HOW TO GUIDE - AUGUST 2022

UNDERSTANDING YOUR IT ENVIRONMENT

BDO

CONTENTS

1 UNDERSTANDING INFORMATION SYSTEMS RELEVANT TO FINANCIAL REPORTING

2 HOW IS THIS INFORMATION OBTAINED?

3 WHAT CHALLENGES MAY BE ENCOUNTERED IN OBTAINING A COMPLETED UITE?

4 WHAT IS THE STRUCTURE OF THE UITE?

5 CONCLUSION

INTRODUCTION

This publication provides guidance to engagement teams to effectively obtain an understanding of an entity's Information Technology (IT) environment through the use of the 'Understanding Your IT Environment' template. This publication can also be used to provide further detail regarding the information requested to allow the engagement team to have an informed conversation with our clients.

Understanding the entity's IT environment is a component of the system of internal control which engagement teams must evaluate during risk assessment procedures in accordance with ISA 315 (Revised 2019), *Identifying and Assessing Risks of Material Misstatement*. The objective of understanding the IT environment is to identify potential risks arising from the use of IT through identifying key IT applications and processes relevant to the audit. This information will then assist in identifying IT general controls (ITGCs) that address those risks and creating specific audit responses to address those risks, as applicable. This is the same process followed for business cycles and identifying related control activities relevant to the audit (CARA).

GO FORWARD

GO BACK

RETURN TO INDEX

1.

Understanding information systems relevant to financial reporting

Understanding the entity's information systems includes the information processing activities relevant to the financial reporting which includes:

- Initiation of transactions, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger, and reported in the financial statements.
- The accounting records, specific accounts in the financial statements and other supporting records.
- The financial reporting process used to prepare the entity's financial statements, including disclosures.

This information should be documented as part of the business cycle understanding

Engagement teams cannot fully understand the information systems without also understanding the IT applications that are used in the various information processing activities, as well as the overall IT environment within which those IT applications operate.

UNDERSTAND THE IT ENVIRONMENT RELATED TO THE INFORMATION SYSTEMS RELEVANT TO FINANCIAL REPORTING

The IT environment consists of the IT applications and supporting IT infrastructure, as well as the IT processes and personnel involved in those processes that an entity uses to support business operations and achieve business strategies.

DEFINITIONS

An **IT APPLICATION** is a program or a set of programs that is used in the initiation, processing, recording and reporting of transactions or information. IT applications include data warehouses and report writers.

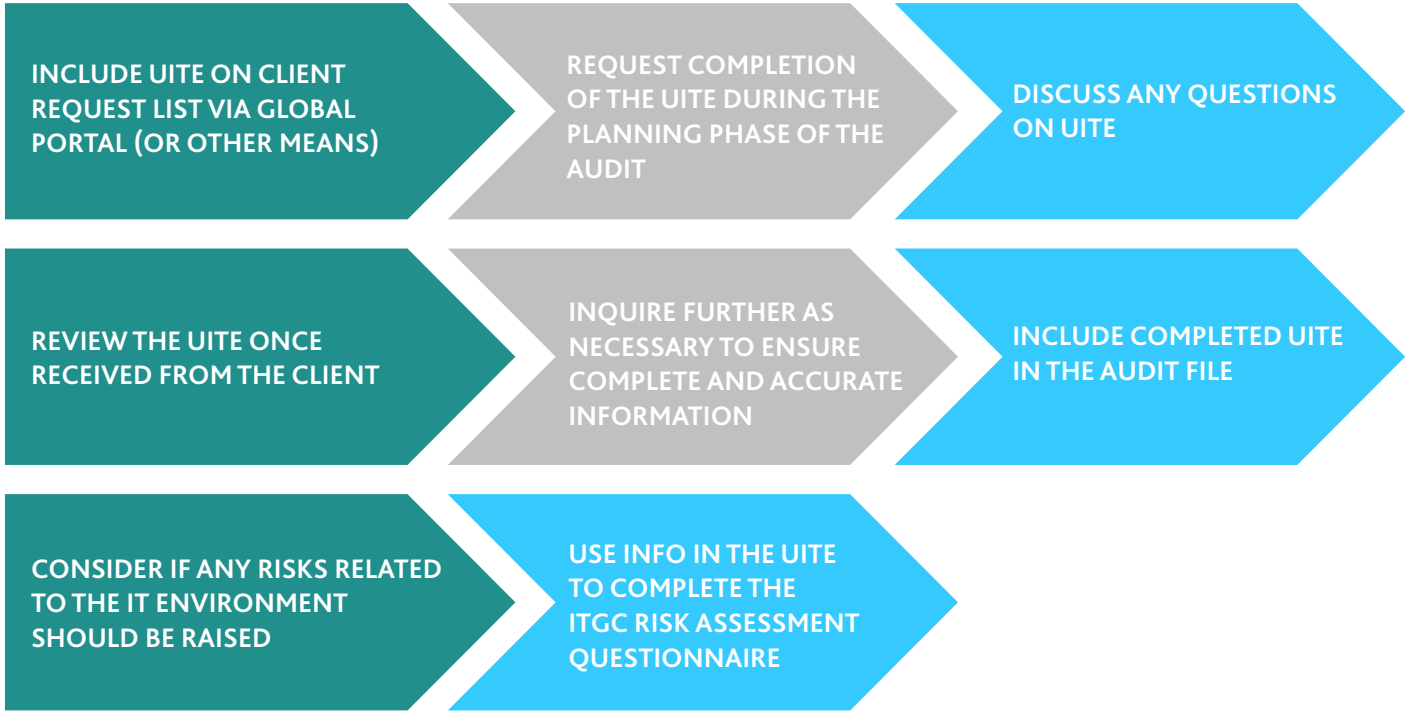
The **IT INFRASTRUCTURE** comprises the network, operating systems, and databases and their related hardware and software.

The **IT PROCESSES** are the entity's processes and controls to manage access to the IT environment, manage program changes or changes to the IT environment and manage IT operations.

2.

How is this information obtained?

The 'Understanding Your IT Environment' (UITE) (document 2.06.01 in the international APT library) is available to assist in gathering the relevant information about the IT environment.



Alternatively, rather than sending the UITE template to the client to complete, an engagement team may prefer to make direct inquiries of relevant IT personnel at the entity and record their answers in the template. The entity's IT personnel will also be asked to send supporting documents, as applicable, to the engagement team who then reviews them to confirm their understanding. Either option is acceptable; engagement teams should choose the option that works best for each entity. Keep in mind that the less sophisticated the entity and the related IT structure, the more guidance that may need to be provided.

Once the template has been obtained in the first year, it can be utilized in subsequent years as a starting point for our IT understanding. Engagement teams and the entity will review and update the document each year to determine if any relevant changes to the information/processes are required (e.g., new software implementations, cyber-attacks, changes in IS/IT structure, etc.) as this information may present additional risks arising from the use of IT.

3.

What challenges may be encountered in obtaining a completed UITE?

CHALLENGE	POTENTIAL APPROACH TO ADDRESS
Only partial responses were given to some questions	Set up a phone call or in-person meeting with relevant members of the IT and/or Finance teams to discuss the document and determine whether the partial responses were due to items not being applicable or the entity not understanding what was being asked.
The entity does not know how to complete the template / understand what we are looking for	There may be instances where the entity we are auditing does not have a detailed understanding of their IT environment or does not have dedicated IT personnel. In such circumstances, engagement teams may consider setting up a phone call or in-person meeting with the client or third party service provider who is familiar with the entity's IT environment to discuss in further detail. In many cases, the entity may not be using the IT systems in a complex manner; therefore, many of the information gathering sections may be N/A. Consider consulting with an IS Audit Specialist if information is unable to be obtained.
The entity refuses to submit the information due to confidentiality concerns	All of our engagement letters should include clauses in relation to client confidentiality, which includes information related to IT systems. If this challenge is presented, the engagement team shall understand the reasons for the refusal, and inform the engagement partner who can then have relevant conversations with management and/or those charged with governance as applicable.

4.

What is the structure of the UITE?

The template includes three main sections:

SECTION 1 - ORGANIZATION AND SYSTEMS OVERVIEW

Understanding obtained: Documents an overview of the IT functions and infrastructure, as well as the IT applications supporting financial reporting.

Purpose: To determine how IT systems are managed (internally and externally), identify key components of the IT environment to understand how the entity is using IT, identify IT applications that may be relevant to the audit, and understand significant changes in the IT environment that may pose additional risk to the audit.

The following information is documented in this section:

- Main client contacts
- The IT function and IS Security function
- Relevant IT suppliers or external service providers
- Network infrastructure and security
- Significant changes in the IT environment
- List of applications / systems / data warehouses relevant for processing and recording of financial information.

SECTION 2 - AUTOMATION AND USE OF DATA

Understanding obtained: Document interfaces that transfer transactions or financial data between their financial applications.

Purpose: To identify and understand how information is transferred from one system to another, which may pose additional risks to the audit, and also to identify key reports / IPE that may be utilized as part of the audit approach (we assess the reliability of any IPE used as audit evidence later).

The following information is documented in this section:

- Data flow diagram of financial reporting applications
- Main interfaces between applications that support the business processes / cycles
- The use of complex technology components (e.g., blockchain, robotic processing automation (RPA), artificial intelligence, etc.).

SECTION 3 - DESCRIPTION OF IT PROCESSES

Understanding obtained: Documents the processes and controls surrounding the IT environment to build our understanding of the control environment.

Purpose: To understand what processes an entity has in place to address the risks related to the use of IT and whether any IT related events occurred during the year that could give rise to a material misstatement.

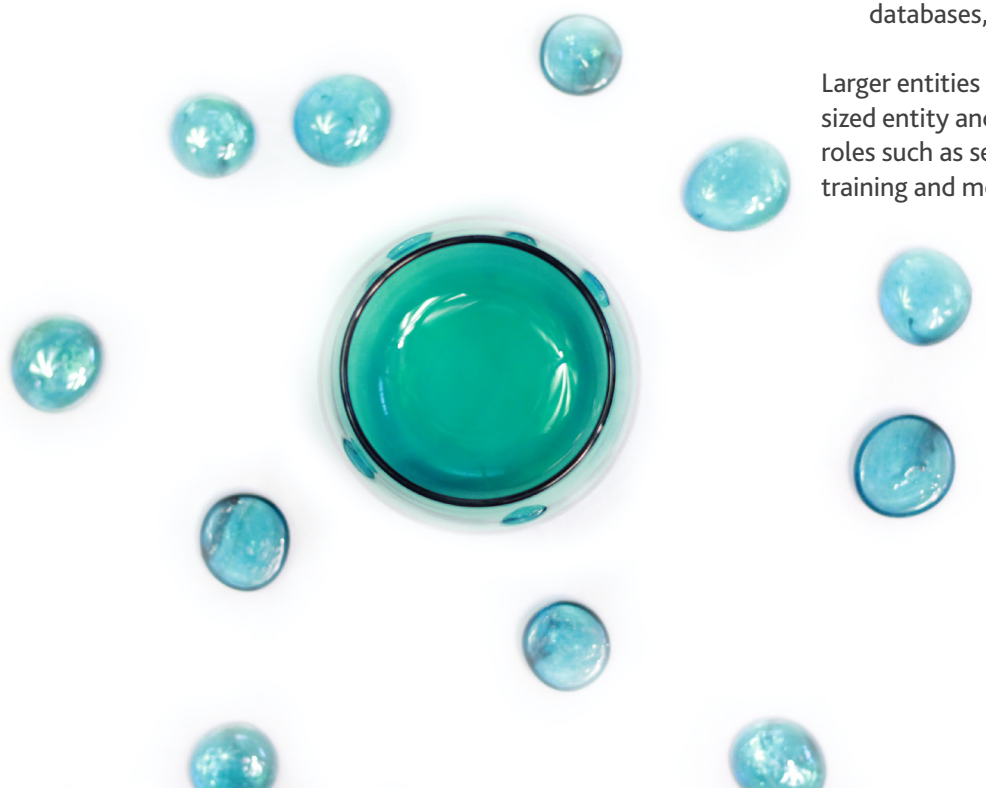
The following IT processes or events are documented:

- Manage access
- Manage changes
- IT operations (data processing)
- Other relevant IT processes such as backups and physical security
- Security events that occurred during the period and security processes.

HOW TO COMPLETE SECTION 1 - ORGANIZATION AND SYSTEMS OVERVIEW

SECTIONS 1.1. AND 1.2

Indicate the main IT and accounting contact(s) in Section 1.1, and briefly describe the IT function and IS security function in Section 1.2. This section can be completed either by obtaining IT and IS function organizational charts or describing the relevant functions in narrative form. This information assists in understanding the competence of the IT personnel and the structure of the overall IT environment.



IT functions at small, medium and large entities

The organization of the IT function at a small entity may consist of a limited number of employees responsible for all the IT processes and resources, or the IT function may be outsourced to an IT service provider.

At a medium-sized entity, the IT function usually includes the following units:

- System Development unit - responsible for applications development and program changes
- Service Support unit – responsible for service interruptions and providing service desk support
- System Support unit – responsible for the maintenance of databases, networks, servers, firewalls and other systems.

Larger entities generally include the functions of a medium sized entity and may also have additional service and process roles such as service architecture, operational management, training and more.

IS Security functions at small, medium and large entities

The IS security function in a small organization is likely to be outsourced to a third party due to resource and/or knowledge constraints.

In medium and large entities, the IS security function is likely to be present and, if in-house, should be separated from the IT function due to its nature (i.e., a monitoring and control function).

Where internal service providers (i.e., group shared resources) or external service providers are utilized, they should be included within the organization chart or table provided within the document as they are an integral part of the IT or IS functions.

The IS Security function, which is typically managed by the Chief Information Security Officer (CISO), is normally responsible for securing the confidentiality, integrity and availability of entity information. They do this by developing and implementing a security program which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats. Additional responsibilities of an IS Security function may also include:

- Conducting employee IT security awareness training
- Developing secure business and communication practices
- Identifying security objectives and metrics
- Choosing and purchasing security products from vendors
- Ensuring that the entity is in regulatory compliance.

SECTION 1.3

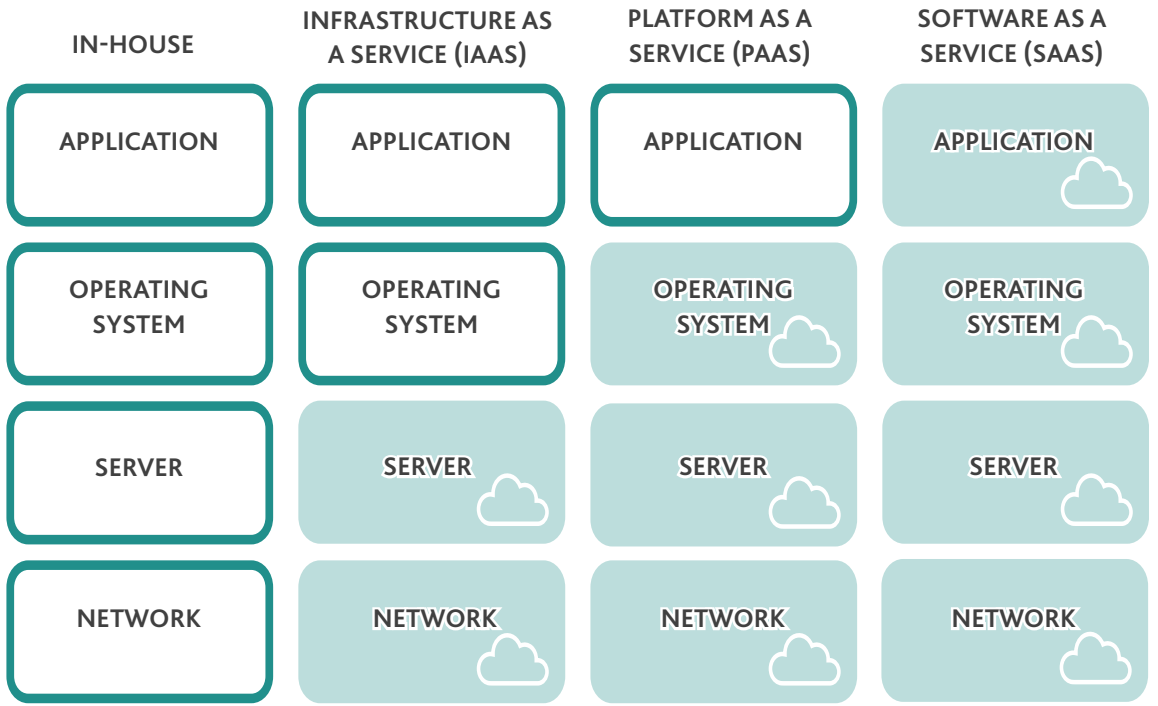
This section documents the external service providers supplying services to the entity that may directly or indirectly affect the completeness and accuracy of financial data or that results in a significant dependency by the entity on the third partly services that may result in unavailability of financial data and transactions.

Common services that may be outsourced or allocated to external service providers include:

- Software development and maintenance
- Infrastructure maintenance (operating systems, network and security tools)
- Outsourcing of IT personnel
- Hardware purchase and maintenance
- Cloud services such as:
    - Infrastructure as a service (IaaS) - This is a type of cloud computing service where the service provider offers server and networking resources on demand while the entity manages the operating system and applications
    - Platform as a service (PaaS) – This is a cloud computing service where the service provider offers network, server and operating system resources while the entity manages only the applications.
    - Software as a service (SaaS) – This is a type of cloud computing service where the service provider offers network, server, operating system and applications resources on demand. It allows the entity to connect to and use cloud-based apps over the Internet. Common examples are office tools (e.g., Microsoft Office 365), accounting applications (e.g., NetSuite, Xero, MYOB) and sales applications (e.g,, Salesforce.com).

The service provider name is recorded in the table in Section 1.3 as well as the description of the service(s) provided. Additionally, indicate in this table whether the service providers follow the entity's processes or their own processes and whether an ISAE 3402 report *(Assurance Reports on Controls at a Service Organization)* or a SOC 1 report (US equivalent), an ISAE 3000 report *(Assurance Engagements Other Than Audits or Reviews of Historical Financial Information)*, or a SOC 2 report is available. Consult your local firm's policy with respect to the auditors' use of and reliance upon such reports.

The following diagram illustrates the major elements of an information system when they are managed in-house by the entity compared to when they are managed by a service provider under various cloud service arrangements:



SECTION 1.4

WHAT INFORMATION IS REQUIRED TO BE GATHERED RELATED TO THE NETWORK INFRASTRUCTURE AND SECURITY?

In this section, the entity's network infrastructure and security, including the entity's data center location, is described in narrative or diagram form. Also included is whether the entity is using cloud services as explained in Section 1.3 or web-facing applications of a shared service center (i.e., web applications that are visible or accessible from the Internet).

The entity's personnel or engagement team also describes how employees, third parties and business partners can gain remote access to the entity's IT environment (e.g., IT applications, databases, folders or reports) and which security methods and tools are implemented, such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), etc.

Engagement teams are encouraged to attach a network infrastructure and security diagram, if available, to visualize the above description and for better understanding of the entity's network components.

The depth of understanding of the network infrastructure and security depends on the nature and characteristics of the relevant IT applications, the susceptibility of the integrity of underlying information to possible threats and the ability of the entity to continue their operations when incidents occur. For example, the network infrastructure and security are relevant to the audit if external parties could significantly benefit from manipulating underlying information, particularly when such information cannot easily be reconciled to documents or movement of goods.

If external network access is important, we obtain an understanding of the use of the centralized network, the access management system (e.g., Microsoft Active Directory) and the network segmentation (i.e., where the entity has divided the network into subnets and secure zones such as DMZs (demilitarized zones)). In addition, the tools in place to protect the network, such as firewall, IDS (intrusion detection system), IPS (Intrusion Prevention System) and other network monitoring tools, are described in this section. Understanding such tools will require the involvement of an IS Audit Specialist. However, if external network access is less important, an understanding of the access management system may be sufficient to understand access to IT applications, databases and the operating system.

SECTION 1.5

This table is completed only if significant changes have been made to the IT environment during the audit period which could give rise to additional risks from the use of IT. If additional significant changes not included within the table are identified relevant to financial applications, complete the last line and, if needed, add additional lines to the table.

SECTION 1.6

The table in this section documents the IT applications used by the entity which are supporting business cycles or functions and their main characteristics.

The business cycles/functions and IT applications can be pre-populated by the engagement team prior to sending the UITE to the entity during the planning process using the information obtained from the prior year file.
The client can then confirm the accuracy of the information based on their review and update as applicable.

The business cycle or function is recorded in the left column in Section 1.6. Most entities use IT applications for processing and recording financial information relating to their common business cycles such as revenue, purchases, payroll and cash/treasury, as well as for the financial reporting process. Some entities may have additional applications for specific functionality.

EXAMPLE

A construction company may use a project management application, or a production company may use an application to manage the production process, which flows into the financial reporting process and therefore should be included within the table.

In the 'Application' column in Section 1.6, record the IT application's official name as defined by the supplier and also include the supplier's name (if the IT application name and supplier name are not the same). Record the version number in the next column. Some in-house applications are not named, and, in such cases, name the application as follows: 'in-house developed' and then describe the module/function (e.g., general ledger).

When listing applications, also include (if applicable) any data warehouses used by the entity which generate financial reports.

A data warehouse is a system that pulls together data from different sources within an organization for reporting and analysis. Reports created from complex queries within a data warehouse are used to improve business efficiency, decision making and financial reporting.

EXAMPLE

An entity may use a data warehouse system to create a credit loss report which pulls data from various sources and is a key IPE report.

Drop-down menus within the table are provided to assist with recording:

- Whether or not the application was implemented or upgraded during the audit period
- How it is hosted (the infrastructure location is onsite on the entity's server, with a third party or at a shared service center)
- If authentication to this application is done using a single sign on mechanism
- The type of application software (e.g., in-house developed, standard off-the-shelf, customized off-the shelf or software as a service).

If the application is hosted on the entity's servers or within a shared service center, add the name of the application's operating system, the database type and the database version in the relevant columns of the table. Entities using a cloud hosted application may not be able to obtain such information, so those fields should be labelled not applicable or N/A.

Add either "Yes" or "No" to the configurable setting question in the right column. Answer "Yes" if the IT department, users, data owners or suppliers can change the application settings in a way that may influence the input, processing and output of transactional data in the system. Application configuration changes may range from limited changes (for example, simple user preference changes) to those with a significant impact on financial reporting (for example, changes to inventory and fixed asset valuation methods, system access management, ageing report parameters, automated application control settings, application workflow settings, etc.). As a result, configuration changes may impact the audit approach, and therefore it is important for the engagement team to understand when configurable settings can be changed.

APT Next Gen linkage: The information obtained within Section 1.6 includes the information necessary to complete the 'IT applications relevant to the audit' table within the ITGC Risk Assessment Questionnaire. Information entered in this questionnaire also determines whether an IS Audit Specialist needs to be involved in assessing the ITGCs.

HOW TO COMPLETE SECTION 2 - AUTOMATION AND USE OF DATA

Within this section, information is gathered to understand how data is transferred from one system to another, whether in a fully automated, semi-automated or manual manner. Document interfaces that transfer transactions or financial data between financial applications. Such interfaces may be within the entity or with external parties.

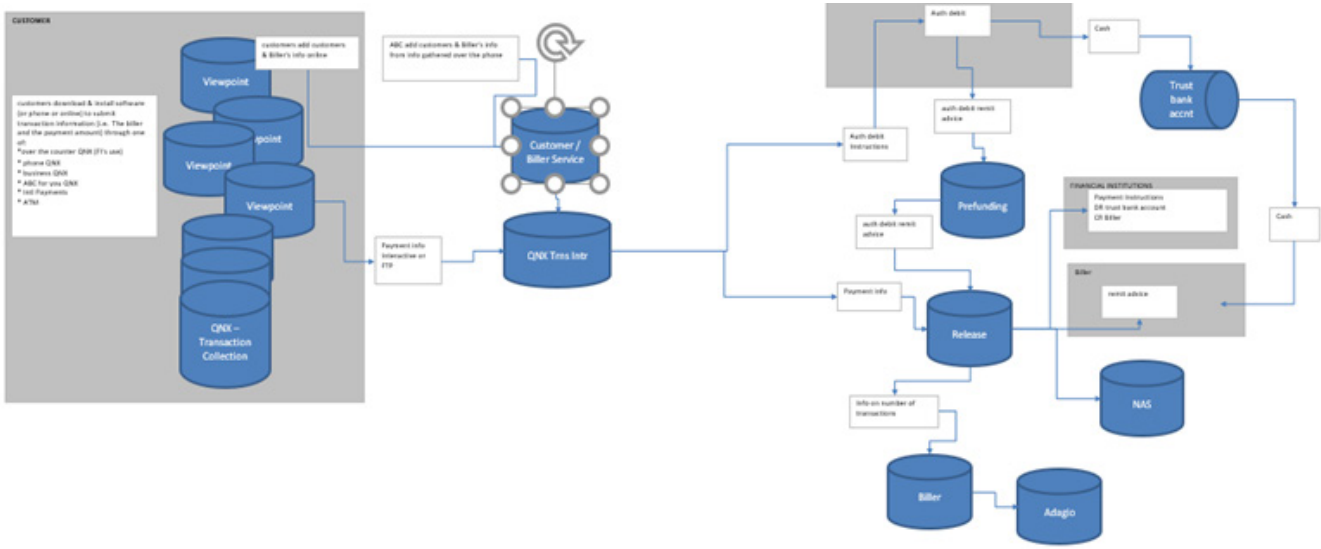
EXAMPLES

1. Invoices may be automatically transferred from a billing application to the general ledger in the accounting application.
2. The transfer of sales and receipts information from a cashier in a shop to the accounting application may occur in a semi-automated manner (i.e., when triggered by a human action such as an approval).
3. A user-generated export of monthly payroll entries to Excel from a payroll application and an import of these entries to the general ledger is an example of a semi-automated interface.

NOTE 1: Interfaces that transfer non-financial information which is not relevant to business cycles or financial reporting (e.g., help desk tickets transferred from an external system to the entity's help desk application, or product reviews being transferred from external applications) would not be included within this section.

Data used by various modules of a single ERP system that has a central database are not considered interfaces. However, if the data is exported from the ERP system to a data warehouse system or other system for reporting purposes, or if bank statements are imported to the ERP system, those movements are considered interfaces.

The diagram below provides an example of what a data flow diagram of transactions or financial data could look like.



The application names included should be consistent with those recorded in Section 1.6. If any additional applications are identified, these applications may need to be added in both sections to ensure a complete population of relevant applications.

If such a data flow diagram does not exist, the description and frequency of data flows between applications may be recorded in the table provided in Section 2.2 of the UITE.

In the 'details on the interface' column in Section 2.2, briefly describe data which is transferred and the interface automation level (fully automated, semi-automated or manual interface) as well as the monitoring controls implemented by the entity to assure data completeness and accuracy (e.g., log review, exception reports, manual reconciliations, batch monitoring, etc.).

The frequency column includes a drop-down menu with the following options:

- 'Batch' (e.g., where data is accumulated and then transferred overnight, 'x times daily' or at the end of the month in an automated or semi-automated manner)
- 'Real-time' (i.e., the data is transferred within a specified timeframe, which is usually a very short time, such as within minutes)

Identifying the interfaces between IT applications may help the engagement team identify where risks could exist in certain cycles. For example, if data is transferred manually between IT applications, there is potential for human error in what is recorded in the general ledger.

Complete Section 2.3 only if complex technology components are used by the entity such as recording transaction on public ledger (i.e., blockchain), use of robotic processing automation (RPA) or artificial intelligence. If the entity uses any of these complex technologies in areas that affect financial reporting, consultation with an IS Audit Specialist on the extent of involvement would be necessary.

HOW TO COMPLETE SECTION 3 - DESCRIPTION OF IT PROCESSES

This section documents the IT processes implemented by the entity. Documentation includes how the entity manages access to its IT resources (i.e., logical access), as well as changes to programs, databases, operating systems and network components (i.e., program changes) and the IT operations of data processing. Additionally, the following processes should also be recorded: the backup process and IT continuity, physical security controls around data centers, and security events and processes.

APT Next Gen linkage: The questions in Section 3 relate directly to the assessment of relevant ITGCs in the ITGC Risk Assessment Questionnaire. We can utilize these responses in documenting our understanding of ITGC design within the questionnaire.

Depending on the sophistication of the IT environment and personnel, the entity may have formal internal policies and procedures documented which they are able to send in lieu of providing a narrative description. If the entity does not have formal policies or procedures documented, we can still obtain an understanding of their processes by having them complete the description in a narrative format within the UITE template.

APT Next Gen linkage: These policies can be added to the audit file, as deemed applicable, and linked from the design section of the ITGC Risk Assessment Questionnaire where relevant using the # functionality.

SECTION 3.1 - MANAGE ACCESS

Document in Section 3.1.1 how the entity manages access to the network, IT applications, operating systems, and databases. Describe if access to the IT resources is through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Access should be limited to authorized personnel, based on their job responsibilities and assigned role, and such access should be approved by management or process owners. Describe the user access termination process and periodic review of user rights.

Also include the entity's resources that are managed by an external party. Here are typical examples of such circumstances:

An entity using a cloud environment (SaaS) may not be able to manage access to the databases and operating systems as that is done by the service provider.	An entity using an off the-shelf application may not be able to manage access to the application database which is probably locked by the software supplier.	If an entity has outsourced its IT operations to a third party, access to databases and operating systems is controlled by the third party.

Describe in Section 3.1.2 the privileged user account administration process (e.g., software administrators, network administrators and database administrators). Document the process of granting and disabling privileged accounts access to systems and resources and the segregation of duties.

In addition, describe the user account management processes (e.g., manually manage the users' rights or use an automated tool that executes the changes). Also describe user accounts authentication to relevant applications / systems (e.g., passwords, tokens, smartcards, biometrics, etc.).

Document in Section 3.1.3, for each type of IT resource (applications, operating systems and databases) included in Section 1.6, the parameters regarding password strength and describe the nature of two factor authentication, if applied. IT resources with different password parameters or different two factor authentication methods should be separately described. For example, if an entity is using an ERP system (where the password rules include a minimum length of 8 characters with at least one capital letter and one symbol) and a separate payroll application (where the password rules only require a minimal length of 4 characters with no other complexity rules), these should be separately documented in the table.

Although the most common authentication method is the use of passwords, due to recent cyber-attacks, entities are increasingly using two factor authentication. Examples of two factor authentication may include a token that generates a one-time password, smart cards or instant SMS messages with a code, or use of biometric authentication. If an entity uses two factor authentication, select 'Yes' in that column and describe details about the two factor authentication in the last column of the table..

Application / operating system / databases	Password strength (document parameters or provide a screenshot of the settings)	Two factor authentication (i.e., token, SMS, other) (Y/N)	Describe two factor authentication (if applicable)
Domain controller	8-character minimum length, complex character composition requirements, 90 day password resets	Yes	Token

SECTION 3.2 - MANAGE CHANGE

Document in this section the processes for managing changes and updates to IT applications / programs, databases and operating systems. Changes may be necessary or recommended for the following reasons:

- System maintenance
- Business and regulatory requirements
- IT vendor's version updates
- Patches to eliminate security vulnerabilities
- Implementation of new software.

Briefly describe in Section 3.2.1 the change request process and the internal procedures that the entity has implemented. Describe if the changes are to be performed by the IT function, an IT consultant / external party or processed by a software supplier. Additionally, document how the change requests are submitted, reviewed, approved and evidenced.

Describe in Section 3.2.2 whether the entity implemented separate environments for development, testing and production, which is essential to prevent unauthorized or untested changes to IT applications, databases and operating systems from affecting the live financial data supporting the financial statements. These separate environments may be physically separated (i.e., different servers or network segments) or logically separated in virtual server environments.

Typically, an engagement team would expect to find within most entities at least the following three separate environments :

DEVELOPMENT
Environment in which changes to software code are developed (if the entity does development).

TESTING
The test environment allows either automated tests or human testers to check the changed code.

PRODUCTION
Also known as 'live'; this is the environment in which end users directly interact with the business applications and data, enter and process financial transactions, and generate IPE and other reports.

Complete Section 3.2.3 if the entity changed code or reports due to regulatory or accounting changes. For example, IFRS 9 on financial instruments required many entities to change the code, parameters and definition of new reports.

Complete Section 3.2.4 if the entity had implemented a new application relevant to financial reporting (which should have been identified in Section 1.5). Describe the project phases and its current status, the date the entity started to use the new application and the data migration process.

SECTION 3.3 - IT OPERATIONS (DATA PROCESSING)

If it was identified in Section 2 that the entity relies on automated or semi-automated data transfer between its applications, complete this section. While Section 2 described the nature of the interfaces and the financial data being transferred, in the current section describe how financial data is managed and processed by the IT department (e.g., accuracy and completeness reports, error-handling controls and segregation of duties).

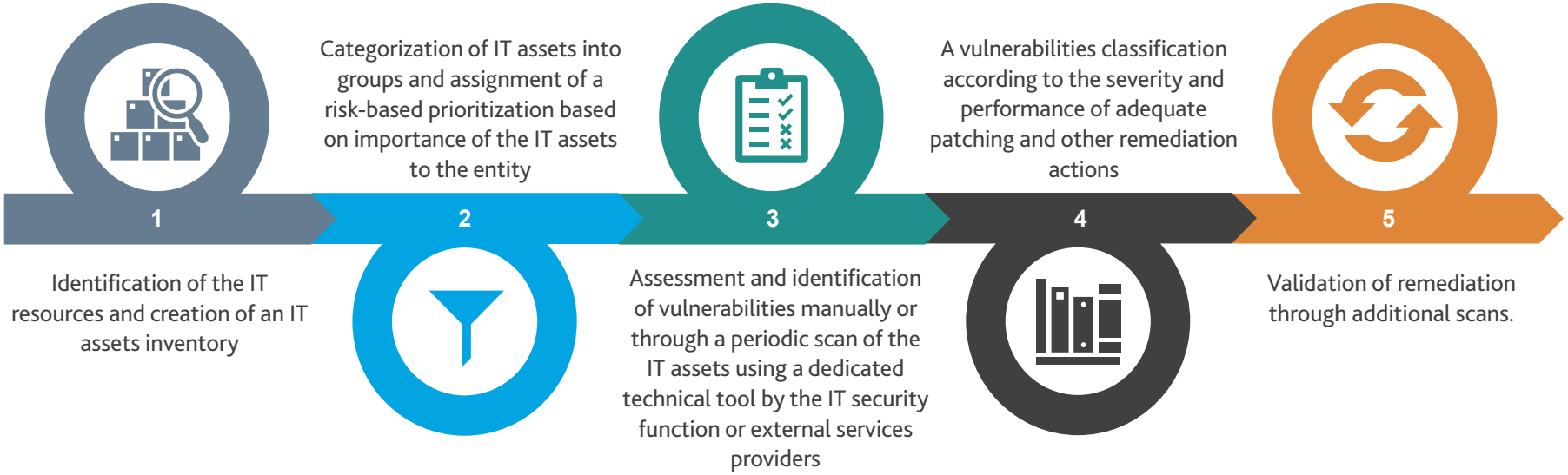
SECTION 3.4 - OTHER RELEVANT IT PROCESSES

Document in this section other IT processes considered relevant to financial reporting or to the entity's IT environment. While we may not have previously documented details related to data backup, IT continuity and physical security around data centers in the past, these areas are specifically mentioned as relevant according to the revised ISA 315. Other additional processes and controls that are relevant to the entity may be added as well.

Note that in Sections 3.4.1 and 3.4.2, when the entity is using a cloud-based infrastructure, the physical security controls and data backup process are outsourced to the cloud service provider.

SECTION 3.5 - SECURITY EVENTS AND PROCESSES

This section describes the security vulnerability management process, which is a process to identify existing technical vulnerabilities in applications, operating systems, databases and networks which can be used by adversaries to exploit the entity's IT resources. A common process includes:



If cyber-attacks or cyber incidents occurred during the audited period, complete Section 3.5.2. Describe the root cause and impact of the attack/incident. If the entity was not subject to a cyber-attack / incident during the audit period, choose 'No' from the drop-down menu in the 'applicable?' column.

If security events have occurred during the period under audit, a potential IRMM should be added and an appropriate response planned as such security events can significantly impact the nature, timing and extent of audit procedures. It is important that we have the information and knowledge necessary to properly evaluate the impact of the security event; therefore, an IS Audit Specialist may need to be consulted to determine the extent of involvement required.

5.

Conclusion

Obtaining the information requested in the Understanding Your IT Environment template is critical to fully understand the information systems, how they are being utilized by the entity and the risks arising from the use of IT. Through this understanding we are able to identify potential risks of material misstatement and plan specific procedures to address the risks.

The Understanding Your IT Environment template is a key source of information when the engagement team completes the ITGC Risk Assessment Questionnaire in APT Next Gen, and in particular, the ITGC section. The ITGCs identified in that questionnaire are the controls that address the common risks arising from the use of IT. The engagement team evaluates the design and implementation of relevant ITGCs, which provides useful information for determining the nature of the response to the IT risks identified.

CONTACT US:

AUDIT@BDO.GLOBAL

How to Guide is issued by the Global Assurance Department and distributed to the International A&A Coordinators. Please share this publication with relevant partners and staff in your firms.

BDO internal use only.

BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent firms ('the BDO network'), and their related entities.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BV and the firms is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the firms of the BDO network. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO firms.