MEST Journal
DOI 10.12709/mest.13.13.01.08

ENHANCING IT MATURITY THROUGH IT GENERAL CONTROLS (ITGC) AUDITS

Haris Hamidovic
MKF/MKD EKI Sarajevo, Sarajevo, Bosnia and Herzegovina
https://orcid.org/0000-0002-1296-5008

JEL Category: **K22, M15**

Abstract

IT General Controls (ITGC) audits are vital for organizations that rely on information technology, as they offer independent assurance regarding the effectiveness of internal controls, governance, and risk management. This process enables management to understand the strengths and weaknesses of their IT controls and receive practical recommendations for improvement. Using best practice frameworks from IIA and ISACA, ITGC audits align with industry standards, helping organizations meet legal and regulatory requirements while supporting secure and efficient IT operations. Competent auditors, equipped with formal education, experience, and certifications like CISA, CISM, CRISC, and CISSP play a critical role in these audits. They ensure that IT systems and processes comply with governance criteria, protect data integrity, confidentiality, and availability, and align IT operations with organizational objectives. Through ITGC audits, auditors can identify risks in areas such as change management, logical access, business continuity, and physical security, helping organizations enhance their IT maturity and resilience.

Keywords: IT General Controls, ITGC, GITC, IT audit, Risk Management, Information Security.

1 INTRODUCTION

The purpose of the audit function is to provide management and senior leadership with independent assurance concerning internal controls, governance, and the organization's risk management activities. While the board and stakeholders define the mission and strategy of the enterprise, management is responsible for executing them. Auditors play a crucial role in independently and objectively ensuring that management activities are aligned with corporate objectives.

Different types of audits include (ISACA, 2022):

- IT Audit: Assessment of IT systems and security controls.
- Financial Audit: Verification of financial data accuracy.
- Operational Audit: Evaluation of efficiency and effectiveness.
- Integrated Audit: A combination of financial, operational, and IT audits.

Each type of audit helps an organization maintain comprehensive control over business operations and ensure compliance with laws and standards.

Address of the corresponding author:
Haris Hamidović
haris.hamidovic@eki.ba

An IT audit is a formal examination and/or testing of information systems aimed at determining whether (ISACA, 2022):

- IT systems meet applicable laws, regulations, contracts, and/or industry guidelines.
- IT systems and processes comply with governance criteria and relevant policies and procedures.
- Data has appropriate levels of confidentiality, integrity, and availability.
- IT operations are conducted efficiently and aligned with objectives.

The IT audit also assesses whether the internal controls implemented by management provide reasonable assurance that business objectives will be met and that undesired events are either prevented or promptly detected and corrected.

Examples of audits that may fall under IT audit evaluations include (ISACA, 2022):

- IT General Controls (ITGC) audits
- Application audits
- IT process audits
- Cybersecurity audits
- IT governance audits
- IT infrastructure audits
- Physical security audits
- IT compliance audits
- Business continuity and disaster recovery audits

This paper provides an overview of the concept and components of IT General Controls (ITGC) auditing.

2 IT GENERAL CONTROLS (ITGC)

The Institute of Internal Auditors (IIA), a leading global authority in internal auditing, emphasizes in its Global Technology Audit Guide (GTAG) 1 that “internal auditor must understand the range of controls available for mitigating IT risks. Controls may be classified to clarify their purposes and where they fit within the overall system of internal controls. By understanding these classifications, control analysts and auditors are better equipped to position them within the control framework and address key questions, such as: Are detective controls adequate for identifying errors that might bypass preventive controls? Are corrective controls sufficient for addressing errors once detected?” Figure 1 presents one of the control classifications, as illustrated in the IIA's GTAG 1 document. (IIA, 2012)

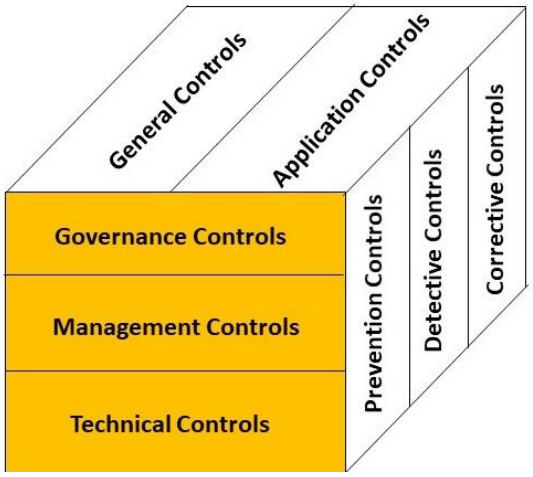

Figure 1. Control classifications according to IIA’s GTAG 1

Source: (IIA, 2012)

A common classification of IT controls is between general and application controls. (IIA, 2012)

ISACA defines IT General Controls (ITGC) in its IT Audit Fundamentals Study Guide as follows: “A general computer (IT) control is a control, other than an application control, that relates to the environment within which computer-based application systems are developed, maintained, and operated, and is therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, as well as the integrity of program and data files and/or computer operations. Like application controls, general controls may be either manual or programmed. General controls support the entire enterprise in a centralized manner as part of the IT infrastructure. Since the infrastructure is often shared among different departments within the same organization, the term "general controls" is also used to describe all controls in the infrastructure, including those that support operating systems, networks, or facilities. These controls typically include centralized user administration policies, standards and procedures, and technical elements such as access controls, firewalls, and intrusion detection systems.” (ISACA, 2022)

In the field of IT audit, "IT General Controls" (ITGC) and "General IT Controls" (GITC) are used interchangeably, but for this paper, we will use the abbreviation ITGC.

According to ISACA guidelines, common IT general controls (ITGC) include the following (ISACA, 2022):

- Logical access controls
- Change, patch, release, and configuration management controls
- Data backup, storage, and recovery controls
- Business continuity and disaster recovery controls
- IT operations controls
- Physical access and environmental controls
- System development life cycle (SDLC) controls

On the other hand, ISACA defines application controls as the policies, procedures, and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved. As such, application controls are controls over input, processing, and output functions. They include methods for ensuring that (ISACA, 2022):

- Only complete, accurate, and valid data are entered and updated in a computer system.
- Processing accomplishes the correct task.
- Processing results meet expectations.
- Data are maintained completely and accurately and are available for reporting.

3 BASIC PHASES OF ITGC AUDIT

IT audit consists of three basic phases (ISACA, 2022):

1. Planning: The scope and methodology of the audit are defined, including resource allocation and a timeline.
2. Fieldwork: Evidence is gathered and analyzed through control testing and system assessment.
3. Reporting: In this phase, the auditor presents findings and makes recommendations to key stakeholders.

The goal of each phase is to ensure that the audit process is comprehensive and focused on achieving relevant business objectives.

During the preparation of IT auditors for an ITGC audit, the recommendations provided in guidelines for IT auditors, published by professional auditing associations such as the IIA and ISACA, can be of great assistance. For example, the IIA, in its handbook Fundamentals of IT Audit for Operational Auditors, lists example documents or sources of information that may be collected by the internal auditor during an ITGC audit. For example, during the SLDC audit, the IT auditor should pay attention to the following records (IIA, 2022):

- The project framework contains scope, objectives, team composition, timeline, consideration of changes, etc., with evidence of review/approval from the project owner and project sponsor.
- The project schedule (and related documents) outlining key tasks, dependencies, effort, resource assignments, and dates.
- Evidence of initial budget approval and any changes to the budget since the initial approval.
- Evidence of current budget monitoring tools used to manage/track the budget, ensuring all resource expenses are up to date.
- The business case for the project.
- A benefits realization strategy that includes a detailed plan to achieve the project/business goals, with timelines and milestones.
- Approved business, technical, and functional documentation, etc.

These guidelines can be of great practical use to new and experienced IT auditors as a foundation for preparation.

The ISACA CISA Review Manual is also an excellent practical tool for preparing IT auditors to conduct ITGC audits. Based on practical experience, it contains sets of questions designed to help auditors prepare for conducting audits. (ISACA, 2024).

An IT auditor should provide a balanced report, describing not only negative issues in terms of findings, but also giving positive, constructive comments regarding improved processes, controls, or the efficiency of existing controls. (ISACA, 2022) Unfortunately, in practice, auditors often highlight what is wrong, making it difficult for business stakeholders reading the report to understand the positive aspects of the ITGC environment within the organization. Given this, it could be beneficial to use a maturity model based on the ISACA COBIT framework during ITGC audits (ISACA, 2019), which would highlight the current maturity level of various ITGC components and could serve as a basis for developing an

improvement plan towards the desired state. Figure 2 provides a simplified graphical representation from ISACA COBIT 4.1, showing the current maturity level, the industry average (if known), and the desired maturity level. (ISACA, 2007)

Fig. 2 Example of the current maturity level, the industry average, and the desired maturity level
Source: (ISACA, 2007)

4 EXPECTATIONS OF AN IT AUDITOR

An IT auditor is expected to maintain a high level of professionalism and expertise, adhering to a code of ethics, ensuring impartiality, and applying due professional care. According to the IT audit code of ethics, the auditor must act with integrity, safeguard data confidentiality, and continually develop their skills. The auditor must remain objective, avoid conflicts of interest, and protect the autonomy of the IT audit function to ensure the quality and credibility of the entire audit process.

IT audit is expected to provide objective assessments that assist management in making informed decisions. Management is responsible for:

- Ensuring adequate IT resources,
- Implementing security measures and regulatory compliance,
- Defining internal policies to regulate employee behavior.

IT auditor evaluates these aspects, tests their application, and identifies areas that need improvement.

According to the IT Audit Framework, IT audit and assurance practitioners should (ISACA, 2020):

- Demonstrate sufficient professional competencies—such as relevant skills, knowledge, and experience—before commencing the planned engagement.
- Evaluate alternative methods for acquiring the necessary skills to perform the engagement. This may involve subcontracting, outsourcing certain tasks, postponing the assignment until the skills are available, or otherwise ensuring the availability of appropriate expertise.
- Ensure that team members involved in the IT audit and assurance engagement possess either a CISA certification or another relevant professional designation, along with adequate formal education, training, and work experience.
- Provide reasonable assurance, when leading an IT audit or assurance engagement, that all team members have the requisite professional competency to carry out their assigned tasks.
- Possess sufficient knowledge of key areas necessary to effectively and efficiently conduct the IT audit or assurance engagement, in collaboration with other team members and any involved specialists.
- Meet the continuing professional education or development requirements associated with CISA or other relevant professional designations.
- Regularly update professional knowledge through educational courses, seminars, conferences, webcasts, and on-the-job training, ensuring a level of professional

service appropriate to the IT audit or assurance role.
- Consider utilizing external resources if the required competencies are unlikely to be available within the necessary timeframe.

For specialized audits, such as those focused on cybersecurity, additional respected certifications include ISACA's CISM and CRISC, as well as ISC2's CISSP. (IIA, 2015)

The Institute of Internal Auditors has developed a specialized program for internal auditors related to ITGC, which covers the following areas:

- Recognize the importance of the governance of enterprise IT.
- Associate project delivery with effective and efficient technology-driven processes.
- Realize the impact technology has on business processes.
- Identify and assess basic IT general controls related to:
- IT Change Management,
- Business Resilience,
- Logical Security,
- Physical Security,
- Environmental Controls,
- IT Operations and Services Management,
- System Development Life Cycle.

This program is designed to enhance the internal auditors' skills in assessing critical areas of ITGC, helping them support organizational governance and security.

5 CASE STUDY: ITGC AUDIT IN A PUBLIC HEALTHCARE INSTITUTION

A public healthcare institution struggled with outdated IT systems and insufficient data management controls, especially concerning patient data security. The lack of a centralized IT governance strategy increased the risk of data breaches and non-compliance with regulations like GDPR and national healthcare standards.

ITGC Audit Implementation:

The audit focused on addressing vulnerabilities in three critical areas:

1. *Access Controls*: Assessing who has access to sensitive data and how access is granted and monitored.
2. *Change Management*: Evaluating the procedures for updating and maintaining IT systems.
3. *Operational Resilience*: Ensuring reliable data backups and testing disaster recovery plans.

Findings:

- Unauthorized access was identified due to poorly defined access control policies.
- Software updates were managed informally, leading to unplanned system downtimes.
- Backup systems were unreliable and did not cover all critical data repositories.

Actions Taken:

- A centralized access control system was implemented, incorporating multi-factor authentication and regular audits.
- Standardized procedures for approving and testing IT system changes were introduced.
- Automated backup processes were established, with regular disaster recovery testing.

Outcomes:

- Compliance with regulatory requirements significantly improved, reducing the risk of data breaches.
- Operational resilience was enhanced, ensuring faster recovery from potential incidents.
- Trust from patients and regulatory authorities in the institution's data management practices increased.

This example demonstrates how ITGC audits can help public institutions strengthen IT governance, improve data protection, and achieve regulatory compliance.

In the article "Six ITGC audit controls to improve business continuity" on TechTarget, the author provides a sample checklist that can serve as a starting point for planning, scheduling, and conducting an ITGC audit. These six critical ITGC controls include essential areas such as access management, change management, and disaster recovery, among others. These controls form a comprehensive framework that helps organizations ensure effective IT governance, mitigate risks, and improve business continuity strategies. The checklist offers actionable steps for conducting a thorough ITGC audit and is a

practical guide for auditors and IT managers. (TechTarget, n.d.).

6 CONCLUSIONS

The audit of IT General Controls (ITGC) is crucial for all business organizations that rely on information technology, as it ensures the reliability, security, and integrity of their IT systems. By following established best practice frameworks developed by the Institute of Internal Auditors (IIA) and ISACA, organizations can standardize their ITGC audits, enhancing both their effectiveness and alignment with industry standards. Competent auditors, with formal education, practical experience, and recognized IT audit and security certifications, are essential for conducting these audits effectively. This expertise enables auditors to provide management with objective assurance on the current state of ITGC controls. Additionally, auditors can offer practical recommendations to improve the maturity level of these controls, helping organizations mitigate risks and strengthen their IT infrastructure in line with evolving industry demands.

WORKS CITED

IIA. (2012). Global Technology Audit Guide (GTAG) 1 Information Technology Risk and Controls, 2nd Edition

IIA. (2015). Lifelong learning for internal auditors

IIA. (2022). Fundamentals of IT Audit for Operational Auditors

ISACA. (2007). COBIT 4.1: Framework for IT Governance and Control

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives

ISACA. (2020). IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit, 4th Edition

ISACA. (2022). IT Audit Fundamentals Study Guide

ISACA. (2024). CISA Review Manual

TechTarget. (n.d.). Six ITGC audit controls to improve business continuity. Retrieved December 10, 2024, from https://www.techtarget.com/searchdisasterrecovery/tip/Six-ITGC-audit-controls-to-improve-business-continuity

Received for publication: 05.08.2024
Revision received: 17.08.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Hamidovic, H. (2025, 01 15). Enhancing IT Maturity through IT General Controls (ITGC) Audits. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 82-88. doi:10.12709/mest.13.13.01.08

Style – **Chicago** *Sixteenth Edition:*

Hamidovic, Haris. "Enhancing IT Maturity through IT General Controls (ITGC) Audits." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 82-88.

Style – **GOST** *Name Sort:*

Hamidovic Haris Enhancing IT Maturity through IT General Controls (ITGC) Audits [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 82-88.

Style – **Harvard** *Anglia:*

Hamidovic, H., 2025. Enhancing IT Maturity through IT General Controls (ITGC) Audits. *MEST Journal,* 15 01, 13(1), pp. 82-88.

Style – **ISO 690** *Numerical Reference:*

Enhancing IT Maturity through IT General Controls (ITGC) Audits. **Hamidovic, Haris.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 82-88.