

General IT Controls (GITC)

Risk and Impact

November 2018

Table of Contents

Introduction	02
IT scoping for evaluation of internal controls	04
Importance of GITC	06
Implications of GITC deficiencies	07
Stepping towards a controlled IT environment	08
Conclusive remarks	13
Impact of GITC failure on the overall ICFR framework	15
Contact	16

Introduction

The importance of information technology (IT) controls has recently caught the attention of organisations using advanced IT products and services.

This thought paper has been developed for the management of companies that are required to establish framework on internal controls and to ensure its effective operation throughout the year. This document draws attention on how applications should be scoped-in for monitoring internal controls and how control gaps need to be assessed and concluded.

Increasing complexity of the IT setup has resulted in a greater focus around controls in the IT environment.

With mandates emanating from various regulations, internal controls have gained more momentum in India during recent years. There is a trend of automation in processes and controls by adoption of advanced IT products and services for enabling greater efficiency in operations, compliance and reporting activities. This requires an increased focus on effective operation of controls around IT assets and services.


Internal Financial Controls over Financial Reporting


“Internal controls” refers to those activities within a company that are placed by the management to mitigate the risks that could hinder the company from achieving its objectives. Under the Committee on Sponsoring Organizations (COSO) framework revised in May 2013, there are three types of objectives which internal controls need to meet, as depicted below:








In many cases, a control may address more than one of these objectives. Under the COSO framework, there are five interrelated “components” of an effective internal control system; these are derived from the way the company is managed on a day-to-day basis:

- 

The company’s control environment at the top-management level with respect to controls. This includes elements such as “tone at the top,” and the effectiveness of the board’s audit committee in its high-level oversight of financial reporting. This component is known as the Control Environment.
- 

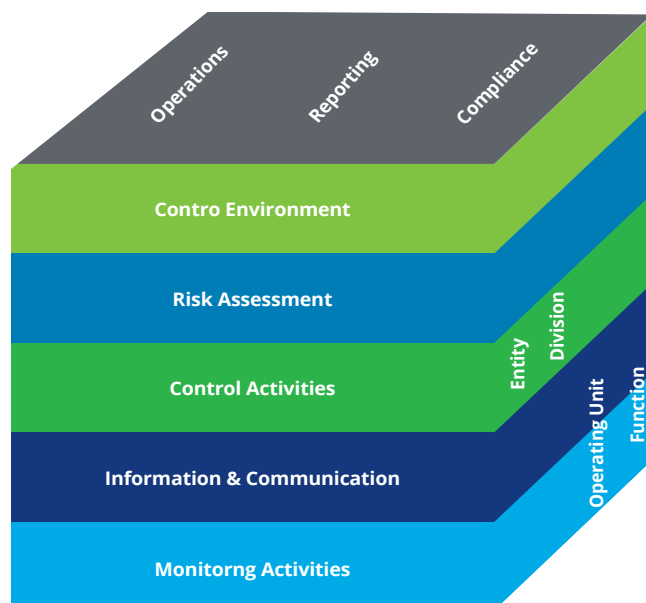
Risk assessment of various processes and factors that might hinder the company from achieving its objectives. For example, a process that is highly susceptible to fraud would be considered a high-risk area.
- 

The way in which controls are designed and implemented within the company, so as to address identified risks. This component is known as Control Activities.
- 

The way in which information within the company is gathered and shared, both to people within the company responsible for operations and financial reporting, and to external users of financial reports. This component is known as Information and Communication.
- 

The way in which the effectiveness of these controls are monitored by the company management who take corrective actions wherever necessary.

COSO Cube (2013)



Purpose of Internal Control

Internal control is designed, implemented, and monitored to address identified business risks that threaten the achievement of any of the entity’s objectives that concern

- The reliability of the entity’s financial reporting;
- The effectiveness and efficiency of its operations; and
- Its compliance with applicable laws and regulations.

IT scoping for evaluation of internal controls

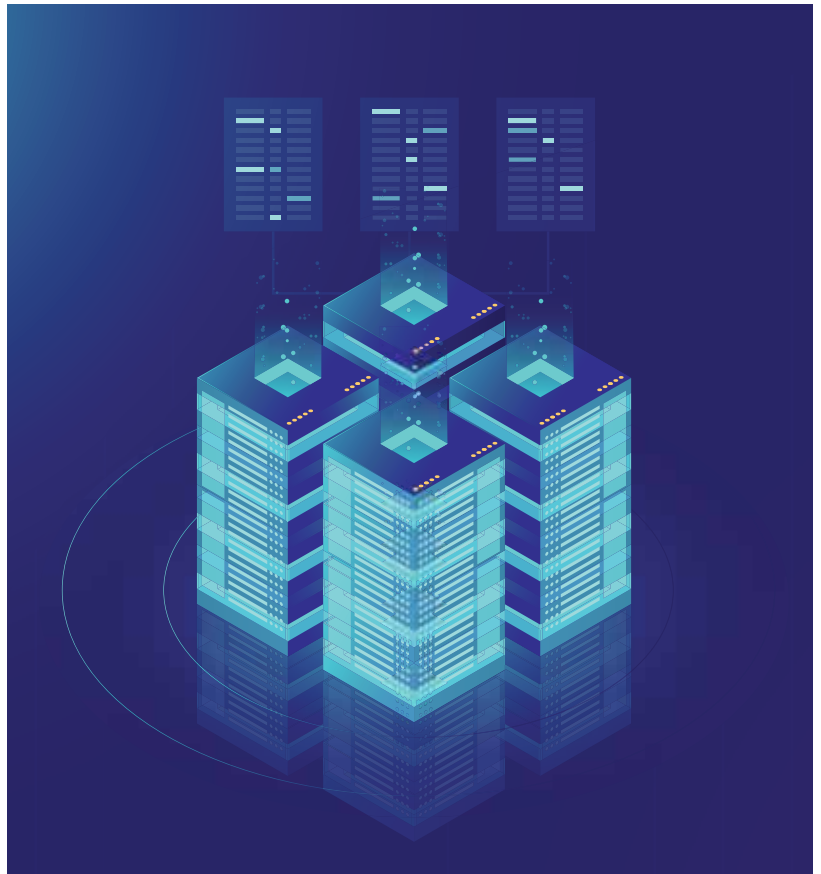
Multiple application systems, data warehouses, report writers, and layers of supporting IT infrastructure (database, operating system, and network) may be involved in the business process, right from initiation of a transaction to its recording in the general ledger. Such transactions ultimately lead to reporting in the financial statements, and therefore, any or all of these systems and IT infrastructure may be relevant to the audit.

Scoping considerations for IT applications relevant to audit

The management needs to maintain documentation for understanding the system landscape mapped to key business processes that are relevant to financial reporting, including:

- The classes of transactions in the company's operations that are significant to the financial statements;
- The procedures, within both automated and manual systems, by which those transactions are initiated, authorised, processed, recorded, and reported;
- Significant account balances that are material with respect to financial reporting;
- Ways in which the information system captures transaction, events and conditions that are significant to the financial statements; and
- The period-end financial reporting process.

The determination as to which application system, data warehouses, or report writers are relevant to the audit requires general IT controls to address their integrity and reliability.





Data

The management relies on an application system or data warehouse to process or maintain data (e.g. transactions or other relevant data) related to significant accounts or disclosures or reports used in the operation of relevant control.



Automated Controls

The management relies upon the application system to perform certain automated functions that are relevant to the audit.



System-Generated Reports

The management relies on an application, data warehouse query, or report writer to generate a report that is used in the operation of relevant controls.

For Example

Assume that an entity's SAP application runs on a UNIX server (operating system) and uses an Oracle database. User authentication is dependent upon Windows Active Directory (operating system) and the entity is using Cisco network management software. In this example, the UNIX and Windows Active Directory operating systems, Oracle database, and Cisco network management software are the technology elements supporting the SAP application system, and all of these technology elements are relevant to the audit.









Importance of GITC

Sustaining reliable financial information is dependent upon effective internal control and General IT Controls (GITCs) are a key part of entities' internal control framework.

GITCs are a critical component of business operations and financial information controls. They provide the foundation for reliance on data, reports, automated controls, and other system functionality underlying business processes. The security, integrity, and reliability of financial information relies on proper access controls, change management, and operational controls.

The importance and relevance of General IT Controls to key stakeholders—owners, investors, regulators, audit committees, management, and auditors— continues to increase.

					
Effective controls in operations, compliance with laws and regulations, and financial reporting are fundamental to well-managed entities. Entities recognise the importance of internal control to the reliability of the business processes that they use to run the entity.	The processes, controls, and financial data relevant to financial information are often also relied upon by the management to manage the business and key decision-making.	While financial information is not new, the complexity of financial reporting, business models, and the technology used to support them continues to evolve.	Regulators expect enhanced reliability of financial information, and stakeholders are looking for more specific information and transparency. Entities and auditors need to address these concerns to meet evolving owner, investor, and regulator expectations.	Cyber security is a broad business risk, which extends to financial information.	Automation is becoming increasingly important given the reliance on automated controls such as calculations, access controls, segregation of duties and input, processing, and output controls. These automated controls rely on GITCs to ensure they function properly.

Implications of GITC deficiencies

Deficiencies in GITCs may hinder the management's ability to prepare accurate financial information. If these deficiencies are not identified and addressed in a timely manner, they may impact the overall functioning of internal controls, thereby resulting in delayed financial closing process, impact on internal decisions and/or public disclosure. This could ultimately affect the reputation and brand of the company.

Deficiencies in GITCs may increase audit effort and cost due to additional audit procedures needed to respond to unaddressed IT risks.

Certain GITC deficiencies present "a greater risk" of resulting in a misstatement that could be pervasive in nature and could have far-reaching implications. The proximity of the GITC deficiency to financial reporting (e.g., a deficiency at the application layer versus the operating system layer), and the level

of technical skill necessary to exploit the deficiency, among other factors, could affect the severity of a deficiency.

As such, when considering the nature and cause of the deficiency, it is important to consider whether the GITC deficiency presents a "lesser risk" of misstatement or a "greater risk" of misstatement. These considerations are relevant to determine the nature, timing, and extent of additional audit procedures.



Stepping towards a controlled IT environment

The security, integrity, and reliability of financial information relies on proper access controls, change management, and operational controls. IT systems are becoming more integrated with business processes and controls over financial information. This is compelling organisations to increase their focus on IT controls in order to maintain the reliability of business processes within the organisation.

The information within IT systems is crucial for meeting many requirements in an organisation, including:

- Financial information relied upon by decision makers that is maintained within the IT systems;
- The continuously changing and increasing complexity of financial reporting;
- The ability of an organisation to meet the demands of regulators and investors
- The ability of an organisation to meet the demands of regulators and investors

Following topics are elaborated in detail below



User Access Management



Change Management



Outsourced Service Provider



User Access Management

User access provisioning

Granting any new user access is the initial step for maintaining a controlled environment on the IT application. An inappropriate user access could result in posting of unauthorised financial transactions.

Excessive access

Access to business application needs to be granted based on roles and responsibilities of users. Provision of access that is not in line with the user's job responsibilities could lead to posting of unauthorised financial transactions.

For Example

If an employee has access to approve purchase order, create goods receipt as well as vendor invoice processing, there is a possibility of unauthorised vendor payment processing which may be in excess to what is to be paid.

Generic User ID and Privilege access

Generic User IDs could lead to accountability issues for transactions processed using such IDs. Further, if privileged (administrator) access is granted to Generic User IDs then such access can be misused for posting transactions that could have a pervasive impact on the financial statements.

For Example

Generic User ID is used for background job processing and granted with privilege access. A user who accesses this Generic ID may make inappropriate changes to the background job which can post unauthorised financial entries.

User access de-provisioning

While access provisioning needs to be controlled, it is equally important to control the access revocation process. When employees are separated from the organisation, their User IDs can be misused for processing of financial transactions. Such transactions would not only be unauthorised, but also lack accountability.

Furthermore, if an employee gets transferred to another division/ department and the old access provisioned to him doesn't become obsolete, it leaves a chance to be used later on. Such access also needs to be de-provisioned on the transfer of employee.

In both contexts, it is important to revoke the access on time.

User access review

While streamlining, user access provisioning is key to controlling the access management of an IT application; periodic user access review keeps the access aligned with respect to business requirements. In the absence of periodic user access review, excessive access may remain with the user. User access review also detects if there are any anomalies in access provisioned, de-provisioned or any other privilege/ excessive access.



Change management

Direct change access

Access to make direct changes in a stable IT application's production environment may lead to serious data integrity issues. Direct changes are usually not tested previously, so it could lead to an adverse impact which would be difficult to roll-back.

Direct change may override already existing automated application control for a particular financial transactions or certain set of transactions. In the absence of audit logs, such direct changes will remain undetected.

Inappropriate access to modify data can affect the ability to rely upon the data within the IT systems. Further, review-type-control over direct changes would enable one to detect any inappropriate change to the IT application. However, a number of transactions would have already been processed by the time an inappropriate change is identified.

For Example

A direct change made to the calculation algorithm of depreciation posting program may lead to inappropriate depreciation posting for the company's asset. Further, if this direct change is performed near to the period/year end, it may lead to incorrect representation of asset values.

Change evaluation

A change can be initiated either due to a new requirement or when an enhancement is required in an already implemented functionality of IT applications. In any of these cases, change is to be developed, tested and then implemented in the Production environment.

An emergency change is implemented to perform an immediate fix and usually does not involve rigorous testing prior to implementation in production. If a change is implemented without testing, its impact cannot be determined.

For Example

If a change is implemented in Production for inclusion of one of the pricing element in sales order, then without testing, it cannot be ascertained that this pricing element will make any impact on other modes of sales order, such as domestic sale or import sale.

Change Authorisation

If an unauthorised change is implemented in the production environment then it may cause severe data integrity issues, including but not limited to the following:

- An unauthorised change may be incomplete, leading to instability of the underlying transactions processed.
- An unauthorised change may have bundled together with other changes as comparison to the original change request, leading to processing of incorrect business data.
- An unauthorised change might not be intended for implementation, and may lead to frauds in the worst case scenario.

Change authorisation timing is an important aspect from controlling perspective. Usually, a change is authorised at 2 levels—once prior to development and finally just before migration/implementation of change in production environment.

Change authorisation prior to its development will ensure that the intended change is aligned to business requirements. Change authorisation before migration/implementation in production will ensure that the developed change is tested by end user and found aligned to what is requested.

Direct changes in production

Direct changes in IT application's production environment would override the established change management process. This could result in inappropriate and untested application changes that can potentially affect the system's stability and sanity of financial data.

A direct change made to the production environment cannot be assessed for its impact if the corresponding quality/testing environment of the applications is not available. Further, if the quality/testing environment is available, but not synchronised with the production environment, the direct change testing performed on quality environment might not serve the testing purpose.

For Example

A company code is directly created in Production environment and later on pricing elements are to be configured in the sales order applicable to that company code. In such cases, pricing element related change cannot be tested in quality environment as the relevant company code is not available in quality/test environment.

Segregation of duties in change management

Segregation of duties plays an important role in the entire change management process. If a developer has also provisioned the change migration/implementation access in production environment, then it may lead to both unauthorised and/or inappropriate change implementation in the production environment.

For Example

A developer develops the change, tests and migrates it to the production environment by himself leading to the possibility of incorrect change implementation in production even though the production environment is separate from the development and quality/ test environment. As a developer, the user may not be aware of business requirements that need to be evaluated for changes to be appropriate.





Outsourced Service Provider for Infrastructure services

Today's global economy means virtually all entities use external service providers. Service providers must be able to demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

Many service organisations perform controls for multiple customers and provide an independent service auditor report that includes results from tests of controls.

The intent of 'Service Auditor Report' (SAR) is to provide guidance and uniformity in the way service providers disclose their control activities and processes to their customers and the entity's auditors.

An entity needs to evaluate the service audit reports on following aspects, but not limited to:

Not evaluating exceptions related to relevant controls in the SAR

An organisation needs to evaluate the SAR report from the perspective of exceptions/ deficiencies identified by service auditors. For example, if the physical access controls to outsourced data centre are mentioned as deficient in SAR, there is possibility of inappropriate access to entity financial data.

Not properly evaluating the appropriateness of the SAR

An organisation needs to assess whether the period of coverage of the report is adequate to cover the underlying risk. If the service auditor report is issued only for 6 months, it means the underlying IT Control might be ineffective for the remaining period of the financial year.

Conclusive remarks

GITC deficiencies may seem to be isolated gaps when assessed individually based on the mitigating controls and procedures. However, it is essential to assess gaps in a domain collectively as logically similar gaps can increase the overall vulnerability. An evaluation with this approach can help the management and auditors to identify failures across multiple levels that could ultimately result in frauds or financial misstatements.



In order to illustrate this approach, we could consider following gaps that are commonly identified in IT controls:

Logical access

Deficiency identified	Deficiency type	Unaddressed risk and risk in aggregation
<p>Appropriate approvals were not available for 8 out of 25 samples tested.</p> <p>Mitigating procedure: Noted based on further testing that these cases belonged to super users, generic IDs and functional support users</p>	Operating Effectiveness	<ul style="list-style-type: none"> • Testing of user creation/modification has been carried out on sample basis. Since the root case is regarding users with privileged access, generic IDs and support users, the total population of such users is 45 in the application. Therefore, this may not remain merely as an OE gap if all such instances are considered. • For cases where email addresses of separated employees were active or deactivated with a delay, it may be feasible to assess all the document changes such as master creation/updates and creation/updates to purchase order and invoicing, sales order. • The detective control regarding log monitoring of privileged accounts has also failed and therefore activities of inappropriate users with privileged access can go undetected. • The detected control regarding review of users and the appropriateness of access is also not comprehensive and hence no comfort can be obtained on the sanity of information recorded by all the users in the application. <p>All the gaps pertain to appropriateness of user access in the application and are logically related. When these gaps are assessed together, one can notice that both preventive as well as detective controls have failed due to which the risk remains unaddressed.</p>
<p>20 user IDs were active and 45 user IDs were deactivated with a delay after employee's separation</p> <p>Mitigating procedure: No financial entries were posted using these IDs.</p>	Operating Effectiveness	
<p>Log monitoring of privileged accounts are not performed for critical system administrative activities.</p> <p>Mitigating procedure: Noted appropriate users to have privileged access. No financial entries were posted using these IDs.</p>	Design & Implementation	
<p>Appropriate review process was not followed for periodic user access review. The review only considered roles mapped against respective users rather than evaluating the appropriateness of specific activities/ transactions that users have access to. Further, not all HODs provided confirmation regarding the appropriateness of users and their authorisations – no response was considered to be users having appropriate access.</p> <p>Mitigating Controls: Preventive controls regarding user access provisioning and de-provisioning were noted to be operating effectively with only OE gaps. The risk for these gaps were mitigated based on additional procedures.</p>	Design & Implementation	

Change Management

Deficiency identified	Deficiency type	Unaddressed risk and risk in aggregation
<p>Production client through SCC4 was opened for direct changes during the audit period and appropriate approval was obtained for the last change. However, since audit logs have been disabled, testing of operating effectiveness could not be tested.</p>	Operating Effectiveness	<p>A combination of these 3 gaps could allow users with developer key and access to modify programs/tables to make direct changes to programs in production environment by circumventing the structured change management process if the client is open.</p> <p>Combination of these gaps could result in a fraud risk where users can temporarily alter system behaviour and reverse the settings once fraudulent transactions are posted.</p>
<p>2 users have developer key in production environment which would allow these users to carry out direct changes when the client is open for changes.</p>	Design & Implementation	
<p>5 users have inappropriate access to modify programs and data dictionary in production environment.</p>		

Impact of GITC failure on the overall ICFR framework

We saw that combination of gaps can result in non-reliance on GITC in an IT setup comprising applications, databases and operating systems. This conclusion ultimately affects the reliance that is planned for automated controls, management reports, interfaces and the overall data integrity.

01

Automated applications controls and management reports

Reliance on automated controls and management reports depend on the appropriate changes made to system logics during the year. A structured process for system changes established by the management governs the system logic or behaviour. Combination of gaps in change management which leaves an open risk for inappropriate system changes would directly impact the comfort that can be taken on automated controls and management reports.

When change management domain cannot be relied upon, the management and the auditor would have to look for manual mitigating controls that could replace automated controls.

Even if logic of the report is validated and noted to be appropriate as on the date of assessment, since inappropriate change could have been done anytime during the year and restored to original setting, the management report cannot be relied upon. In such a case, direct test of management reports would have to be performed where accuracy and completeness of information in the report is validated for every instance in which this management report is used.

02

Interfaces

Automated interfaces ensure accurate and complete transfer of information between various applications based on the schedule defined in the system. Monitoring of batch jobs ensure that jobs that are responsible for the data transfer run successfully. In event of a GITC failure, one cannot be sure of data integrity during transfer of information. Users with inappropriate access can either manipulate information during data transfer or could also modify data during transit by accessing the file in shared folder, FTP path, etc.

03

Data Integrity

Gaps around logical access could impact the sanity of financial data in the application as that would be prone to unauthorised changes. Any specific mitigating procedure in such a case would be impractical as one cannot validate millions of transactions posted by users during the year.

In such a case, one has to explore review type controls, how reviewers validate sanity of information in reports with independent source documents, entity level controls and periodic MIS reporting. The idea would be to consider controls outside the system in order to eliminate system dependency.

Contact

Deepa Seshadri

Partner

deseshadri@deloitte.com

Johar Batterywala

Partner

jobatterywala@deloitte.com

Kedar Sawale

Partner

ksawale@deloitte.com

Ramu N

Partner

ramun@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material has been prepared by Deloitte Touche Tohmatsu India LLP (“DTTILLP”), a member of Deloitte Touche Tohmatsu Limited, on a specific request from you and contains proprietary and confidential information. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. The information contained in this material is intended solely for you. Any disclosure, copying or further distribution of this material or its contents is strictly prohibited.

Nothing in this material creates any contractual relationship between DTTILLP and you. Any mutually binding legal obligations or rights may only be created between you and DTTILLP upon execution of a legally binding contract. By using this material and any information contained in it, the user accepts this entire notice and terms of use.

©2018 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited Deloitte Touche Tohmatsu India Private Limited (U74140MH199 5PTC093339), a private company limited by shares, was converted into Deloitte Touche Tohmatsu India LLP, a limited liability partnership (LLP Identification No. AAE-8458), with effect from October 1, 2015.

© 2018 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited