizations use ITIL as a roadmap to implement ITSM processes and achieve operational excellence. Once processes are established, they can pursue ISO/IEC 20000 certification to demonstrate compliance and validate their ITSM practices.

ISO 20000 outlines the requirements for organizations to establish, implement, maintain, and continuously enhance a **service management system** (**SMS**). The standard covers the planning, design, transition, delivery, and improvement of services to meet organizational needs and deliver value effectively.

ITIL has been a cornerstone of the ITSM industry, offering guidance, training, and certification programs. It has transformed traditional ITSM practices by incorporating customer experience, value streams, and digital transformation. ITIL also embraces modern methodologies such as Lean, Agile, and DevOps. ITIL is currently at version 4 and equips organizations to tackle emerging service management challenges and leverage modern technology. It provides a flexible, coordinated, and integrated framework for the governance and management of IT-enabled services.

ITIL and ISO 20000 framework together help an organization to achieve the following:

- **Integrated service management framework**: Combines standardization with practical implementation.
- **Improved service delivery**: Consistent, reliable, and high-quality IT services.

ITIL is a set of best practices and guidelines for ITSM that originated in the United Kingdom. It provides a framework for aligning IT services with business needs and focuses on continuous improvement. ITIL covers various aspects of ITSM, including service strategy, design, transition, operation, and continual service improvement.

ISO 20000 is an international standard for IT service management. It outlines best practices and requirements for the effective management of IT services. ISO 20000 focuses on improving the quality of IT service delivery, enhancing customer satisfaction, and ensuring continuous service improvement. It is a formal and structured framework with specific requirements that organizations must adhere to in order to achieve certification.

To summarize, the comparison between ITIL and ISO 20000 is as follows:

Aspect	ITIL	ISO/IEC 20000
Nature	Best practice framework	International standard
Focus	Guidance for IT service management	Certification of organizations
Audience	Individuals (IT Professionals)	Organizations
Approach	Flexible and adaptable	Mandatory (auditable) requirements
Purpose	Service management best practices	Formal compliance and certification

***Table 1.1**: Comparison of ITIL framework and ISO 20000 standard*

ISO standard provides the approach to compliance through a layered approach in documenting the auditable requirements in alignment with the business objectives and the compliance requirements. At the first level, the policies are drafted, which highlight what all processes have to be addressed for obtaining compliance, then come the control objectives, which provide the best practices from the industry. This is followed by procedures, which capture the methods of carrying out the objectives that are captured in the policies. There will be guidelines that are provided for information on how the activities are to be carried out to address the policies.

The following figure explains the layered approach:

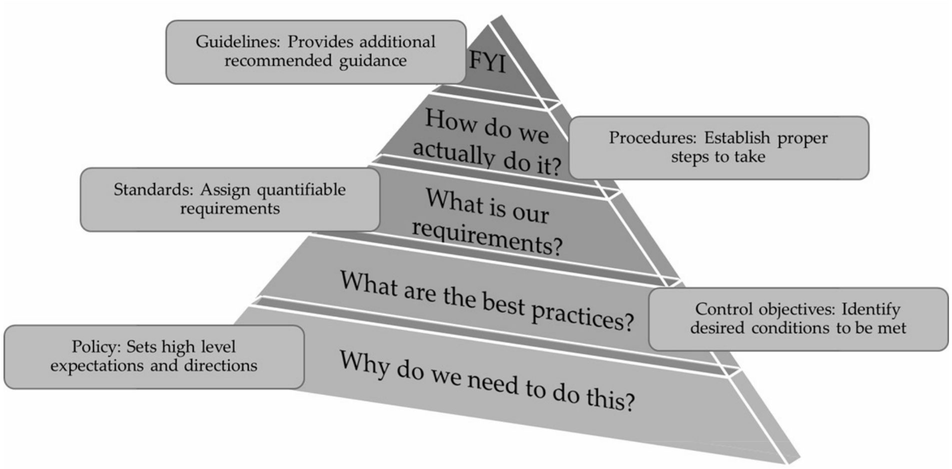

***Figure 1.1**: Layered approach as per ISO standard*

Some widely recognized core standards and frameworks used in IT audits are as follows:

- **ISACA's IT Assurance Framework (ITAF):** ITAF provides guidelines, standards, and tools for performing IT audits. Its key areas include audit planning, execution, and reporting.

  ISACA's **Information Technology Audit Framework** (**ITAF**) is a comprehensive IT audit framework that establishes standards that address IT audit and assurance practitioners' roles and responsibilities, ethics, expected professional behavior, and required knowledge and skills; provides guidance and techniques for planning, performing, and reporting of IT audit and assurance engagements. Based on ISACA's material, ITAF provides a single source for IT audit and assurance to practitioners to obtain guidance on the performance of audits and the development of effective audit reports.

- **COBIT Framework: Control Objectives for Information and Related Technologies** (**COBIT**) is a globally recognized framework developed by ISACA for managing and governing enterprise IT. It provides a comprehensive set of guidelines, principles, and best practices for aligning IT processes with business objectives, ensuring effective governance, risk management, and compliance. COBIT enables organizations to achieve strategic goals by optimizing the value derived from IT investments while managing risks and ensuring resource efficiency. It supports stakeholders in ensuring IT operations are secure, reliable, and aligned with organizational priorities. The framework is widely used across industries to enhance IT governance and improve decision-making.