Are IT General Controls Outdated?

Data Protection and Internal Control Over Financial Reporting

Ook verkrijgbaar in het Nederlands
www.isaca.org/currentissue

For an IT auditor working in the accountancy business, the importance of IT general controls, especially in the domain of access management for financial statements, is clear. For more than a decade IT general controls have barely changed, while frameworks such as the Trust Services Criteria from the American Institute of Certified Public Accountants (AICPA) and the Cloud Controls Matrix from the Cloud Security Alliance (CSA) have evolved. The information security framework of the International Organization for Standardization (ISO) standard ISO 27002 is also undergoing a major upgrade, including new controls. Is it possible that the financial reporting risk factors within the data life cycle have hardly changed? Data are kept within a system such as a database, and functionality ensures that data can be accessed and processed. However, IT environments have changed significantly with the outsourcing of information systems and the use of (virtual) hardware. To determine whether IT general controls need to be updated or whether they are still sufficient to cover most IT environments, it is useful to examine the controls as they apply to data security (mostly integrity and confidentiality). Then, a selection of IT general controls can be compared with frequently used and generally accepted frameworks within service organization assurance reports and their data protection controls.

IT General Controls

The auditor identifies controls using a basic set of (suggested) IT general controls such as those defined in the guidelines published by the International Auditing and Assurance Standards Board (IAASB) in International Standards on Auditing (ISA) 315 (revised 2019).[1] The controls identified can differ based on their application and on other aspects of the IT environment. The IT general controls concerning data security are defined in appendix 6 of ISA 315.[2]

Within the area of access management, controls that can impact data protection include:

- **Authentication controls**—Ensures that a user accessing the IT application or other aspect of the IT environment is not using another user's log-in credentials.
- **Authorization controls**—Allows users to access the information necessary for their job responsibilities and nothing further, which facilitates appropriate segregation of duties.
- **Provisioning controls**—Authorizes new users and modifications to existing users' access privileges.
- **Deprovisioning controls**—Removes user access upon termination or transfer.
- **Privileged access controls**—Authorizes administrative or powerful users' access.
- **User access reviews controls**—Recertifies or evaluates user access for ongoing authorization over time.

JOUKE ALBEDA | CISA, CISSP, RE

Is an experienced IT auditor and director at 3angles. He supports enterprises with audit, risk and compliance. Previously, he worked as a risk and compliance manager at Datacenter.com and worked for Binder Dijker Otte (BDO) and Ernst & Young (EY) within the external IT audit practice. His articles have been published in *Audit Magazine, de IT-Auditor* and the *ISACA® Journal*.

- **Security configuration controls**—Each technology generally has key configuration settings that help restrict access to the environment.
- **Physical access controls**—Authorizes physical access to the data center and hardware, as such access may be used to override other controls.[3]

Within the area of change management, the controls that can impact data protection include:

- **Data conversion controls**—Authorizes the conversion of data during development, implementation or upgrades to the IT environment.[4]

Within the area of IT operations management, the controls that can impact data protection include:

- **Intrusion detection controls**—Monitors for vulnerabilities and/or intrusions in the IT environment.[5]

ISA 315 mentions these controls as possible IT general controls an auditor might consider. The auditor must perform a risk assessment and use professional judgment to determine the risk factors in the IT environment and the appropriate controls to mitigate them. The list of IT general controls defined in ISA 315 is similar to the IT general control guidelines defined by other organizations.[6] The ISA standard is, therefore, an appropriate reflection of IT general controls used by IT auditors.

In addition to IT general controls, which are needed to rely on information systems for financial reporting, most service organizations provide assurance reports to their clients to demonstrate their compliance with control frameworks.

Control Frameworks Used for Outsourcing

In addition to IT general controls, which are needed to rely on information systems for financial reporting, most service organizations provide assurance reports to their clients to demonstrate their compliance with control frameworks. Control frameworks, such as those developed by the AICPA and CSA, contain more controls than the familiar IT general controls. When controls from other frameworks are deemed ineffective, or if an assurance report has a qualified opinion, an impact assessment is performed to determine whether the deficiencies can negatively impact financial reporting. As service organization control (SOC) reports often cover more than just IT general controls, accountants and IT auditors must determine the impact of additional controls that generally would not be assessed when testing only IT general controls.

To identify the controls related to data protection that are excluded from IT general controls, a gap analysis was performed for both the Trust Services Criteria and the Cloud Controls Matrix. For the Trust Services Criteria, additional data protection controls were identified:

- The entity selects, develops and performs ongoing or separate evaluations to ascertain whether the components of internal control are present and functioning.
- The entity implements logical access security software, infrastructure and architecture for information assets to protect them from security events.
- The entity restricts the transmission, movement and removal of information to authorized internal and external users and processes, and protects it during transmission, movement or removal.
- The entity implements controls to prevent or detect and act on the introduction of unauthorized or malicious software.
- The entity uses detection and monitoring procedures to identify changes to configurations that result in the introduction of new vulnerabilities and susceptibilities to newly discovered vulnerabilities.
- The entity monitors system components and the operation of those components for anomalies indicative of malicious acts, natural disasters and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
- The entity disposes of confidential information to meet the entity's objectives related to confidentiality.[7]

For the Cloud Controls Matrix, additional data protection controls were identified (because the matrix has specific and granular controls, some of them are grouped), including:

- Automated application security testing
- Application vulnerability remediation
- Cryptography, encryption and key management
- Secure disposal/data retention and deletion
- Sensitive data transfer
- Safeguard logs integrity
- Security monitoring and alerting
- Audit logs access and accountability
- Logging and monitoring (including failures and anomalies)
- Penetration testing
- Universal endpoint management (e.g., storage encryption, firewall)
- Data loss prevention[8]

A popular information security framework that is not often used to provide assurance for financial reporting is ISO/IEC 27001/27002. ISO 27002 has been updated and will be transferred to a new ISO 27001 framework.[9] Some controls have been introduced to meet the current requirements for information security within the IT environment, including:

- Threat intelligence
- Physical security monitoring
- Configuration management (including security configurations)
- Information deletion
- Data masking
- Data leakage prevention
- Monitoring activities
- Web filtering[10]

These controls were also identified in the gap analyses of the Cloud Controls Matrix and the Trust Services Criteria. This emphasizes the need for additional controls to secure data and manage data security risk.

New IT General Controls to Consider

Examining the controls that exist in the Trust Services Criteria and Cloud Controls Matrix and are not reflected within the IT general controls shows there are additional IT general controls for the auditor to consider (**figure 1**).

Both the traditional IT general controls and the new suggested controls should be considered for testing the application, database, operating system and network components in the IT environment.

Both the traditional IT general controls and the new suggested controls should be considered for testing the application, database, operating system and network components in the IT environment.

When auditing IT general controls to ensure the reliability of information systems in financial reporting, data integrity is important, but it is debatable whether confidentiality is equally important. If strong authentication controls are in place and direct access to the data is strictly limited to appropriate individuals, are the new controls necessary? In this case, it would seem that the risk of an unauthorized individual gaining access to and altering data is low. To understand the relevance of these controls, a close look at the risk of fraud and lack of data integrity is needed.

Relevance of Additional IT General Controls

When performing an IT audit on information systems, the key risk factors are data insecurity and fraud. In 2016, the US National Institute of Standards and Technology (NIST) described three cyberattack scenarios that can lead to data integrity issues: ransomware, data destruction and data manipulation (insider threat).[11] Another recent study described multiple attacks in the cloud that can lead to data integrity concerns.[12] In information systems connected to the Internet or the cloud, the attack surface is much bigger; therefore, data security is a significant issue.

The increased use of cloud platforms and the increased number of risk factors associated with them are reflected in the amount of fraud being perpetrated. In one recent survey, "nearly 70 [percent]

LOOKING FOR MORE?

- Read *IT Audit Framework, 4th Edition. www.isaca.org/itaf*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 1

Mapping Gap Analysis Findings to New IT General Controls

Trust Services Criteria	Cloud Controls Matrix	Suggested New IT General Controls
The entity selects, develops and performs ongoing or separate evaluations to ascertain whether the components of internal control are present and functioning.	Automated application security testing Penetration testing	**Security assessments**—Controls that test appropriate functioning of system-hardening controls
The entity implements logical access security software, infrastructure and architecture for information assets to protect them from security events.	Cryptography, encryption and key management	**Data asset protection**—Controls that prevent data within the data management life cycle from being altered or compromised (e.g., using encryption technology)
The entity restricts the transmission, movement and removal of information to authorized internal and external users and processes, and protects it during transmission, movement or removal.	Sensitive data transfer Data loss prevention (DLP) Cryptography, encryption and key management	**Secure data in transit**—Controls that ensure data in transit are secure from alteration and compromise
The entity implements controls to prevent or detect and act on the introduction of unauthorized or malicious software.	Universal endpoint management (e.g., storage encryption, firewall)	**Endpoint protection**—Controls that prevent unauthorized or malicious software from accessing the network
The entity uses detection and monitoring procedures to identify changes to configurations that result in the introduction of new vulnerabilities and susceptibilities to newly discovered vulnerabilities.	Vulnerability identification Application vulnerability remediation	**Vulnerability monitoring**—Controls that monitor the IT environment for new vulnerabilities (should be separate from intrusion detection)
The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Safeguard logs integrity Security monitoring and alerting Audit logs access and accountability Logging and monitoring (including failures and anomalies)	**Security monitoring**—Controls that monitor system logs for anomalies
The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Secure disposal/data retention and deletion	**Secure disposal**—Controls that ensure that discontinued information assets are disposed of securely

of organizations experiencing fraud reported that the most disruptive incident came via an external attack or collusion between external and internal sources."[13] The same survey suggests that cyberfraud is more common than asset misappropriation.

Conclusion

Are IT general controls outdated? Although professional auditors can always define their own controls based on the risk assessment being performed, the IT general control guidance is outdated. As IT environments keep changing, the requirements for data protection need to evolve as well. To address this, frameworks such as the Trust Services Criteria, Cloud Controls Matrix and ISO/IEC 27002 have been developed over time.

When testing IT general controls, additional controls related to security assessments, data asset protection, secure data transit, endpoint protection, vulnerability monitoring, security monitoring and secure disposal should be considered for the relevant application, database, operating system and network components in the IT environment.

Endnotes

1 International Auditing and Assurance Standards Board (IAASB), *International Standards on Auditing (ISA) 315 (Revised 2019): Identifying and Assessing the Risks of Material Misstatement*, USA, 19 December 2019, *https://www.iaasb.org/publications/isa-315-revised-2019-identifying-and-assessing-risks-material-misstatement*

2 *Ibid*.
3 *Ibid*.
4 *Ibid*.
5 *Ibid*.
6 Deloitte, *General IT Controls (GITC) Risk and Impact*, India, November 2018, *https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-general-it-controls-noexp.pdf*
7 American Institute of Certified Public Accountants (AICPA), *TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, USA, March 2020, *https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf*
8 Cloud Security Alliance (CSA), "STAR Level and Scheme Requirements," USA, 4 September 2019, *https://cloudsecurityalliance.org/artifacts/star-level-and-scheme-requirements/*
9 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection—Information security controls*, Switzerland, February 2022, *https://www.iso.org/standard/75652.html*
10 *Ibid*.
11 Tobin, D.; M. J. Stone; A. Townsend; H. Perper; S. Weeks; *Data Integrity: Recovering From a Destructive Malware Attack,* National Institute of Standards and Technology (NIST) and National Cybersecurity Center of Excellence (NCCOE), USA, May 2016, *https://www.nccoe.nist.gov/sites/default/files/legacy-files/data-integrity-project-description-final.pdf*
12 Kaja, D.; A. B. Mailewa; Y. Fatima; "Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques," *International Journal of Research Publication and Reviews*, vol. 3, iss. 2, 2022, *https://ijrpr.com/uploads/V3ISSUE2/ijrpr2704-data-integrity-attacks-in-cloud-computing.pdf*
13 Pricewaterhouse Coopers (PwC), *PwC's Global Economic Crime and Fraud Survey 2022: Protecting the Perimeter: The Rise of External Fraud*, United Kingdom, 2022, *https://www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf*