Control Objective		
CO No	**Control Objective Description**	**CA No**
1.1	IT Strategic Planning. The organization should have an effective Information Technology governance structure to oversee information technology.	1.1.1
1.1	IT Strategic Planning. The organization should have an effective Information Technology governance structure to oversee information technology.	1.1.2
1.2	IT Policies. The organization should have appropriate and relevant policies, procedures, and standards.	1.2.1

1.2	IT Policies. The organization should have appropriate and relevant policies, procedures, and standards.	1.2.2
1.3	IT Organization and Relationships. The organization should have appropriate and clearly understood IT roles and responsibilities.	1.3.1

1.3	IT Organization and Relationships. The organization should have appropriate and clearly understood IT roles and responsibilities.	1.3.2
1.4	Educate and Train Users. The organization should educate and train users on IT policies and procedures.	1.4.1

1.4	Educate and Train Users. The organization should educate and train users on IT policies and procedures.	1.4.2
1.5	Policy Compliance. The organization should have effective and adhered to policies, procedures, and standards.	1.5.1
2.1	Assessment of Risks. The organization should have an integrated business and IT risk assessment framework to assess and manage information risk to achieve overall business objectives.	2.1.1
2.1	Assessment of Risks. The organization should have an integrated business and IT risk assessment framework to assess and manage information risk to achieve overall business objectives.	2.1.2

3.1	Access Controls. The organization should have effective systems to ensure that access to the entity's information assets is appropriate for each individual's role and job function.	3.1.1
3.1	Access Controls. The organization should have effective systems to ensure that access to the entity's information assets is appropriate for each individual's role and job function.	3.1.2
3.1	Access Controls. The organization should have effective systems to ensure that access to the entity's information assets is appropriate for each individual's role and job function.	3.1.3
3.1	Access Controls. The organization should have effective systems to ensure that access to the entity's information assets is appropriate for each individual's role and job function.	3.1.4

3.1	Access Controls. The organization should have effective systems to ensure that access to the entity's information assets is appropriate for each individual's role and job function.	3.1.5
3.2	Physical Security. The organization should have effective physical security controls in line with business requirements.	3.2.1
3.2	Physical Security. The organization should have effective physical security controls in line with business requirements.	3.2.2
3.2	Physical Security. The organization should have effective physical security controls in line with business requirements.	3.2.3

3.3	Environmental Security. The organization should have effective protection measures against environmental factors.	3.3.1
3.3	Environmental Security. The organization should have effective protection measures against environmental factors.	3.3.2
3.3	Environmental Security. The organization should have effective protection measures against environmental factors.	3.3.3
3.3	Environmental Security. The organization should have effective protection measures against environmental factors.	3.3.4

3.3	Environmental Security. The organization should have effective protection measures against environmental factors.	3.3.5
3.4	Network Security. The organization should have effective appropriate network security systems that would reasonably prevent unauthorized access to the entity's information assets.	3.4.1
3.4	Network Security. The organization should have effective appropriate network security systems that would reasonably prevent unauthorized access to the entity's information assets.	3.4.2
3.4	Network Security. The organization should have effective appropriate network security systems that would reasonably prevent unauthorized access to the entity's information assets.	3.4.3
3.4	Network Security. The organization should have effective appropriate network security systems that would reasonably prevent unauthorized access to the entity's information assets.	3.4.4

3.5	Anti Virus and Malware protection. The organization should have appropriate systems to prevent against viruses and other malware (e.g. trojans, spyware)	3.5.1
3.5	Anti Virus and Malware protection. The organization should have appropriate systems to prevent against viruses and other malware (e.g. trojans, spyware)	3.5.2
3.5	Anti Virus and Malware protection. The organization should have appropriate systems to prevent against viruses and other malware (e.g. trojans, spyware)	3.5.3
3.6	Maintain and Manage the Configuration. The organization should have systems to manage and maintain infrastructure configuration information.	3.6.1

3.6	Maintain and Manage the Configuration. The organization should have systems to manage and maintain infrastructure configuration information.	3.6.2
3.6	Maintain and Manage the Configuration. The organization should have systems to manage and maintain infrastructure configuration information.	3.6.3
3.6	Maintain and Manage the Configuration. The organization should have systems to manage and maintain infrastructure configuration information.	3.6.4

3.7	Authentication. The organization should be able to authenticate users and be able to trace actions to a single user.	3.7.1
3.7	Authentication. The organization should be able to authenticate users and be able to trace actions to a single user.	3.7.2

4.1	Change Management. The organization should manage all changes to systems & applications throughout the entire lifecycle of the change.	4.1.1
4.1	Change Management. The organization should manage all changes to systems & applications throughout the entire lifecycle of the change.	4.1.2
4.1	Change Management. The organization should manage all changes to systems & applications throughout the entire lifecycle of the change.	4.1.3

4.1	Change Management. The organization should manage all changes to systems & applications throughout the entire lifecycle of the change.	4.1.4
4.2	Approval of Changes. The organization should ensure that all changes are properly approved.	4.2.1
4.2	Approval of Changes. The organization should ensure that all changes are properly approved.	4.2.2
4.2	Approval of Changes. The organization should ensure that all changes are properly approved.	4.2.3
4.3	Change Testing. The organization should ensure that all changes are properly tested.	4.3.1

4.3	Change Testing. The organization should ensure that all changes are properly tested.	4.3.2
4.4	Emergency Changes. The organization should ensure that all emergency changes are appropriate.	4.4.1
5.1	Project Development. The organization should ensure that all projects are properly developed and meet expectations.	5.1.1
5.1	Project Development. The organization should ensure that all projects are properly developed and meet expectations.	5.1.2
5.2	Post-Implementation Review. The organization should ensure that a PIR is performed.	5.2.1

6.1	Problem and Incident Management. The organization should ensure that problem and incident management processes properly identify, record, analyze, resolve, and report problems and incidents.	6.1.1
6.1	Problem and Incident Management. The organization should ensure that problem and incident management processes properly identify, record, analyze, resolve, and report problems and incidents.	6.1.2

7.1	DRP. The IT group should ensure there is an effective DRP.	7.1.1
7.1	DRP. The IT group should ensure there is an effective DRP.	7.1.2
7.1	DRP. The IT group should ensure there is an effective DRP.	7.1.3

7.1	DRP. The IT group should ensure there is an effective DRP.	7.1.4
7.2	Back-Up and Restoration. The organization should ensure that there is appropriate back-up and restoration capabilities.	7.2.1
7.3	Back-Up Media. The organization should ensure that back-up media is protected.	7.3.1
7.3	Back-Up Media. The organization should ensure that back-up media is protected.	7.3.2
7.3	Back-Up Media. The organization should ensure that back-up media is protected.	7.3.3

8.1	Outsourced Service Providers. The organization should ensure that there are adequate controls over outsourced service providers.	8.1.1
8.1	Outsourced Service Providers. The organization should ensure that there are adequate controls over outsourced service providers.	8.1.2
8.1	Outsourced Service Providers. The organization should ensure that there are adequate controls over outsourced service providers.	8.1.3
8.1	Outsourced Service Providers. The organization should ensure that there are adequate controls over outsourced service providers.	8.1.4

8.1	Outsourced Service Providers. The organization should ensure that there are adequate controls over outsourced service providers.	8.1.5
9.1	End User Computing. The organization should ensure that EUC controls are appropriate.	9.1.1

Control Activity **OAG Suggested Control Activity**	
An IT steering committee (or equivalent) is composed of executive, business and IT management to: • Determine prioritization of IT-enabled investment programs in line with the enterprise's business strategy and priorities • Oversee/ Monitor status of projects and resolve resource conflict • Monitor service levels and service improvements.	
The organization has an IT strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks.	
The organization has developed and approved a comprehensive set of IT policies, procedures, and standards to support the IT strategy and to meet all local and international laws, regulations, and other governmental requirements that must be complied with. Policies (or supporting policies, procedures, and standards) should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines as appropriate. The organization has an effective control process to regularly review policies, procedures, and standards and ensure their relevance and changes are confirmed and approved by senior or executive management.	

The organization has developed and maintains an IT control framework that defines the organization's control processes to mitigate identified risks.	
The organization has a control process to ensure that In-Scope information assets (e.g. financial systems, key business systems, and security devices) are identified and inventoried. Data owners have been identified and ownership responsibilities have been allocated and agreed to for these systems and devices.	

IT management has implemented a division of roles and responsibilities (segregation of duties) or other mitigating controls that reasonably prevents a single individual from subverting a critical process.	
The organization has a control process to ensure that personnel are provided adequate orientation and training when hired and ongoing training to maintain their knowledge, skills, abilities, and awareness of internal controls and security.	

The organization has a documented and effective control process to ensure that all IT personnel understand and accept their responsibility regarding security and internal control.	
The organization has an effective classification scheme that applies throughout the enterprise, and is based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data.	
The organization has an integrated business and IT risk assessment framework that is used to identify and assess risks to the organization. The risk assessment framework is used to achieve overall business objectives.	
The organization has a documented and effective control process to identify and implement effective IT controls to mitigate identified risks or to document the acceptance of unmitigated or residual risks.	

The organization has documented and effective control processes for requesting, establishing, issuing, suspending and promptly closing all user account access to all financial or in-scope applications and systems and supporting infrastructure. The control process or procedures must cover all user access including end user, IT, system, DBA, privileged access and procedures for authenticating transactions originating outside the organization.	
The organization has effective control processes to ensure that there are appropriate segregation of duties between requesting, approving, and granting access to systems and data.	
The organization has a documented and effective control process to periodically review and confirm all user and system account access rights. Includes access for end users, IT personnel, external users, administers, DBAs, system accounts, and “privileged users”.	
The organization has a documented and effective control processes to monitor and log security and access violations for all financial and business critical systems and databases. Access and security violations are reported to senior management as applicable.	

The organization has documented and effective procedures to ensure that application software and data storage systems are properly configured to provision user access based on the individual's demonstrated need to view, add, change or delete data.	
The organization has documented physical and environmental security standards for all areas that host in-scope financial or business critical systems or devices that support these systems. There is a process to ensure these standards are consistently met.	
The organization has a documented and effective control process to monitor all environmental and physical security controls. There is a documented and effective process to identify document and track through to resolution all physical and environmental alerts as applicable.	
The organization has documented and effective procedures to restrict physical access to areas hosting in-scope financial or business critical systems and the devices that support them. Access to these areas is authorized, reviewed, logged, and monitored.	

The organization has appropriate fire detection and suppression in all areas that host in-scope financial and business critical systems.	
The organization has appropriate temperature or air-conditioning controls and alarms in place for all areas hosting in-scope financial and business critical systems.	
The organization has appropriate humidity controls and alarms in place for all areas hosting in-scope financial and business critical systems.	
The organization has appropriate moisture controls and alarms in place for all areas hosting in-scope financial and business critical systems.	

The organization has appropriate UPS or back up power to support all financial and business critical systems based on system availability requirements. Back Up power systems are tested regularly.	
The organization has appropriate security technology (e.g., firewalls, security appliances, network segmentation, intrusion detection as appropriate) and documented and effective supporting management procedures to authorize and control access and information flows to and from networks and in-scope applications.	
The organization has documented and effective control processes to: - monitor and log security activity at the operating system, application, and database levels, - remediate security violations as per documented procedures and; - report security violations to senior management as appropriate.	
The organization has documented and effective procedures that ensure security devices and systems infrastructure, including firewalls, routers, switches, network operating systems, servers and other devices, is properly configured and prevents unauthorized access.	
The organization has documented and effective procedures for wireless infrastructure and wireless devices within the organization.	

The organization has documented and effective preventative, detective, and corrective Anti Virus procedures in place to protect information assets from malware. (e.g., viruses, worms, spyware, and spam).	
The Anti-Virus system is regularly updated automatically. All applicable or in-scope servers and computing devices receive automatic updates.	
Anti Virus software is configured so it cannot be removed or disabled from end user computing devices, and is monitored to ensure that Anti Virus software is operating and updated.	
The organization has documented and effective procedures to ensure that IT assets are documented. The organization monitors, records, and maintains changes to the configuration of all (or in-scope) IT assets.	

The organization has documented and effective procedures to monitor for and prevent unauthorized devices (including wireless) and software from entering the computing environment. There is a documented and effective process to identify and remove unauthorized devices and software or to bring them into compliance with all policies and standards.	
The organization has documented and effective procedures to ensure that all servers and devices hosting or supporting in-scope financial or business critical applications are built to documented standards and are properly tested prior to use in the production environment.	
The organization has a documented and effective “patch” or upgrade control process that ensures all servers and devices hosting or supporting in-scope financial or business critical applications are monitored and updated / patched as appropriate.	

The organization has documented and effective procedures to authenticate all users, both internal and external, of the organization's systems. (E.g. unique user IDs, strong passwords, and account lockouts) These procedures meet or exceed best practices for identity and authentication standards (e.g. NIST) as applicable.	
If the organization uses a VPN or other remote access system, there is a documented and effective control process to ensure that the remote access system is properly configured so that only authorized users can access the organization’s information assets and that access is adequately secured.	

The organization has documented and effective change management procedures to assess and implement all requests for changes in a structured way. Control processes ensure that all change requests are standardized, logged, approved, documented, and subject to formal change management procedures.	
The organization has documented and effective procedures to update associated user documentation and procedures when changes are made where applicable.	
The organization has documented and effective procedures to establish an implementation and fallback/backout plan.	

The organization has documented and effective procedures to review changes after implementation to ensure that the changes are operating as expected.	
The organization has documented and effective procedures to obtain approval from relevant parties after applicable changes are tested and before changes can be migrated to production.	
The organization has documented and effective procedures to ensure there is a separation of duties among the initiators, approvers, developers, and implementers of changes as applicable.	
The organization has documented and effective procedures to ensure that only properly approved persons make or migrate changes to the production environment.	
The organization has established a secure and separate test environment that is representative of the planned production environment. The organization's development and test system's data is either scrambled or has requisite security over sensitive data.	

The organization has documented and effective procedures to ensure that changes were tested in accordance with a defined test plan prior to migration to the production environment. Testing should be conducted independently and should consider security and performance as applicable.	
The organization has documented and effective controls to ensure that “emergency changes” are properly documented and reviewed for compliance with all change management requirements after being implemented.	
The organization has a documented and effective procedure to determine what projects or significant changes must follow a/the SDLC or PDM.	
The organization has a documented and effective System Development Life Cycle (SDLC) or Project Development Methodology (PDM) for implementing new systems or making “significant” changes to the organization’s existing systems.	
The organization has a documented and effective process to conduct a Post Implementation Review (PIR) or a “lessons learned” follow up on all projects or significant changes. This review should ensure that all projects or changes met the original goals or objectives, and that controls in the system are working as applicable.	

The organization has documented and effective incident and problem management procedures. These procedures may include but are not limited to: • document and classify incidents or problems that have been identified. • ensure integrity and access control incidents are recorded and reported to management • escalate incidents that cannot be resolved immediately • ensure that incidents are resolved and the resolution meets expectations.	
IT management has a documented and effective process to obtain and review service desk activity reports to measure service performance and response times to identify trends or recurring problems, so service can be continually improved.	

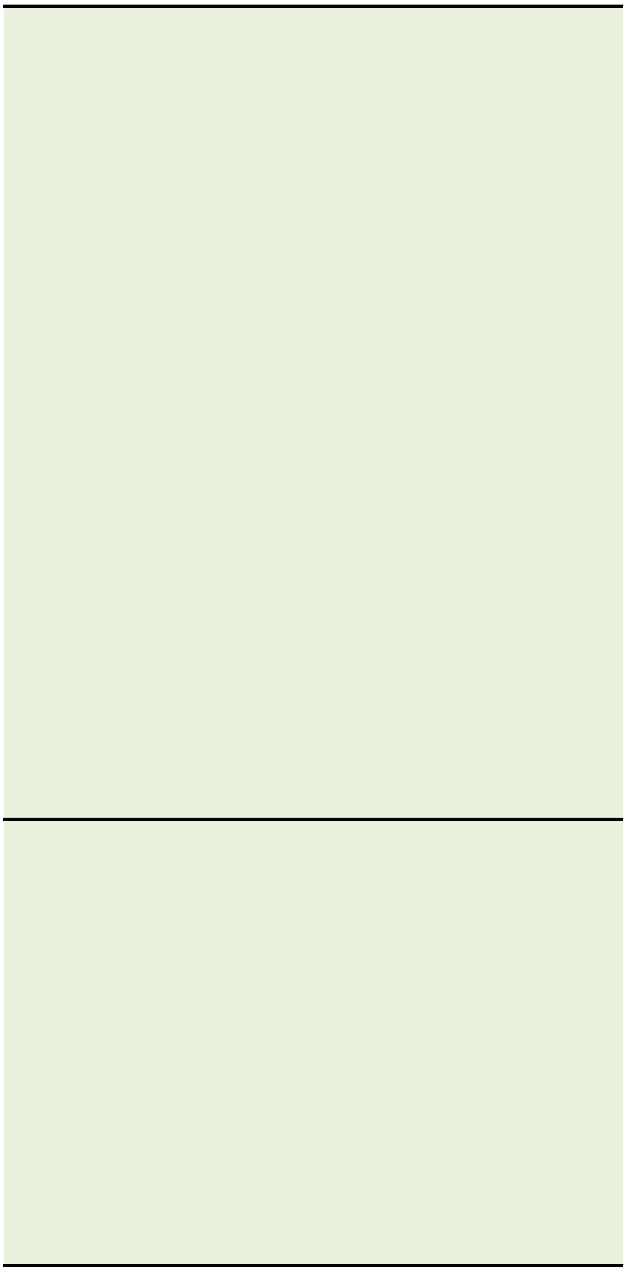
The organization has a documented IT Continuity or Disaster Recovery Plan (DRP) designed to reduce the impact of a major disruption on key business functions and processes. The DRP supports the organization's overall BCP.	
The IT continuity or disaster recovery plans (DRP) should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. The DRP should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach	
The organization has documented and effective plans to regularly test the DRP (IT continuity plan).	

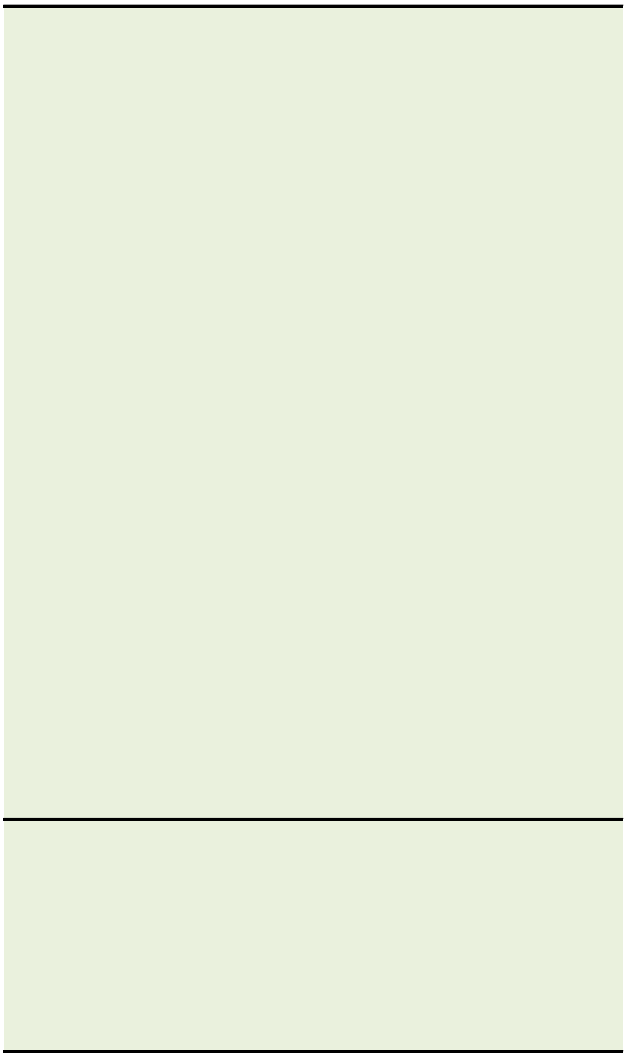
The organization has documented and effective procedures to assess the adequacy of the DRP after testing or use, and updates and communicates the changes as appropriate.	
The organization has documented and effective procedures for the backup and restoration of systems, applications, data and documentation for in-scope systems that are in line with business requirements and the continuity plan.	
The organization has documented and effective procedures to ensure that backup media for all in-scope financial and business critical systems is tested regularly to support business recovery objectives. * May be accomplished through DRP testing.	
The organization has documented and effective procedures that restrict access to back up media, including when in transit between onsite and off site locations to only authorized personnel.	
The organization has documented and effective plans to store all critical backup media, documentation, and other IT resources necessary for IT recovery and business continuity plans at an offsite location as applicable. The offsite location (if used) is assessed, at least annually, for content, environmental controls, and security.	

The organization has documented and effective procedures for establishing, modifying and terminating contracts for all outsourced service providers and vendors.	
The organization has a documented and effective process to ensure that all outsourced service providers are properly qualified and capable of providing the services prior to entering into a contract with them.	
The organization has a documented and effective process to monitor and report on the achievement of agreed upon Service Level Agreements, security, or other contractual obligations. There is a process to log and remediate issues or escalate as appropriate	
The organization has documented and effective control processes to ensure that contracts between the organization and outsourced service providers that addresses risk and security controls and procedures for all data, information systems, and networks in the contract.	

If an outsourced service provider hosts, or could have physical, logical, or administrative control of the organization's financial or critical business systems, then the contract should allow the organization to gain assurance over the outsourced service providers compliance to IT controls. This could be achieved in several ways including the organization auditing the service provider, or the service provider giving the organization a Service Auditor Report (i.e. SAS 70 II, Section 5970) or a SysTrust report.	
End User Computing (EUC) policies and procedures, concerning security, availability, and processing integrity are documented and are followed.	

Auditee Control Activity Owner / Description





Suggested Mappir
COBIT
PO4.3 IT Steering Committee Establish an IT steering committee (or equivalent) composed of executive, business and IT management to: • Determine prioritization of IT-enabled investment programs in line with the enterprise's business strategy and priorities • Track status of projects and resolve resource conflict • Monitor service levels and service improvements
PO1.2 Business-IT Alignment Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration. Mediate between business and IT imperatives so priorities can be mutually agreed. PO1.4 IT Strategic Plan Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programs, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.
ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organization's IT policies, standards, procedures and methodologies.

PO6.2 Enterprise IT Risk and Control Framework
Develop and maintain a framework that defines the enterprise's overall approach to IT risk and control and that aligns with the IT policy and control environment and the enterprise risk and control framework.

PO4.9 Data and System Ownership
Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information
systems. Owners should make decisions about classifying information and systems and protecting them in line with this
classification.
DS9.1 Configuration Repository and Baseline
Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record
all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.
This is a configuration item and we should have it somewhere.

PO4.6 Establishment of Roles and Responsibilities
Establish and communicate roles and responsibilities for IT personnel and end users that delineate between IT personnel and end-user authority, responsibilities and accountability for meeting the organization's needs.
PO4.11 Segregation of Duties Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorized duties

PO7.4 Personnel Training
Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities,
internal controls and security awareness at the level required to achieve organizational goals.

DS7.1 Identification of Education and Training Needs
Establish and regularly update a curriculum for each target group of employees considering:
• Current and future business needs and strategy
• Value of information as an asset
• Corporate values (ethical values, control and security culture, etc.)
• Implementation of new IT infrastructure and software (i.e., packages, applications)
• Current and future skills, competence profiles, and certification and/or credentialing needs as well as required re-accreditation
• Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing.

PO4.6 Establishment of Roles and Responsibilities
Establish and communicate roles and responsibilities for IT personnel and end users that delineate between IT personnel and
end-user authority, responsibilities and accountability for meeting the organization's needs.

PO6.1 IT Policy and Control Environment
Define the elements of a control environment for IT, aligned with the enterprise's management philosophy and operating style.
These elements should include expectations/requirements regarding delivery of value from IT investments, appetite for risk,
integrity, ethical values, staff competence, accountability and responsibility.
The control environment should be based on a culture that supports value delivery whilst managing significant risks, encourages cross-divisional co-operation and teamwork, promotes compliance and continuous process improvement, and handles process deviations (including failure) well.

PO6.3 IT Policies Management
Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.

ME3.2 Optimization of Response to External Requirements
Review and adjust IT policies, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.
ME3.3 Evaluation of Compliance With External Requirements
Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements

PO9.5 Risk Response
Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.

DS5.4 User Account Management Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.
PO4.11 Segregation of Duties Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorized duties relevant to their respective jobs and positions.
DS5.4 User Account Management Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.
N/A

DS5.4 User Account Management Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.
DS5.2 IT Security Plan Translate business information requirements, IT configuration, information risk action plans and information security culture into an overall IT security plan. The plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Security policies and procedures are communicated to stakeholders and users.
N/A
DS12.3 Physical Access Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.

DS12.2 Physical Security Measures
Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.
DS12.4 Protection Against Environmental Factors
Design and implement measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.

DS12.2 Physical Security Measures
Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating

DS12.2 Physical Security Measures
Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.
DS12.4 Protection Against Environmental Factors
Design and implement measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.

DS12.2 Physical Security Measures
Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.
DS12.4 Protection Against Environmental Factors
Design and implement measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.

DS12.2 Physical Security Measures Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives. DS12.4 Protection Against Environmental Factors Design and implement measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment. DS12.5 Physical Facilities Management Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.
DS5.10 Network Security Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.
DS5.5 Security Testing, Surveillance and Monitoring Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.
DS5.7 Protection of Security Technology Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.
DS5.7 Protection of Security Technology Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily. DS5.10 Network Security Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks

DS5.9 Malicious Software Prevention, Detection and Correction Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).
DS5.9 Malicious Software Prevention, Detection and Correction Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).
DS5.9 Malicious Software Prevention, Detection and Correction Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).
DS9.1 Configuration Repository and Baseline Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.

DS9.3 Configuration Integrity Review
Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.

DS5.7 Protection of Security Technology
Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.

DS5.9 Malicious Software Prevention, Detection and Correction
Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

DS5.10 Network Security
Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.

AI3.2 Infrastructure Resource Protection and Availability
Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated

AI3.3 Infrastructure Maintenance
Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organization's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment, and security requirements.

AI6.1 Change Standards and Procedures
Set up formal change management procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes,

DS5.3 Identity Management
Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement Authentication and enforce access rights.

DS5.4 User Account Management
Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be

DS5.11 Exchange of Sensitive Data
Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, and proof of receipt and non-repudiation of origin.

AI6.1 Change Standards and Procedures
Set up formal change management procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.2 Impact Assessment, Prioritization and Authorization
Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorized, prioritized and authorized.

AI6.5 Change Closure and Documentation
Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.

AI7.3 Implementation Plan
Establish an implementation and fallback/backout plan. Obtain approval from relevant parties.

AI7.8 Promotion to Production
Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in
parallel with the old system for a while, and compare behavior and results.

AI7.9 Post-implementation Review - Changes
Establish procedures in line with the organizational change management standards to require a post-implementation review as set out in the implementation plan.

AI7.3 Implementation Plan
Establish an implementation and fallback/backout plan. Obtain approval from relevant parties.

AI7.8 Promotion to Production
Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in
parallel with the old system for a while, and compare behavior and results.

AI7.8 Promotion to Production
Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in
parallel with the old system for a while, and compare behavior and results.

AI7.8 Promotion to Production
Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in
parallel with the old system for a while, and compare behavior and results.

AI7.4 Test Environment
Define and establish a secure test environment representative of the planned operations environment relative to security, internal controls, operational practices, data quality and privacy requirements, and workloads.

AI7.6 Testing of Changes Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.
AI6.3 Emergency Changes Establish a process for defining, raising, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process.
Although there is no direct mapping to this control in COBIT I inserted this to cut down on the prescriptivness of all of the requirements in AI for implementing new systems or significant changes to existing systems. We will assess the Auditee's process to determine what is a project and what must follow the PDM and then test those projects that must follow the PDM.
PO8.3 Development and Acquisition Standards Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.
AI7.9 Post-implementation Review – projects Establish procedures in line with the organizational change management standards to require a post-implementation review as set out in the implementation plan.

DS10.1 Identification and Classification of Problems
Implement processes to report and classify problems that have been identified as part of incident management. The steps involved in problem classification are similar to the steps in classifying incidents; they are to determine category, impact, urgency and priority. Categorize problems as appropriate into related groups or domains (e.g., hardware, software, support software). These groups may match the organizational responsibilities of the user and customer base, and should be the basis for allocating problems to support staff.
DS8.3 Incident Escalation
Establish service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. Ensure that incident ownership and life cycle monitoring remain with the service desk for user-based incidents, regardless which IT group is working on resolution activities.
DS8.4 Incident Closure
Establish procedures for the timely monitoring of clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem

DS8.5 Reporting and Trend Analysis Produce reports of service desk activity to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved.

DS4.2 IT Continuity Plans
Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

DS4.2 IT Continuity Plans
Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

DS4.5 Testing of the IT Continuity Plan
Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.

DS4.4 Maintenance of the IT Continuity Plan
Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner.

DS4.7 Distribution of the IT Continuity Plan
Determine that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorized interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.

DS4.10 Post-resumption Review
Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly.

DS11.5 Backup and Restoration
Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.

DS11.5 Backup and Restoration
Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.

DS11.6 Security Requirements for Data Management
Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organization's security policy and regulatory requirements.

DS4.9 Offsite Backup Storage
Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans.
Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to

AI5.2 Supplier Contract Management
Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organizational, documentary, performance, security, intellectual property, and termination responsibilities
and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors.

AI5.3 Supplier Selection
Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimized with input from potential suppliers.

DS2.3 Supplier Risk Management
Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.

DS2.2 Supplier Relationship Management
Formalize the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).

DS2.4 Supplier Performance Monitoring
Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.

DS2.3 Supplier Risk Management
Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.

ME2.6 Internal Control at Third Parties Assess the status of external service providers' internal controls. Confirm that external service providers comply with legal and regulatory requirements and contractual obligations.
The following illustrative controls for end-user computing have been extracted from the control guidance in figures 15 to 26 and are presented to address the characteristics of a typical end-user computing environment. Appropriate COBIT processes apply to this environment.

ng	
ITGI	**Sugguested Documentation (note: do not rely entirely on this column it is simply a list of suggested documents)**
An IT steering committee is not required by the ITGI ICFR guidelines. However, there are numerous references to such throughout the document.	IT Steering Committee: -Charter/Terms of Reference. -Meeting minutes for the fiscal year
Aligns to ITGI Fig. 11 Section 1.1. Has management prepared strategic plans for IT that aligns business objectives with IT strategies? Does the planning approach include mechanisms to solicit input from relevant internal and external stakeholders affected by the IT strategic plans?	IT Strategic plan and Business Plan -w/Evidence of IT goals matching business goals (some ministries track this through a spreadsheet to show the alignment between IT and business) OAG can also check the documents.
N/A	All IT related policies: eg. Password policy, security policy, antivirus policy, chanage management policy, project management policy, outsourcing policy, data classification, etc.

This does not map directly to an ITGI requirement. However the ITGI has numerous references to the need for an IT control framework. Preferably one that maps to COSO like COBIT.	Documentation of Control framework used (note a risk assessment must also be supplied in order for this to be considered effective)
Aligns with ITGI Fig 11 Sections 6. Have relevant systems and data been inventoried and their owners identified? 9. Have data integrity ownership and responsibilities been communicated to appropriate data/business owners and have they accepted these responsibilities?	Evidence of Critical assets and ownership documented, approved and responsibilities allocated for example: The Application Inventory The Hardware Inventory DRP application listing BCP application listings

Aligns with ITGI Fig 11 Sections 7. Are roles and responsibilities of the IT organization defined, documented and understood? 10. Has IT management implemented a division of roles and responsibilities (segregation of duties) that reasonably prevents a single individual from subverting a	IT Organization chart. -Evidence of segregation of duties within IT teams. Something that shows the different areas within IT.
Aligns with ITGI Fig 11 Sections 8. Do IT personnel understand and accept their responsibility regarding internal control? 12. Does IT management provide education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards and security responsibilities of all staff?	Security awareness training -program/process -Evidence of the SA training program and frequency -participation rates

N/A	-Security awareness training process and frequency for IT staff -Acceptable use policy and OAG will test a sample of users to make sure that they have signed their AUP.
Figure 22. ♦ An information security policy exists and has been approved by an appropriate level of executive management.	-practices relating to labeling, storing, and transmitting information assets that have been classified as well as practices related to ensuring appropriate access to information and protecting the integrity of information.
Standards to reflect changing business conditions. The organization has policies and procedures regarding program development, program change, access programs and data, and computer operations, which are periodically reviewed, updated and approved by management. 14. Does IT management have a process in place to assess compliance with its policies, procedures and standards?	The IT Risk Management Framework • Update schedule for the IT Risk Management Framework • Listing of evaluated threat consequences and probabilities • Risk mitigation strategies from BCP and DRP
18. Where risks are considered acceptable, is there formal documentation and acceptance of residual risk with related offsets, including adequate insurance coverage, contractually negotiated liabilities and self-insurance? Where risks have not been accepted, does management have an action plan to implement risk	Risk mitigation action plan

Figure 22. ♦ Procedures exist and are followed relating to timely action for requesting, establishing, issuing, suspending and closing user accounts. (Include procedures for authenticating transactions originating outside the organization.) Figure 22. ♦ Procedures exist and are followed to authenticate all users of the system (both internal and external) to support the existence of transactions.	-User Access Control policy and procedures -list of all network/active directory users -list of new hires and terminations from HR
Figure 22. ♦ Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.	-Staff added/deleted/changed roles for fiscal year (from HR) -Systems Access Request forms or email approvals for adding new users or deleting current ones.
Figure 22. ♦ A control process exists and is followed to periodically review and confirm access rights.	-Policy/process to review user access periodically, including IT staff -Evidence of this occuring. Screenshot, signoffs.
Figure 22. ♦ IT security administration monitors and logs security activity at the operating system, application, and database levels the application and security violations are reported to senior management.	-Documented and approved process for log monitoring and review. -Security and access violation logs for me to review to see if anything significant was missed/not followed up on.

Figure 23 ♦Application software and data storage systems are properly configured to provision access based on the individual's demonstrated need to view, add, change or delete data.	-Policy/process to review user access periodically, including IT staff -Evidence of this occuring. Screenshot, signoffs.
Figure 22 A framework of security standards has been developed that supports the objectives of the security policy. • Physical and environmental security	Server room/Data center physical and environmental controls policy or standard
Figure 22. ♦ IT security administration monitors and logs security activity at the operating system, application, and database levels the application and security violations are reported to senior management.	Alert management process for the data center -Data center related incident reports or tickets.
Figure 22 Access to facilities is restricted to authorized personnel and requires appropriate identification authentication.	Physical access control process to grant, revoke and review access. Process to review unauthorized access.

N/A	OAG to testing during the Data Center Inspection. Fire alarm monitoring agreement or SLA with alarm company
N/A	OAG to testing during the Data Center Inspection.
N/A	OAG to testing during the Data Center Inspection.
N/A	OAG to testing during the Data Center Inspection.

N/A	OAG to testing during the Data Center Inspection.
Figure 22 Appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access via public networks.	-Network topology diagram -firewall configuration or log (to verify existence of the firewall) -other evidence of IDS/IPS or VLans
Figure 22. ♦ IT security administration monitors and logs security activity at the operating system, application, and database levels and identified security violations are reported to senior management.	Log monitoring policy and process
Figure 23 System infrastructure, including firewalls, routers, switches, network operating systems, servers and other devices, is properly configured to prevent unauthorized access.	Process for configuring devices process for testing configurations for vulnerabilities.
Figure 23 System infrastructure, including firewalls, routers, switches, network operating systems, servers and other devices, is properly configured to prevent unauthorized access.	-Wireless access policy (may be integrated in the security policy) Procedures to managing wireless: -Eg. What do you do if you find a rogue wireless access point?

Figure 23 IT management has established procedures across the organization to protect information systems and technology from computer viruses.	-Anti Virus standards/procedures -Screenshots of AV server settings. -Eg. Trend - Main control panel showing that AV is enabled on all networked computers.
Figure 23 IT management has established procedures across the organization to protect information systems and technology from computer viruses	-Anti Virus update status and monitoring process -Screenshots demonstrating that AV is up to date. Eg. Trend - Main control panel showing which computers have the current AV signatures.
Figure 23 IT management has established procedures across the organization to protect information systems and technology from computer viruses.	-AV configuration settings via screenshot showing that AV cannot be disabled. Should be on the Main control panel.
N/A	IT asset policy -application inventory -SMS inventory of software/PC -server inventory

N/A	Process for monitoring for unauthorized devices or software eg. via SMS
Figure 17 ♦The organization develops, maintains operates its systems and applications in accordance with its supported, documented policies and procedures.	Process for configuring devices Evidence that the devices/servers are built to documented standards. (screenshots of settings)
Figure 17 ♦The organization develops, maintains operates its systems and applications in accordance with its supported, documented policies and procedures	Patch management process OAG to review batch file results to assess patches applied compared to best practices.

Figure 22. ♦ Procedures exist and are followed to authenticate all users of the system (both internal and external) to support the existence of transactions. Figure 22. ♦ Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes).	-Security policy or password standards document. -screenshot of this from cmd prompt: net accounts /domain password /more (for unix) or active directory showing what the implemented password settings are.
Figure 22 Where appropriate, controls exist so that neither party can deny transactions, and controls are implemented to provide nonrepudiation of origin or receipt, proof of submission, and receipt of transactions. Figure 22 Appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access via public networks.	-remote access policy (likely from security policy) -list of remote users and remote website -evidence of VPN in use and the server side settings for it.

Figure 17 ♦ The organization has policies and procedures regarding program development, program change, access to programs and data, and computer operations, which are periodically reviewed, updated and approved by management. Figure 19 ♦ Requests for program changes, system changes, and maintenance (including changes to system software) are standardized, logged, approved, documented, and subject to formal change management procedures. AI6.1, AI6.2, AI6.5, AI7.3, AI7.8, AI7.8, AI7.9, AI7.10, AI7.11	Change management policy and procedures
Figure 19 ♦ Requests for program changes, system changes, and maintenance (including changes to system software) are standardized, logged, approved, documented, and subject to formal change management procedures. AI6.1, AI6.2, AI6.4, AI6.5, AI7.3, AI7.8, AI7.8, AI7.9, AI7.10, AI7.11	-List of ALL application changes (NO infrastructure changes) for the fiscal year. -OAG will then select samples of changes to test from the listing
Figure 19 ♦ Requests for program changes, system changes, and maintenance (including changes to system software) are standardized, logged, approved, documented, and subject to formal change management procedures. AI6.1, AI6.2, AI6.4, AI6.5, AI7.3, AI7.8, AI7.9, AI7.10, AI7.11	see 4.1.2

Figure 19 ♦ Requests for program changes, system changes, and maintenance (including changes to system software) are standardized, logged, approved, documented, and subject to formal change management procedures. AI6.1, AI6.2, AI6.4, AI6.5, AI7.3, AI7.8, AI7.9, AI7.10, AI7.11	see 4.1.2
Figure 19 ♦ Requests for program changes, system changes, and maintenance (including changes to system software) are standardized, logged, approved, documented, and subject to formal change management procedures. AI6.1, AI6.2, AI6.4, AI6.5, AI7.3, AI7.8, AI7.9, AI7.10, AI7.11	see 4.1.2
Figure 19 ♦ Controls are in place to restrict migration of programs to production by authorized individuals only.	see 4.1.2
Figure 19 ♦ Controls are in place to restrict migration of programs to production by authorized individuals only.	access control list for different environments or mitigating controls
N/A	This will be tested via the Server room inspection, network topology diagram and inquiries with application development, change management staff.

N/A	OAG to review sampled items.
Figure 19 ♦ Emergency change requests are documented and subject to formal and change management procedures.	emergency change management procedures/policy list of all emergency changes
N/A	-Process to indicate what projects require a Project management methodology
Figure 15 ♦ The organization has a system development life cycle (SDLC) methodology, which includes security and processing integrity requirements of the organization.	List of all projects initiated AND completed during the fiscal year
Post implementation reviews are performed to verify that controls are operating effectively.	OAG to select project charters to see if they have a PIR.

Figure 24 ♦ IT management has defined and implemented an incident and problem management system such that data integrity and access control incidents are recorded, analyzed, resolved in a timely manner and reported to management.	Standard incident management communication initiation procedure documentation Incident management communication procedure reviews
Figure 24♦ IT management has defined and implemented an incident and problem management system such that data integrity and access control incidents are recorded, analyzed, resolved in a timely manner and reported to management.	Service/help desk activity reports and evidence of management review (signoffs, emails, operations/tactical meeting minutes)

N/A	Documented DRP, BCP
N/A	Documented DRP, BCP
Business continuity and disaster recovery plans are not considered a part of ICFR. However – Figure 25 ♦ The restoration of information is periodically tested.	DRP data restoration procedures Logs/notes from last restoration during DRP testing

N/A	documented DRP test procedures and post DRP test assessment
Figure 25 ♦ Management has implemented a strategy for cyclical backup of data and programs.	documented backup and recovery procedures
Figure 25 ♦ The restoration of information is periodically tested	DRP test results (note: individual application recovery results will also be considered but it will not completely satisfy the control unless they are integrated to support business recovery objectives)
Management protects sensitive information—logically and physically, in storage and during transmission—against unauthorized access or modification.	Offsite tape transportation and storage procedures
N/A	Offsite tape transportation and storage procedures Courier logs/tickets that show that the tapes being transferred to the offsite location. SAS 70 Type II or Section 5970 report over the controls at the offsite location.

Figure 21. Selection of vendors for outsourced services is performed in accordance with the organization's vendor management policy.	documented procedures for entering into third party contracts.
Figure 21. IT management determines that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service and a review of their financial viability.	contract template, RFP template and an actual contract/RFP to see how it was implemented.
Figure 21. Procedures exist and are followed that include requirements that for third-party services a formal contract be defined and agreed to before work is performed initiated, including definition of internal control requirements and acceptance of the organization's policies and procedures.	contract template, RFP template and an actual contract/RFP to see how it was implemented. Performance metric monitoring documentation
Figure 21. Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	contract template, RFP template and an actual contract/RFP to see how it was implemented.

Figure 21. ♦ A regular review of security and processing integrity is performed by third-party service providers (e.g., SAS 70, Canadian 5970, and ISA 402).	see column on the left
Figure 27 ♦ End-user computing policies and procedures concerning security and processing integrity exist and are followed.	The financial audit team will inform ISA if this area needs to be tested or not. Is so: permission on folders, versioning on excel spreadsheets, etc.