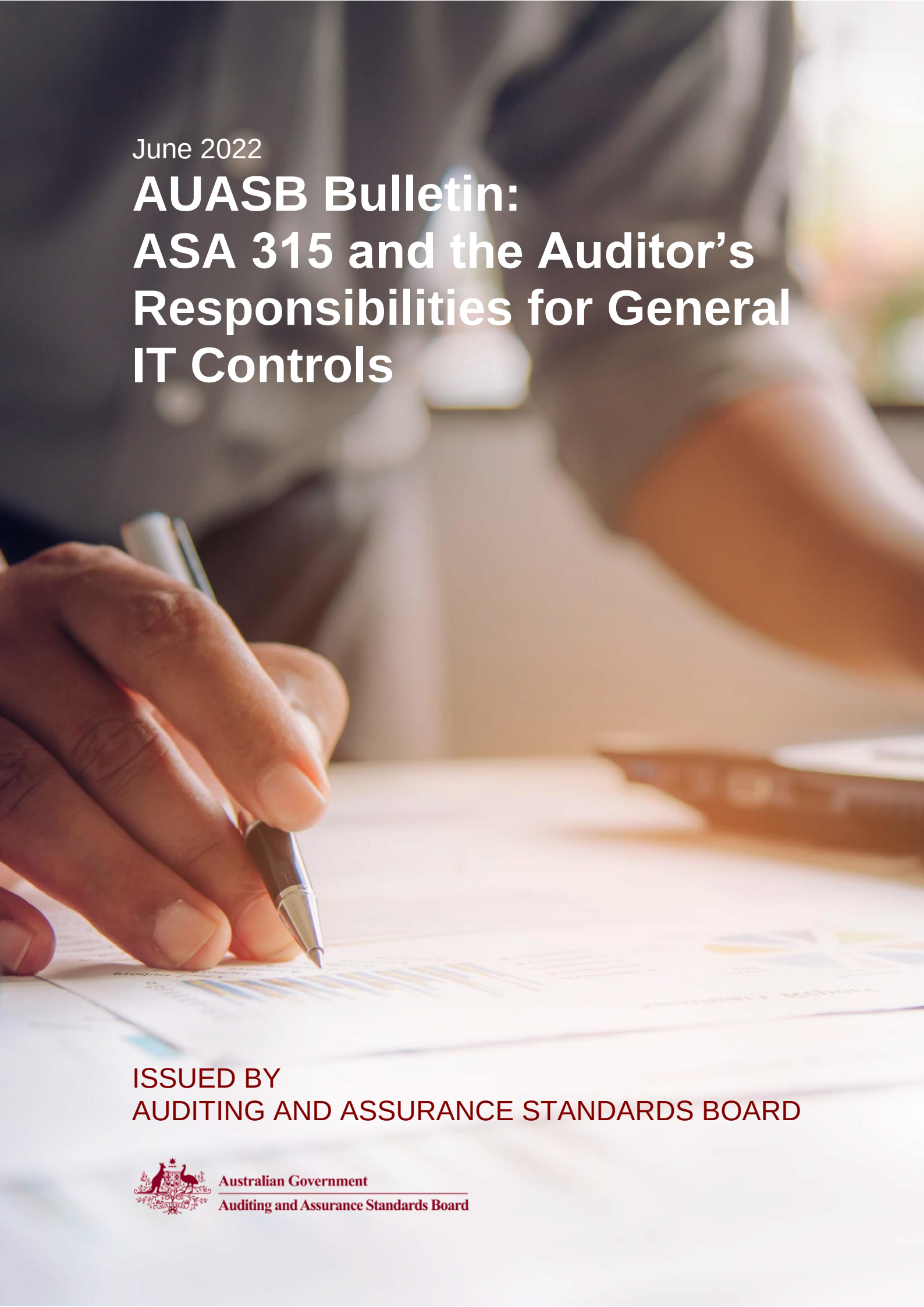


June 2022

AUASB Bulletin: ASA 315 and the Auditor's Responsibilities for General IT Controls

ISSUED BY
AUDITING AND ASSURANCE STANDARDS BOARD

Australian Government
Auditing and Assurance Standards Board

About the AUASB

The Auditing and Assurance Standards Board (AUASB) is an independent, Non-corporate Commonwealth entity of the Australian Government, responsible for developing, issuing and maintaining auditing and assurance standards.

Sound public interest-oriented auditing and assurance standards are necessary to reinforce the credibility of the auditing and assurance processes for those who use financial and other information. The AUASB standards are legally enforceable for audits ore reviews of financial reports required under the *Corporations Act 2001*. For more information about the AUASB see the AUASB Website.

Disclaimer

This publication has been prepared by the Staff of the Office of Auditing and Assurance Standards Board.

The views expressed in this publication are those of the author(s) and those views do not necessarily coincide with the views of the Auditing and Assurance Standards Board. Any errors or omissions remain the responsibility of the principal authors.

Enquiries

Auditing and Assurance Standards Board
PO Box 204
Collins Street West,
Victoria, 8007
Australia

Tel: +61 3 8080 7400

Email: enquiries@auasb.gov.au

Website: www.auasb.gov.au

Copyright

Table of contents

Introduction

The Auditing and Assurance Standards Board (AUASB) has prepared this AUASB Bulletin to assist auditors in understanding the role of *General Information Technology Controls (GITCs)* in the audit of a financial report and the auditor's responsibilities related to GITCs.

This issue is particularly relevant as a result of the modernised and revised ASA 315 *Identifying and Assessing the Risks of Material Misstatement*, which is effective for audits commencing on or after 15 December 2021, which has been enhanced to include auditor considerations in relation to IT, including new and updated appendices for understanding IT and GITCs.

The objective of this publication is to address common questions from auditors about GITCs in the audit of a financial report and the auditor's responsibilities related to GITCs throughout the audit, not just as part of risk assessment in ASA 315. The responses to these common questions are presented as Frequently Asked Questions (FAQs) on pages 6 – 14.

This publication reinforces that the auditor is not responsible for understanding and testing all GITCs within an entity's control environment. The auditor's responsibility is limited to controls which have a direct link to the preparation of the financial report as identified by the auditor in paragraph 26 of ASA 315.

The Auditor's Understanding of the IT Environment and the Identification of General IT Controls

The revised ASA 315 includes significant new material related to IT and the audit of a financial report and has clarified the auditor's responsibilities related to GITCs and the impact they have on how the auditor obtains sufficient appropriate audit evidence. Whilst GITCs on their own are not sufficiently precise enough to respond to risks of material misstatement, they are still an important part of the entity's system of internal control and support the operation of controls and the integrity of data related to the preparation of the financial report.

ASA 315 paragraph 25 requires the auditor to understand the entity's information system relevant to the preparation of the financial report, in particular how information flows through the entity's information system including the IT environment (see paragraph 12(g)).

In paragraph 26(a) the auditor is required to identify controls that address risks of material misstatement at the assertion level, being controls which address significant risks, controls over journal entries, controls which the auditor is planning to use as part of their response to risk and other controls that the auditor, based on their professional judgement, considers appropriate.

Based on the controls identified in 26(a) and using the understanding of the IT environment obtained in paragraph 25, paragraph 26(b) requires the auditor, for each control identified, to identify the IT applications and other aspects of the entity's IT environment that are subject to *risks arising from the use of IT (see FAQ 1)*.

Where no IT applications or other elements of the IT environment are subject to risks arising from the use of IT, there is no requirement to identify GITCs or evaluate the effectiveness of their design and determine whether they have been implemented.

Para. 26(b)
Based on understanding of **para.25(a-b)**, and the identification of controls in accordance with **para. 26(a)**, identify IT applications and other aspects of the entity's IT environment that are subject to risks arising from the use of IT.

Para.A167-A172
The auditor may focus on:

a) Automated controls that management is relying on.
b) Controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.
c) Controls which maintain the integrity of information relating to significant classes of transactions, account balances and disclosures.
d) System generated reports on which the auditor intends to rely upon.

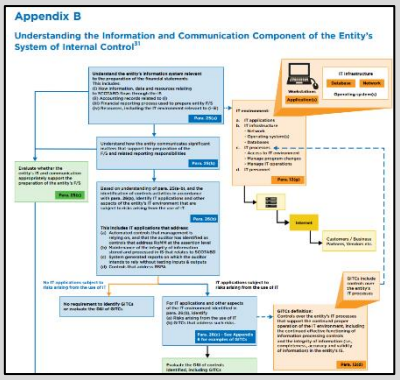
For IT applications and other aspects of the IT environment identified in paragraph 26(b), paragraph 26(c) requires the auditor to identify the specific *risks arising from the use of IT* and the entity's *GITC*s that address those risks and in paragraph 26(d) evaluate the effectiveness of the design of the GITC and determine whether the GITC has been implemented.

For IT applications and other aspects of the IT environment identified in **para. 26(b)**, identify:

a) Risks arising from the use of IT.
b) GITCs that address such risk.

Evaluate the D&I of controls identified in 26(a) and/or 26(c)(iii).

Note:
CPA Canada have developed a **useful flowchart** of paragraphs 25 and 26 of ISA 315 as part of their implementing ISA 315 tool for auditors (see Appendix B of the tool).



Frequently Asked Questions

FAQ 1 – What are risks arising from the use of IT?

Risks arising from the use of IT refers to the susceptibility of information processing controls to ineffective design or operation, or risks to the integrity of information in the entity's information system, due to ineffective design or operation of controls in the entity's IT processes.

Risks arising from the use of IT are identified by the auditor in accordance with paragraph 26(b) based on the controls identified by the auditor in paragraph 26(a). Paragraph 26(b) requires the auditor to identify the IT applications as well as other areas of the entity's IT environment such as databases, network and operating systems, that are subject to risks arising from the use of IT. Common *risks arising from the use of IT* include unauthorised program changes, unauthorised access and inappropriate manual interventions.

Examples of risks arising from the use of IT at an IT application level include:

- Automated controls – Where the entity is relying on an automated three-way match information processing control within an IT application, the IT application may be subject to risks arising from the use of IT such as unauthorised changes to the way in which the control operates or override of the control by management.

- System generated reports – Where system-generated reports are relied upon by management as part of a control, the IT application where the report is produced may be subject to risks arising from the use of IT such as unauthorised or inappropriate changes to the way in which the report operates or direct changes to the underlying data that flows into the report.

The susceptibility of an entity's IT applications to risks arising from the use of IT depends on factors such as the extent to which the entity can access source code and make changes, how IT applications are interfaced and the complexity of the functionality of IT applications. **Appendix 5** of ASA 315 provides helpful material for auditors when identifying risks arising from the use of IT as well as **Appendix 6** which outlines considerations for understanding GITCs.

When the auditor identifies IT applications that are subject to risks arising from the use of IT, other aspects of the IT environment are also typically subject to risks arising from the use of IT. As noted above, the other aspects of the IT environment include databases, operating systems and network.

Examples of risks arising from the use of IT at the IT environment level include:

- Databases – A database which stores data directly related to the preparation of the financial report can be directly accessed by management.

- Operating system – The operating system through which IT applications and databases relevant to the preparation of the financial report are accessed may be subject to risks arising from IT where it does not appropriately manage access.

FAQ 2 – What are General IT Controls (GITCs) and how are they different from Information Processing Controls?

What are 'General IT controls'?

ASA 315 paragraph 12(d) defines *General IT Controls* (GITCs) as controls over the entity's IT processes that **support** the continued proper operation of the IT environment, including the continued effective functioning of information processing controls and the integrity of information in the entity's information system. GITCs may be manual, IT dependent manual controls, or automated, and typically include controls which reduce the risk of:

General IT Controls
Controls that support the continued proper operation of the IT environment, including the continued effective function of IPCs and the integrity of information in the entity's information system.

- Unauthorised access (i.e. controls which authenticate users' access to systems that impact financial reporting)
- Unauthorised changes by privileged users (i.e. controls that manage program or other changes);
- Potential loss of data or inability access data as required (e.g. backup and recovery of financial reporting data in the event of an outage or attack).

Generally, *GITCs* are indirect controls which support the operation of information processing controls and are implemented at the application, database, operating system, or network level[1].

What are 'Information processing controls'?

Information processing controls (referred to in the past as application controls[2]) are defined in ASA 315 paragraph 12(c) as controls relating to the processing of information in IT applications or manual information processes in the entity's information system that **directly address risks** to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information). Information processing controls include controls related to authorisations and approvals, reconciliations, verifications (such as edit and validation checks or automated calculations), segregation of duties, and physical or logical controls, including those addressing safeguarding of assets. When the auditor is identifying controls in accordance with paragraph 26(a), this is focused on information processing controls[3].

Information Processing Controls
Controls relating to the processing of information in IT applications or manual information processes in the entity's information system that directly address risks to the integrity of information.

Information processing controls are generally direct controls that can be automatic (embedded in IT applications) or manual (e.g., input or output controls) and are precise enough to address risks of material misstatement at the assertion level.[4] To operate effectively, information processing controls may rely on other controls, including other information processing controls or GITCs such as those managing access to the source code of the information processing control.

Information processing controls can be automated, manual or hybrid. Some common examples of information processing controls include:

- Automated control – A three-way match control embedded in the entity's accounting package.

---

1 ASA 315 paragraph A150.

2 The IAASB changed *application controls* to *information processing controls* in response to comments raised by stakeholders during the exposure of ISA 315 (revised). The definition of *information processing controls* is drawn from the COSO definition of transaction controls but has been simplified to focus on the role of information processing controls in addressing risks to the integrity of the information in the information system. Refer to the ISA 315 (revised) Basis for Conclusions for a more detailed explanation.

3 ASA 315 paragraph A148.

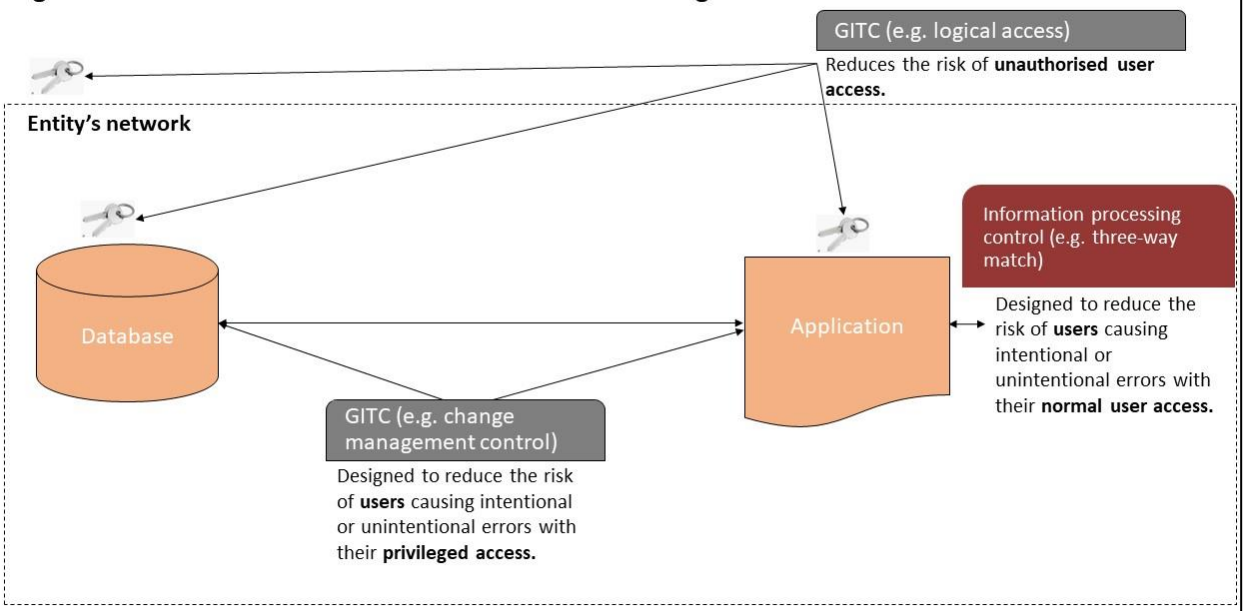
4 ASA 315 para A5-A6.

- IT dependent manual control – Management review monthly a payroll exception report to determine whether there have been any unusual or unauthorised changes to payroll information. The review is done manually by the manager but relies on the information processing controls related to the payroll exception report.

What is the difference?

An important way to distinguish between *information processing controls* and *GITC*s, is the level they operate and what they are targeted at preventing. A common example of a GITC in an entity is the access controls that are in place for specific IT applications as well as databases.

Figure 1 – General IT Controls and Information Processing Controls



In the above example, the logical access *GITC* for the IT application prevents unauthorised users from accessing the application. However, it does not prevent authorised users from making errors once they are in the IT application. The logical access GITC for the database prevents unauthorised access to the database but similarly to the IT application GITC, the GITC does not prevent authorised users from altering data in the database.

Conversely, the three-way match *information processing control* embedded in the IT application is designed to reduce the risk of authorised users making intentional or unintentional errors in the financial data by only processing transactions which have a matching purchase order, vendor shipping document, and vendor invoice.

The GITCs on their own are not sufficiently precise enough to respond to risks of material misstatement but support the operation of information processing controls.

FAQ 3 – When does the operating effectiveness of GITCs need to be tested?

In accordance with ASA 315 paragraph 26(d), the auditor is required, for each control identified in paragraphs 26(a) and 26(c), to evaluate whether the control is designed effectively to address the risk of material misstatement at the assertion level, or effectively designed to support the operation of other controls and determine whether it has been implemented. This occurs regardless of whether the auditor plans to rely on the operating effectiveness of controls as part of the auditor's planned response to address the assessed risks of material misstatement.

Where the auditor plans to rely on the operating effectiveness of controls as part of the auditor's response to address the assessed risk of material misstatement and those controls are dependent upon GITCs, the auditor tests the operating effectiveness of GITCs.[5]

Whilst the most common reason that the operating effectiveness of a GITC is tested is to support the auditor's assessment of the operating effectiveness of an automated information processing control, there may be other instances where evidence about the operating effectiveness of *GITC*s is relevant for other procedures which may include:

- Substantive analytical procedures – GITCs may be relevant where the auditor is testing the reliability of data to be used in a substantive analytical procedure and has determined that this will be done through testing the operating effectiveness of information processing controls. In this situation, the auditor is relying on the operating effectiveness of information processing controls to provide evidence about the completeness, accuracy and validity of data which is forming part of the auditor's substantive analytical procedures. (e.g., unit rates from a master list which will be used to recalculate the value of a certain class of transactions).

- Controls over journal entries – When testing non-standard journal entries as part of journal entry testing, the auditor may rely on GITCs that manage permissions for posting non-standard journal entries.

- Custom built reports – Where the auditor's substantive procedures utilise system-generated reports, the auditor may test the operating effectiveness of GITCs that address the risk of inappropriate, unauthorised or direct changes to the report. (See **FAQ 5** for more information about this).

[5] ASA 330 paragraph 10.

FAQ 4 – What is the impact of GITCs not being appropriately designed and implemented or not operating effectively?

ASA 315 paragraph 34 requires the auditor to assess control risk as part of their assessment of the risk of material misstatement at the assertion level.

The auditor's plans to test the operating effectiveness of controls is based on the expectation that controls are operating effectively, and this will form the basis of the auditor's assessment of control risk. The auditor develops the expectation that controls are operating effectively based on the auditor's evaluation of the design, and the determination of implementation, of the identified controls in paragraph 26.

Where GITCs are not appropriately designed and/or implemented, the auditor considers the impact of this on their assessment of control risk in accordance with paragraph 34 of ASA 315[6]. When a particular GITC is not designed or implemented properly, the auditor's assessment of control risk may take into account whether:

- there are any alternate *GITC*s, or any other controls, that address the related risk(s) arising from the use of IT;
- the auditor can design suitable substantive procedures to address the applicable risks arising from the use of IT.

> **Example**
>
> The auditor has concluded that a *GITC* to prevent unauthorised changes to an automated information processing control was not operating effectively during the audit period but all other relevant GITCs were. The auditor may determine that they can manually review the IT application change log to determine whether any unauthorised changes occurred during the period which would impact on the operating effectiveness of the automated information processing control.

Where there are no alternate GITCs or the auditor is unable to design suitable substantive procedures to address the applicable risks arising from the use of IT, the auditor may be unable to rely on:

- The operating effectiveness of automated controls within the affected IT applications (as such controls may not appropriately prevent or detect unauthorised program changes or access to IT applications);
- The completeness, accuracy and validity of system-generated reports used for audit purposes, or other reports built in-house by the audit client and IT dependent manual controls that rely on such reports (as the integrity of the information content of such reports may not be guaranteed); and
- The operating effectiveness of input controls which provide assurance over data entered into a system (as the IT application may fail to sufficiently reduce the risk of intentional and unintentional erroneous changes to data after it has been entered into the system). This may also affect any substantive analytical procedures that the auditor may have planned to undertake which relies on point in time data.

Where the auditor is relying on the operating effectiveness of controls as part of the auditor's response to address the assessed risks of material misstatement and GITCs are determined to not be operating effectively, the auditor will consider the impact on the controls that are supported by the GITCs.

---

6 ASA 315, paragraph A229.

In addition to the matters raised above as part of the auditor's consideration of the impact of GITCs not being designed or implemented properly, the auditor may also consider:

- Whether the risk of material misstatement is required to be revised to reflect the new information about the operating effectiveness of controls in accordance with ASA 315 paragraph 37.

- Where there are one or more control deficiencies, whether they represent a significant deficiency and require report to those charged with governance in accordance with ASA 265 *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*.

In circumstances where the auditor has determined, in accordance with ASA 315 paragraph 33, that substantive procedures alone cannot provide sufficient appropriate audit evidence to address a risk and alternative procedures are unable to be performed, there may be an impact on the auditor's ability to obtain sufficient appropriate audit evidence and the audit opinion.

FAQ 5 – Are GITCs relevant if I am taking a substantive approach?

As outlined above, *GITCs* are important responses to risks arising from the use of IT, that is risks to the completeness, accuracy and validity of information in the information system. In certain situations, *GITCs* are still relevant for the auditor to evaluate the design and determine whether they have been implemented and test the operating effectiveness of even if the auditor is intending to respond to a risk through performing substantive procedures.

For example, when the auditor intends to use information produced by the entity in their substantive test(s) (e.g. system-generated reports) as audit evidence and that information is produced by an IT application, the auditor may plan to test the information processing controls within that IT application that ensures the completeness and accuracy of the system-generated reports, including identifying and testing the *GITCs* that address risks arising from the use of IT (e.g. inappropriate or unauthorised program changes or direct data changes to the reports).

In some instances, the auditor may be able to test the completeness and accuracy of system-generated reports substantively whilst in other instances, due to the complexity of the system, the auditor may not be able to test the completeness and accuracy of the system generated report substantively.

Regardless of whether the auditor plans to test the operating effectiveness of controls, the auditor is required to obtain an understanding of the control activities component in accordance with ASA 315 paragraph 26, which may include evaluating the design and determining the implementation of GITCs.

FAQ 6 – What is the nature and extent of testing of the operating effectiveness of GITCs?

How the auditor tests the operating effectiveness of GITCs is dependent on the nature of the control and the complexity of the entity's IT environment. **Appendix 6** provides examples of common risks arising from the use of IT and GITCs which respond to those risks. Importantly, the table in Appendix 6 highlights that the types of GITCs to respond to risks arising from the use of IT may change depending on the complexity of the IT environment. In a less complex IT environment, GITCs may more commonly be manual controls (e.g. user access to IT applications is periodically reviewed by management) compared to a more complex IT environment where GITCs are embedded into IT applications and databases and operate automatically (e.g. multifactor authentication to access an IT application).

When testing GITCs, auditors may need to rely on specialist skills such as IT auditors to assist them in obtaining sufficient appropriate audit evidence as the complexity of the IT environment increases. It is the responsibility of the engagement partner under *ASA 220 Quality Management for an Audit of a Financial Report and Other Historical Financial Information* to ensure that members of the engagement team, and any auditor's external experts who are part of the engagement team, collectively have the appropriate competence and capabilities to perform the engagement.

Whilst the auditor's focus may be on *GITCs* that support *information processing controls* embedded in IT applications, as their impact on the financial report can be easily identified, it is also important for the auditor to address *risks arising from the use of IT* identified in other elements of the entity's IT environment (i.e. IT infrastructure such as databases) as part ASA 315 paragraph 26.

IT applications are what most normal users see (e.g. SAP, People Soft, etc.), they are the systems by which normal users input and view data. Where the data is actually stored is underlying databases which are accessible by privileged users (generally IT personnel). Whilst the auditor's focus may be on the risks within IT applications, the auditor should also consider risks arising from other elements of the IT environment such as databases as well as from personnel not involved in inputting data through IT applications but who have privileged access to databases etc.

Example

An auditor is planning to rely on the operating effectiveness of an *information processing control* in the entity's accounting package (IT application) which requires a three-way match of a purchase order, vendor shipping document, and vendor invoice to post a transaction. The auditor has evaluated the design, determined it has been implemented and tested the operating effectiveness of the information processing control and as part of this testing also tests GITCs which prevent unauthorised changes being made to the information processing control by privileged users.

However, the auditor has identified that there are no controls which prevent unauthorised access to the database which stores the usernames and passwords of authorised persons who are able to make changes to the information processing control. This may result in the auditor not being able to rely on the results of the testing, even if the GITC to prevent unauthorised changes to the control was working. The auditor may be able to perform alternative procedures such as manually reviewing logs to verify whether any changes were made to how the control operated.

The extent of the auditor's work around GITCs is a matter of professional judgement. The auditor is not responsible for identifying all controls within the entity's control environment including its IT environment.

FAQ 7 – Does the operating effectiveness of GITCs have to be tested every year?

In certain circumstances, the auditing standards allows auditors to use audit evidence about the operating effectiveness of controls obtained in previous audits. ASA 330 paragraph 13 outlines the considerations for the auditor when determining whether it is appropriate to use audit evidence about the operating effectiveness of controls obtained in previous audits.

However, in paragraph 13 the auditor is specifically required to consider the effectiveness of *GITCs* as part of determining whether audit evidence regarding the effectiveness of a particular control from a prior period can be used in the current period. Due to their importance, *GITCs* should be tested annually if they are to be relied upon as part of the audit.