Bazil Vink
Directorate: Financial Governance
Email: Bazil.Vink@westerncape.gov.za
Tel: +27 21 483 6646 Fax: +27 21 483 3707

Reference: T6/1/3/MRMF

TREASURY CIRCULAR MUN NO. 31/2014

THE MAYOR, CITY OF CAPE TOWN: MS P DE LILLE
THE MAYOR, WEST COAST DISTRICT MUNICIPALITY: MR JH CLEOPHAS
THE MAYOR, MATZIKAMA MUNICIPALITY: MR J BOTHA
THE MAYOR, CEDERBERG MUNICIPALITY: MS L SCHEEPERS
THE MAYOR, BERGRIVIER MUNICIPALITY: MR EB MANUEL
THE MAYOR, SALDANHA BAY MUNICIPALITY: MR F SCHIPPERS
THE MAYOR, SWARTLAND MUNICIPALITY: MR T VAN ESSEN
THE MAYOR, CAPE WINELANDS DISTRICT MUNICIPALITY: MR N DE BRUYN
THE MAYOR, WITZENBERG MUNICIPALITY: MR J KLAZEN
THE MAYOR, DRAKENSTEIN MUNICIPALITY: MS G VAN DEVENTER
THE MAYOR, STELLENBOSCH MUNICIPALITY: MR CJ SIDEGO
THE MAYOR, BREEDE VALLEY MUNICIPALITY: MS A STEYN
THE MAYOR, LANGEBERG MUNICIPALITY: MS D GAGIANO
THE MAYOR, OVERBERG DISTRICT MUNICIPALITY: MR L DE BRUYN
THE MAYOR, THEEWATERSKLOOF MUNICIPALITY: MR CB PUNT
THE MAYOR, OVERSTRAND MUNICIPALITY: MS N BOTHA-GUTHRIE
THE MAYOR, CAPE AGULHAS MUNICIPALITY: MR R MITCHELL
THE MAYOR, SWELLENDAM MUNICIPALITY: MR N MYBURGH
THE MAYOR, EDEN DISTRICT MUNICIPALITY: MR V VAN DER WESTHUIZEN
THE MAYOR, KANNALAND MUNICIPALITY: MR J DONSON
THE MAYOR, HESSEQUA MUNICIPALITY: MS E NEL
THE MAYOR, MOSSEL BAY MUNICIPALITY: MS M FERREIRA
THE MAYOR, GEORGE MUNICIPALITY: MR C STANDERS
THE MAYOR, OUDTSHOORN MUNICIPALITY: MR G APRIL
THE MAYOR, BITOU MUNICIPALITY: MR M BOOYSEN
THE MAYOR, KNYSNA MUNICIPALITY: MS J WOLMARANS
THE MAYOR, CENTRAL KAROO DISTRICT MUNICIPALITY: MR E NJADU
THE MAYOR, LAINGSBURG MUNICIPALITY: MR W THERON
THE MAYOR, PRINCE ALBERT MUNICIPALITY: MR G LOTTERING
THE MAYOR, BEAUFORT WEST MUNICIPALITY: MR HT PRINCE

THE MUNICIPAL MANAGER, CITY OF CAPE TOWN: MR A EBRAHIM
THE MUNICIPAL MANAGER, WEST COAST DISTRICT MUNICIPALITY: MR H PRINS
THE MUNICIPAL MANAGER, MATZIKAMA MUNICIPALITY: MR M BOLTON (ACTING)
THE MUNICIPAL MANAGER, CEDERBERG MUNICIPALITY: MR I KENNED
THE MUNICIPAL MANAGER, BERGRIVIER MUNICIPALITY: ADV H LINDE
THE MUNICIPAL MANAGER, SALDANHA BAY MUNICIPALITY: MR L SCHEEPERS
THE MUNICIPAL MANAGER, SWARTLAND MUNICIPALITY: MR J SCHOLTZ
THE MUNICIPAL MANAGER, CAPE WINELANDS DISTRICT MUNICIPALITY: MR M MGAJO
THE MUNICIPAL MANAGER, WITZENBERG MUNICIPALITY: MR D NASSON
THE MUNICIPAL MANAGER, DRAKENSTEIN MUNICIPALITY: MR J METTLER
THE MUNICIPAL MANAGER, STELLENBOSCH MUNICIPALITY: MS C LIEBENBERG
THE MUNICIPAL MANAGER, BREEDE VALLEY MUNICIPALITY: MR G MATTHYSE
THE MUNICIPAL MANAGER, LANGEBERG MUNICIPALITY: MR SA MOKWENI
THE MUNICIPAL MANAGER, OVERBERG DISTRICT MUNICIPALITY: MR D BERETTI (ACTING)
THE MUNICIPAL MANAGER, THEEWATERSKLOOF MUNICIPALITY: MR HSD WALLACE
THE MUNICIPAL MANAGER, OVERSTRAND MUNICIPALITY: MR C GROENEWALD
THE MUNICIPAL MANAGER, CAPE AGULHAS MUNICIPALITY: MR D O'NEILL
THE MUNICIPAL MANAGER, SWELLENDAM MUNICIPALITY: MR CM AFRICA
THE MUNICIPAL MANAGER, EDEN DISTRICT MUNICIPALITY: MR GW LOUW
THE MUNICIPAL MANAGER, KANNALAND MUNICIPALITY: MR M HOOGBAARD
THE MUNICIPAL MANAGER, HESSEQUA MUNICIPALITY: MR J JACOBS
THE MUNICIPAL MANAGER, MOSSEL BAY MUNICIPALITY: DR M GRATZ

THE MUNICIPAL MANAGER, GEORGE MUNICIPALITY: MR T BOTHA
THE MUNICIPAL MANAGER, OUDTSHOORN MUNICIPALITY: MR R LOTTERING (ACTING)
THE MUNICIPAL MANAGER, BITOU MUNICIPALITY: MR A PAULSE
THE MUNICIPAL MANAGER, KNYSNA MUNICIPALITY: MS L WARING
THE MUNICIPAL MANAGER, CENTRAL KAROO DISTRICT MUNICIPALITY: MR S JOOSTE
THE MUNICIPAL MANAGER, LAINGSBURG MUNICIPALITY: MR P WILLIAMS
THE MUNICIPAL MANAGER, PRINCE ALBERT MUNICIPALITY: MR H METTLER
THE MUNICIPAL MANAGER, BEAUFORT WEST MUNICIPALITY: MR J BOOYSEN

THE CHIEF FINANCIAL OFFICER, CITY OF CAPE TOWN: MR K JACOBY
THE CHIEF FINANCIAL OFFICER, WEST COAST DISTRICT MUNICIPALITY: MR J KOEKEMOER
THE CHIEF FINANCIAL OFFICER, MATZIKAMA MUNICIPALITY: MR M BOLTON
THE CHIEF FINANCIAL OFFICER, CEDERBERG MUNICIPALITY: MR E ALFRED
THE CHIEF FINANCIAL OFFICER, BERGRIVIER MUNICIPALITY: MR JA VAN NIEKERK
THE CHIEF FINANCIAL OFFICER, SALDANHA BAY MUNICIPALITY: MR S VORSTER
THE CHIEF FINANCIAL OFFICER, SWARTLAND MUNICIPALITY: MR K COOPER
THE CHIEF FINANCIAL OFFICER, CAPE WINELANDS DISTRICT MUNICIPALITY: MS FA DU RAAN-GROENEWALD
THE CHIEF FINANCIAL OFFICER, WITZENBERG MUNICIPALITY: MR C KRITZINGER
THE CHIEF FINANCIAL OFFICER, DRAKENSTEIN MUNICIPALITY: MR J CARSTENS
THE CHIEF FINANCIAL OFFICER, STELLENBOSCH MUNICIPALITY: MR M WÜST
THE CHIEF FINANCIAL OFFICER, BREEDE VALLEY MUNICIPALITY: MR D McTHOMAS
THE CHIEF FINANCIAL OFFICER, LANGEBERG MUNICIPALITY: MR CF HOFFMANN
THE CHIEF FINANCIAL OFFICER, OVERBERG DISTRICT MUNICIPALITY: MR J TESSELAAR
THE CHIEF FINANCIAL OFFICER, THEEWATERSKLOOF MUNICIPALITY: MR D LOUW
THE CHIEF FINANCIAL OFFICER, OVERSTRAND MUNICIPALITY: MS S REYNEKE-NAUDE
THE CHIEF FINANCIAL OFFICER, CAPE AGULHAS MUNICIPALITY: MR H VAN BILJON
THE CHIEF FINANCIAL OFFICER, SWELLENDAM MUNICIPALITY: MR H SCHLEBUSCH
THE CHIEF FINANCIAL OFFICER, EDEN DISTRICT MUNICIPALITY: MS L HOEK
THE CHIEF FINANCIAL OFFICER, KANNALAND MUNICIPALITY: MR N DELO
THE CHIEF FINANCIAL OFFICER, HESSEQUA MUNICIPALITY: MS HJ VILJOEN
THE CHIEF FINANCIAL OFFICER, MOSSEL BAY MUNICIPALITY: MR HF BOTHA
THE CHIEF FINANCIAL OFFICER, GEORGE MUNICIPALITY: MR K JORDAAN
THE CHIEF FINANCIAL OFFICER, OUDTSHOORN MUNICIPALITY: MR RF BUTLER (ACTING)
THE CHIEF FINANCIAL OFFICER, BITOU MUNICIPALITY: MR F LÖTTER
THE CHIEF FINANCIAL OFFICER, KNYSNA MUNICIPALITY: MR G EASTON
THE CHIEF FINANCIAL OFFICER, CENTRAL KAROO DISTRICT MUNICIPALITY: MR N NORTJE (ACTING)
THE CHIEF FINANCIAL OFFICER, LAINGSBURG MUNICIPALITY: MS A GROENEWALD
THE CHIEF FINANCIAL OFFICER, PRINCE ALBERT MUNICIPALITY: MR J NEETHLING
THE CHIEF FINANCIAL OFFICER, BEAUFORT WEST MUNICIPALITY: MR J BOOYSEN (ACTING)

THE HEAD OFFICIAL: PROVINCIAL TREASURY (DR JC STEGMANN)
THE HEAD: BRANCH FISCAL AND ECONOMIC SERVICES (MR H MALILA)
THE HEAD: BRANCH GOVERNANCE AND ASSET MANAGEMENT (MR Z HOOSAIN)
THE HEAD: PUBLIC POLICY SERVICES (MR H MALILA) (PRO TEM)
THE HEAD: PROVINCIAL GOVERNMENT PUBLIC FINANCE (MS JD GANTANA)
THE HEAD: LOCAL GOVERNMENT PULIC FINANCE (MR H MALILA) (PRO TEM)
THE HEAD: ASSET MANAGEMENT (MR IG SMITH)
THE HEAD: FINANCIAL GOVERNANCE AND ACCOUNTING (MR A HARDIEN)
THE CHIEF FINANCIAL OFFICER (MR A GILDENHUYS)
THE HEAD: OFFICE OF THE FINANCE MINISTRY (ADV E PRETORIUS)
THE SENIOR MANAGER: BUSINESS INFORMATION AND DATA MANAGEMENT (MR PP PIENAAR)
THE SENIOR MANAGER: FINANCIAL GOVERNANCE (MR B VINK)
THE SENIOR MANAGER: FISCAL POLICY (MR H MALILA) (PRO TEM)
THE SENIOR MANAGER: INFRASTRUCTURE (MS JD GANTANA) (PRO TEM)
THE SENIOR MANAGER: LOCAL GOVERNMENT ACCOUNTING (MS N OLIPHANT)
THE SENIOR MANAGER: LOCAL GOVERNMENT BUDGET OFFICE (MR ML BOOYSEN)
THE SENIOR MANAGER: LOCAL GOVERNMENT REVENUE AND EXPENDITURE (GROUP ONE) (MR F SABBAT)
THE SENIOR MANAGER: LOCAL GOVERNMENT REVENUE AND EXPENDITURE (GROUP TWO) (MR M SIGABI)
THE SENIOR MANAGER: LOCAL GOVERNMENT SUPPLY CHAIN MANAGEMENT (MR TL RADEBE)
THE SENIOR MANAGER: PROVINCIAL GOVERNMENT ACCOUNTING (MR A REDDY)
THE SENIOR MANAGER: PROVINCIAL GOVERNMENT BUDGET OFFICE (MS M KORSTEN)
THE SENIOR MANAGER: PROVINCIAL GOVERNMENT FINANCE (EXPENDITURE MANAGEMENT) (MS A PICK)
THE SENIOR MANAGER: PROVINCIAL GOVERNMENT SUPPLY CHAIN MANAGEMENT (MS N EBRAHIM)
THE SENIOR MANAGER: STRATEGIC AND OPERATIONAL MANAGEMENT SUPPORT (MS A SMIT)
THE SENIOR MANAGER: SUPPORTING AND INTERLINKED FINANCIAL SYSTEMS (MR A BASTIAANSE)

THE PROVINCIAL AUDITOR

MASTER RECORDS OFFICIAL: BUSINESS INFORMATION AND DATA MANAGEMENT

THE HEAD OF DEPARTMENT: LOCAL GOVERNMENT

THE CHIEF DIRECTOR: LOCAL GOVERNMENT BUDGET ANALYSIS – NATIONAL TREASURY (MR J HATTINGH)

THE CHIEF DIRECTOR: MFMA IMPLEMENTATION – NATIONAL TREASURY (MR TV PILLAY)

IT RISK MANAGEMENT STRUCTURE

1. PURPOSE

To provide risk management guidance in the field of IT.

2. BACKGROUND

2.1 The need for developing this guidance document was first realised during the Municipal Risk Management Forum held on 04 October 2013. The necessity of this document was strengthened after assessing municipalities during the Municipal Review and Outlook (MGRO) process.

2.2 In terms of s62(1)(c)(i) of the MFMA, "The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all reasonable steps to ensure that the municipality has and maintains effective, efficient and transparent systems of financial and risk management and internal control".

2.3 To give effect to the above mandate, the accounting officer should ensure that the municipal environment supports the effective function of IT risk management in the broader risk management context.

2.4 To assist municipalities the Western Cape Provincial Treasury embarked on an initiative to develop an IT risk management structure which would possibly assist municipalities.

2.5 Prior to finalisation of the IT risk management structure, the document was presented at the Municipal Risk Management Forum, the CAE forum and the IT Managers forum for comment. All such comments received was taken into consideration during finalisation of the attached guidance document.

3. REQUIRED ACTION

This guidance document is a conceptual structure that must be modified according to the complexity and capability of the municipality.

4. CONCLUSION

Utilisation of the IT risk management structure will assist municipalities in compiling a comprehensive IT risk register for the municipality.

MR B VINK
SENIOR MANAGER: FINANCIAL GOVERNANCE
DATE: 12 June 2014

Western Cape Government
Provincial Treasury

IT GENERAL CONTROLS REVIEW RISK STRUCTURE

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
IT Governance			
IT Governance Framework	ME4.1 Establishment of an IT Governance Framework	• Ineffective responsibilities and accountabilities established for IT processes • The IT portfolio failing to support the enterprise's objectives and strategies • Remedial actions to maintain and improve IT process effectiveness and efficiency not identified or implemented • Controls not operating as expected	1. Establish an IT strategy committee to provide high-level policy guidance (e.g. risk, funding, sourcing, partnering) and verify strategy compliance (e.g. achievement of strategic goals and objectives). 2. Establish processes to define IT enabled investment priorities, assess strategic fit of proposals and perform investment portfolio reviews for continuing strategic relevance. 3. Establish appropriate management structures such as an IT steering committee, technology council, IT architecture review council and IT audit committee. 4. Establish IT investment portfolio management disciplines, which include periodic review of portfolios to verify their continued relevance to the business. 5. Embed into the enterprise an IT governance structure and culture that is accountable, effective and transparent, with defined activities and purposes and with unambiguous responsibilities. 6. Aggregate all IT governance issues and remedial actions into a consolidated management context for reporting. Report to the council the status of IT governance issues and activities and identify their impact on strategic initiatives and enterprise outcomes.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
IT Risk Management	PO9.1 IT Risk Management Framework	• IT risks and business risks managed independently • The impact of an IT risk on the business undetected • Lack of cost control for risk management • Each risk seen as a single threat rather than in an overall context • Ineffective support for risk assessment by senior management	1. Make sure the IT risk management framework fits with the risk management objectives of the enterprise. Use similar risk classification principles and, wherever possible, classify and manage IT risks in a business-driven hierarchy, for example: • Strategic • Programme • Project • Operational 2. Define standard scales for IT risk assessment, covering impact and probability aligned with the enterprise risk management framework. 3. Align the IT risk management appetite and tolerance levels with the enterprise risk management framework.
	PO9.2 Establishment of Risk Context	• Irrelevant risks considered important • Significant risks not given appropriate attention • Inappropriate approach to risk assessment	1. Evaluate risks qualitatively according to their impact (catastrophic, critical, marginal), probability (very likely, probable, improbable) and time frame (imminent, near term, far term), or quantitatively, when appropriate probability data exist. 2. Prioritise risks by separating the 'vital few' from the rest and ranking them based upon a criterion or criteria established by the project team. Techniques for prioritisation include comparison risk ranking, multi-voting, and paring to the top 'n' and top five. 3. Perform risk assessment activities considering the context of the IT management processes that are affected.
	PO9.3 Event Identification	• Irrelevant risk events identified and focused on whilst more important events are missed	1. Obtain agreement and sign-off from stakeholders of key events and their impacts. 2. Identify potential events that could negatively affect enterprise goals or operations considering results of former audits, inspections and identified incidents, using checklists, workshops, process flow analysis, or other tools and techniques.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			3. Identify potential negative impacts that are relevant and significant for the enterprise for each of the selected events. Record and maintain the information in the risk registry, using the enterprise risk management framework terminology. 4. Involve appropriate cross-functional teams in the event and impact identification activity. Depending on the scope of the assessment, these teams may be composed of representatives from the IT, risk management and business functions. 5. Review all potential events as a whole to ensure completeness and to identify interdependencies that could affect impact and probability.
	PO9.4 Risk Assessment	• Irrelevant risks considered important • Each risk seen as a single event rather than in an overall context • Inability to explain significant risks to management • Significant risks possibly missed • Loss of IT assets • Confidentiality or integrity breach of IT assets	1. Determine the likelihood of identified risks qualitatively (e.g. very likely, probable, improbable) or quantitatively using statistical analysis and probability determinations, based on reasonable sources of information that can be appropriately validated. 2. Determine the material impact on the business of identified risks qualitatively (e.g. catastrophic, critical, marginal) or quantitatively (e.g. impact on revenue or shareholder value). 3. Assess risks inherent in the event and after considering the controls that are in place to identify the residual risks for which a risk response will need to be determined. 4. Document the results of the risk assessment, showing the method followed to come to the conclusions.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	PO9.5 Risk Response	• Risk responses not effective • Unidentified residual business risks • Ineffective use of resources to respond to risks • Overreliance on existing poor controls	1. Consider the results of the risk assessment and determine a strategy for mitigating the risks, considering the significance of the risk and the probable cost and benefit of one of more of the options—avoidance, reduction, sharing and acceptance—that aligns with strategic objectives and is in keeping with the enterprise's accepted risk management culture and risk tolerances. 2. Develop a risk action plan to implement the agreed-upon risk response based on a consideration of: • Priorities • Existing controls that could be improved or modified • Practical implementation considerations • Any specific legal, regulatory or contractual requirements • Probable costs • Potential benefits
	PO9.6 Maintenance and Monitoring of a Risk Action Plan	• Risk mitigation controls that do not operate as intended • Compensating controls that deviate from the identified risks	1. Develop the risk action plan containing prioritised risk responses. Identify priorities, responsibilities, schedules, expected outcome of risk mitigation, costs, benefits, performance measures and the review process to be established. 2. Obtain approval for recommended risk response actions from appropriate authorities. Define and document ownership for approved plan activities, and inform affected parties. 3. Ensure that accepted risks are formally recognised, approved by senior management and recorded. 4. Monitor execution of the action plan, report progress and deviations to senior management, and adjust the plan accordingly.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			5. Periodically review the action plan: • To ensure that it continues to efficiently and effectively address the IT risks identified • In light of any changes to business objectives or relevant IT systems • To identify improvement opportunities to the risk assessment and management process
Organisation Structure	PO3.4 Technology Standards	• Incompatibilities between technology platforms and applications • Deviations from the approved technological direction • Licensing violations • Increased support, replacement and maintenance costs • Inability to access historical data on unsupported technology	1. Ensure that corporate technology standards are approved by the IT architecture council and communicated throughout the organisation by using a technology forum. 2. Ensure that management establishes and maintains an approved list of vendors and system components that conform to the technological infrastructure plan and technology standards. 3. Establish a process to prevent the acquisition of non-conforming systems or applications. 4. Put technology guidelines in place to effectively support the organisation's technological solutions. 5. Put in place monitoring and benchmarking processes, such as measuring non-compliance to technology standards, to ensure compliance to the standards. 6. Update technology standards as part of a periodic review of the technological infrastructure plan. Ensure that all stakeholders are involved in the development and approval of migration strategies and change plans, taking into consideration impacts on personnel and operations.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			7. Align the information systems department's recruiting and training practices with the technology standards
	PO3.5 IT Architecture Council	• Incompatibilities between technology platforms and applications • Deviations from the approved technological direction • Uncontrolled acquisition, use and possible proliferation of information systems assets	1. Establish an IT architecture council to provide architecture guidelines and advice on their application. 2. Agree on and formally document the role and authority of the IT architecture council. Establish that the document includes the overall IT architecture design and the alignment with the information architecture. 3. Put a process in place to monitor and benchmark the effect on business strategy and identify instances of non-compliance to technology standards. 4. Ensure that the IT architecture council meets regularly and meeting minutes are taken that include actions, assignments of responsible parties, time lines and tasks
	PO4.2 IT Strategy Committee	• Lack of representation of IT on the council agenda • IT-related risks and value unknown at the council level • Decisions on investments and priorities not based on joint (business and IT) priorities • IT governance separate from corporate governance	1. Define the scope, objectives, membership, roles, responsibilities, etc. of the IT strategy committee. 2. Ensure that the IT strategy committee is composed of council and non-council members with appropriate expertise in the organisation's dependency on IT and opportunities provided by IT. 3. Ensure that the IT strategy committee meets on a regular basis to address strategic issues, including major investment decisions, raised by the council of directors or the organisation. 4. Ascertain that the IT strategy committee reports to the council of directors on IT governance and IT strategic issues.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
		• IT not compliant with governance requirements, potentially impacting management's and the council's public accountability	
	PO4.3 IT Steering Committee	• IT strategy not in line with the organisation's strategy • IT-enabled investment programmes not in support of the organisational goals and objectives • Insufficient support and involvement of IT and senior organisational management in key decision-making processes	1. Ensure that an IT steering committee exists that reports to an appropriate level of senior management and includes representation from the executive level, key business operations areas, IT and key business support areas such as finance, risk management, compliance, human resources, legal and internal audit. 2. Ensure that the IT steering committee includes a key sponsor at the executive level. 3. Ensure that the role and authority of the IT steering committee are agreed upon and formally documented. 4. Ensure that the IT steering committee meets regularly, with an appropriate and monitored frequency. 5. Determine that the responsibilities for the committee include at least: • Determination of prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities • Tracking of status of projects and resolution of resource conflict • Monitoring of service levels and service improvements 6. Ensure that the IT steering committee approves the high-level control requirements, such as consideration of key performance indicators and balanced scorecards in relation to IT, and monitors controls compliance.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	PO 4.4 Organisational placement of the IT Function	• Insufficient commitment from senior organisational management • IT resources not effectively supporting the business • IT not given sufficient strategic importance • IT regarded as separate from the business and vice versa • Lack of business direction and communication of business initiatives	1. Determine that the IT function is headed by a CIO or similar function, of which the authority, responsibility, accountability and reporting line are commensurate with the importance of IT within the enterprise. 2. Define and fund the IT function in such a way that individual user group departments cannot exert undue influence over the IT function and undermine the priorities agreed upon by the IT steering committee. 3. Ensure that the IT function is appropriately resourced (e.g. staffing, contingent workers, budget) to enable the implementation and management of appropriate IT solutions and services to support the business and enable relationships with the business.
	PO 4.5 IT Organisational Structure	• Insufficient business support • Insufficient staffing requirements • Inappropriate sourcing strategies • Inflexibility of IT to changes in business needs	1. Perform periodic reviews of the impact of organisational change as it affects the overall organisation and the structure of the IT function itself. 2. Determine that the IT organisation has flexible resource arrangements to support changing business needs, such as the use of external contractors and flexible third- party service arrangements
Service Level Agreements	DS1.1 Service Level Management Framework	• Gaps between expectations and capabilities, leading to disputes • Customers and providers not understanding their responsibilities	1. Define and document an SLA framework to manage the IT service life cycle. The process should involve senior management representing both the business and IT functions. The framework should identify IT objectives and specify measures of IT performance in meeting business objectives. The respective roles of the business and internal and external service providers should be clearly articulated. Complement the framework with formally

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
		• Inappropriate priority given to different services provided • Inefficient and costly operational service	defined and approved qualitative and quantitative measures that are easily understood and achievable. 2. Create a service catalogue that incorporates service requirements, service definitions, SLAs, OLAs and funding sources. 3. Put in place a process to continually realign SLA objectives and performance measures with business objectives and IT strategy, leveraging subject experts and comparing to accepted industry practice and benchmarks. 4. Define and implement procedures for monitoring and reporting service level performance measures. Establish escalation and resolution methods for service level issues. 5. Establish and implement an appropriate change management process for the framework, service catalogue, SLA objectives and performance measures. 6. Define a service improvement programme
	DS1.2 Definition of Services	• Inappropriately delivered services • Incorrect priority for provided services • Misunderstood impact of incidents, leading to slow response and significant business impact • Different interpretations and misunderstanding of IT services provided	1. Define a process for developing, reviewing, approving and adjusting the service catalogue or portfolio of services based on service characteristics and business requirements. 2. Put in place a management process to ensure that the service catalogue or portfolio is available, complete and up to date, and is periodically reviewed to ensure alignment with business requirements.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	DS1.3 Service Level Agreements	• Failure to meet customer service requirements • Inefficient and ineffective use of service delivery resources • Failure to identify and respond to critical service incidents	1. Ensure that the stakeholders from IT and the business negotiate, agree to and approve service requirements, and document and communicate their SLA as appropriate. The format and contents include exclusions, commercial arrangements and OLAs. 2. Confirm that the SLA management process promotes, promulgates, measures (qualitative and quantitative) and monitors the SLA objectives. 3. Perform periodic reviews of the SLA objectives, effectiveness and efficiency, and report to the SLA stakeholders. 4. Improve or adjust SLAs based on performance feedback and changes to customer and business requirements.
	DS1.4 Operating Level Agreements	• Failure of the provided services to meet the business requirements • Gaps in technical understanding of services leading to incidents • Inefficient and costly use of operational resources	1. Define a process to develop, manage, review and adjust OLAs. 2. Ensure that OLAs are in place that identify, document and explain how the services will be technically delivered to support the SLA(s). Ensure that the OLAs specify all the technical processes that are utilised and the SLAs they support (a single OLA may support several SLAs).
	DS1.5 Monitoring and Reporting of Service Level Achievements	• Lack of defined measures important to the organisation • Unidentified underlying service problems and issues • Dissatisfied users due to lack of information, irrespective of quality of service	1. Define a process to continuously monitor all agreed-upon service levels. 2. Provide regular and formal reporting of SLA performance, including deviations from the agreed-upon values, and distribute this report to different levels in the organisation. 3. Perform regular reviews to forecast and identify trends in service level performance.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	DS1.6 Review of Service Level Agreements and Contracts	• Commercial and legal requirements not met due to out-of-date contracts • Services not meeting changed requirements • Financial losses and incidents due to misaligned services	1. Put in place a process, outlined within the service level framework, to assess and report service level performance and ensure that the agreements and UCs are effective, efficient and up to date. 2. Conduct reviews of SLAs and UCs on a regular basis with all impacted parties to ensure that they remain effective and are in alignment with business objectives.
Performance of IT Service Providers	PO4.14 Contracted Staff Policies and Procedures	• Increased dependence on key (contracted) individuals • Gaps between expectations and the capability of contracted personnel • Work performed not aligned with business requirements • No knowledge capture or skills transfer from contracted personnel • Inefficient and ineffective use of contracted staff • Failure of contracted staff to adhere to organisational policies for the protection of information assets • Litigation costs from disagreements over expectations for responsibility and accountability	1. Implement policies and procedures that describe when, how and what type of work can be performed or augmented by consultants and/or contractors, in accordance with the organisation's enterprise wide IT procurement policy. 2. Require contractors to comply with the organisation's policies and procedures (e.g. requirements for security clearance, physical and logical access control requirements, client equipment and personnel, information confidentiality requirements, and nondisclosure agreements). At the commencement of the contract, the contractor formally agrees to be bound by the organisation's IT policies. Contractors are advised that management reserves the right to monitor and inspect all usage of IT resources, including e-mail, voice communications, and all programs and data files. 3. Provide contractors with a clear definition of their roles and responsibilities as part of their contracts. Contractors are explicitly required to document their work to agreed-upon standards and formats. 4. Ensure that an individual with appropriate authority within the IT function has responsibility for reviewing the contractor's work and approving payments

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	DS2.1 Identification of All Supplier Relationships	• Unidentified significant and critical suppliers • Inefficient and ineffective usage of supplier management resources • Unclear roles and responsibilities leading to miscommunications, poor services and increased costs	1. Define and regularly review criteria to identify and categorise all supplier relationships according to the supplier type, significance and criticality of service. The list should include a category describing vendors as preferred, non-preferred or not recommended. 2. Establish and maintain a detailed register of suppliers, including name, scope, purpose of the service, expected deliverables, service objectives and key contact details.
	DS2.2 Supplier Relationship Management	• Supplier not responsive or committed to the relationship • Problems and issues not resolved • Inadequate service quality	1. Define and formalise roles and responsibilities for each service supplier. 2. Assign relationship owners for all suppliers and make them accountable for the quality of service(s) provided. 3. Document the supplier relationship managers and communicate the information within the organisation. 4. Establish and document a formal communication process between the organisation and the service provider. 5. Ensure that contracts with key service suppliers provide for a review of supplier internal controls by management or independent third parties. 6. Regularly review the reports between the organisation and the service supplier. 7. Register incidents caused by suppliers and report them using the company's internal incident management process. 8. Periodically review and assess supplier performance against established and agreed-upon service levels. Clearly communicate suggested changes to the service supplier.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	DS2.3 Supplier Risk Management	• Non-compliance with regulatory and legal obligations • Security as well as other incidents • Financial losses and reputational damage because of service interruption	1. Identify and monitor supplier risks in accordance with the organisation's established risk management process. 2. Identify and document in the contract supplier risks (and remedies) associated with the supplier's inability to fulfil the contractual agreement(s). 3. When defining the contract, consider remedies including software escrow agreements, alternative suppliers or standby agreements in the event of supplier failure. 4. Review all contracts for legal and regulatory requirements
	DS2.4 Supplier Performance Monitoring	• Undetected service degradation • Inability to challenge costs and service quality • Inability to optimise choice of suppliers	1. Define and document criteria to monitor service suppliers' performance. 2. Ensure that the supplier regularly reports on agreed-upon performance criteria. 3. Invite users to provide feedback for assessment of supplier performance and quality of service. 4. Evaluate the costs and market conditions for the service levels by benchmarking against alternative suppliers, and identify potential for improvement. 5. Define arbitration procedures to consult an arbitration committee before bringing an action.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
Security Management			
IT Security Policies and Procedures	DS5.1 Management of IT Security	• Lack of IT security governance • Misaligned IT and business objectives • Unprotected data and information assets	1. Define a charter for IT security, defining for the security management function: • Scope and objectives for the security management function • Responsibilities • Drivers (e.g., compliance, risk, performance) 2. Confirm that the council, executive management and line management direct the policy development process to ensure that the IT security policy reflects the requirements of the business. 3. Set up an adequate organisational structure and reporting line for information security, ensuring that the security management and administration functions have sufficient authority. Define the interaction with enterprise functions, particularly the control functions such as risk management, compliance and audit. 4. Implement an IT security management reporting mechanism, regularly informing the council and business and IT management of the status of IT security so that appropriate management actions can be taken.
	DS5.2 IT Security Plan	• IT security plan not aligned with business requirements • IT security plan not cost effective • Business exposed to threats not covered in the strategy • Gaps between planned and implemented IT security measures	1. Define and maintain an overall IT security plan that includes: • A complete set of security policies and standards in line with the established information security policy framework • Procedures to implement and enforce the policies and standards • Roles and responsibilities • Staffing requirements • Security awareness and training • Enforcement practices • Investments in required security resources

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
		• Users not aware of the IT security plan • Security measures compromised by stakeholders and users	2. Collect information security requirements from IT tactical plans (PO1), data classification (PO2), technology standards (PO3), security and control policies (PO6), risk management (PO9), and external compliance requirements (ME3) for integration into the overall IT security plan. 3. Translate the overall IT security plan into enterprise information security baselines for all major platforms and integrate it into the configuration baseline (DS9). 4. Provide information security requirements and implementation advice to other processes, including the development of SLAs and OLAs (DS1 and DS2), automated solution requirements (AI1), application software (AI2), and IT infrastructure components (AI3). 5. Communicate to all stakeholders and users in a timely and regular fashion on updates of the information security strategy, plans, policies and procedures
Password Security (Application and O/S)	DS5.3 Identity Management	• Unauthorised changes to hardware and software • Access management failing business requirements and compromising the security of business-critical systems • Unspecified security requirements for all systems • Segregation-of-duty violations • Compromised system information	1. Establish and communicate policies and procedures to uniquely identify, authenticate and authorise access mechanisms and access rights for all users on a need-to-know/ need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved. 2. Ensure that roles and access authorisation criteria for assigning user access rights take into account: • Sensitivity of information and applications involved (data classification) • Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements) • Roles and responsibilities as defined within the enterprise • The need-to-have access rights associated with the function

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			• Standard but individual user access profiles for common job roles in the organisation • Requirements to guarantee appropriate segregation of duties 3. Establish a method for authenticating and authorising users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements. 4. Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person. 5. Ensure that a timely information flow is in place that reports changes in jobs (i.e. people in, people out, people change). Grant, revoke and adapt user access rights in co-ordination with human resources and user departments for users who are new, who have left the organisation, or who have changed roles or jobs.
	DS5.4 User Account Management	• Security breaches • Users failing to comply with security policy • Incidents not solved in a timely manner • Failure to terminate unused accounts in a timely manner, thus impacting corporate security	1. Ensure that access control procedures include but are not limited to: • Using unique user IDs to enable users to be linked to and held accountable for their actions • Awareness that the use of group IDs results in the loss of individual accountability and are permitted only when justified for business or operational reasons and compensated by mitigating controls. Group IDs must be approved and documented. • Checking that the user has authorisation from the system owner for the use of the information system or service, and the level of access granted is appropriate to the business purpose and consistent with the organisational security policy

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			• A procedure to require users to understand and acknowledge their access rights and the conditions of such access • Ensuring that internal and external service providers do not provide access until authorisation procedures have been completed • Maintaining a formal record, including access levels, of all persons registered to use the service • A timely and regular review of user IDs and access rights 2. Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorisations for special privileged access rights should be reviewed independently at more frequent intervals
	DS5.5 Security Testing, Surveillance and Monitoring	• Misuse of users' accounts, compromising organisational security • Undetected security breaches • Unreliable security logs	1. Implement monitoring, testing, reviews and other controls to: • Promptly prevent/detect errors in the results of processing • Promptly identify attempted, successful and unsuccessful security breaches and incidents • Detect security events and thereby prevent security incidents by using detection and prevention technologies • Determine whether the actions taken to resolve a breach of security are effective 2. Conduct effective and efficient security testing procedures at regular intervals to: • Verify that identity management procedures are effective • Verify that user account management is effective • Validate that security-relevant system parameter settings are defined correctly and are in compliance with the information security baseline • Validate that network security controls/settings are configured properly and are in compliance with the information security baseline

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			• Validate that security monitoring procedures are working properly • Consider, where necessary, obtaining expert reviews of the security perimeter
	DS5.6 Security Incident Definition	• Undetected security breaches • Lack of information for performing counterattacks • Missing classification of security breaches	1. Describe what a security incident is considered to be. Document within the characteristics a limited number of impact levels to allow commensurate response. Communicate and distribute this information, or relevant parts thereof, to identify people who need to be notified. 2. Ensure that security incidents and appropriate follow-up actions, including root cause analysis, follow the existing incident and problem management processes. 3. Define measures to protect confidentiality of information related to security incidents.
	DS5.7 Protection of Security Technology	• Exposure of information • Breach of trust with other organisations • Violations of legal and regulatory requirements	1. Ensure that all hardware, software and facilities related to the security function and controls, e.g. security tokens and encryptors, are tamperproof. 2. Secure security documentation and specifications to prevent unauthorised access. However, do not make security of systems reliant solely on secrecy of security specifications. 3. Make the security design of dedicated security technology (e.g. encryption algorithms) strong enough to resist exposure, even if the security design is made available to unauthorised individuals. 4. Evaluate the protection mechanisms on a regular basis (at least annually) and perform updates to the protection of the security technology, if necessary.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	DS5.8 Cryptographic Key Management	• Keys misused by unauthorised parties • Registration of non-verified users, thus compromising system security • Unauthorised access to cryptographic keys	1. Ensure that there are appropriate procedures and practices in place for the generation, storage and renewal of the root key, including dual custody and observation by witnesses. 2. Make sure that procedures are in place to determine when a root key renewal is required (e.g. the root key is compromised or expired). 3. Create and maintain a written certification practice statement that describes the practices that have been implemented in the certification authority, registration authority and directory when using a public-key-based encryption system. 4. Create cryptographic keys in a secure manner. When possible, enable only individuals not involved with the operational use of the keys to create the keys. Verify the credentials of key requestors (e.g. registration authority). 5. Ensure that cryptographic keys are distributed in a secure manner (e.g. offline mechanisms) and stored securely, that is: • In an encrypted form regardless of the storage media used (e.g. write-once disk with encryption) • With adequate physical protection (e.g. sealed, dual custody vault) if stored on paper 6. Create a process that identifies and revokes compromised keys. Notify all stakeholders as soon as possible of the compromised key. 7. Verify the authenticity of the counterparty before establishing a trusted path

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
Anti-Virus	DS5.9 Malicious Software Prevention, Detection and Correction	• Exposure of information • Violations of legal and regulatory requirements • Systems and data that are prone to virus attacks • Ineffective countermeasures	1. Establish, document, communicate and enforce a malicious software prevention policy in the organisation. Ensure that people in the organisation are aware of the need for protection against malicious software, and their responsibilities relative to same. 2. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically). 3. Distribute all protection software centrally (version and patch-level) using centralised configuration and change management. 4. Regularly review and evaluate information on new potential threats. 5. Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information (e.g. spyware, phishing e-mails).
Patch Management	AI3.3 Infrastructure Maintenance	• Disruptions in production processing • Unauthorised access to sensitive software • Technology failing to support business needs • Violation of licence agreements	1. Establish a strategy and plan for infrastructure maintenance to provide overall guidance in line with the organisation's change management procedures. 2. Ensure that maintenance of the installed system software (patches, service packs and other updates) is managed through the established change management process and is performed in accordance with vendor procedures and guidelines by qualified and authorised internal and/or vendor personnel. 3. Maintain documentation of system software, and ensure that it is complete and current. Require vendors to deliver new and updated documentation each time the system software is maintained. 4. Maintain currency of system software by applying vendor upgrades or patches in a timely manner.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			5. Review on a regular basis the amount of maintenance being performed and the vulnerability to unsupported infrastructure; consider future risks, including security vulnerabilities. Report any issues identified for consideration within the infrastructure planning process

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
User Access Control			
Policies & Procedures	PO6.4 Policy, Standard and Procedures Rollout	• Organisation's policies, standards and procedures unknown or not accepted • Lack of communication of management's aims and directions • Control culture not aligned with management's aims • Policies misunderstood or not accepted • Business risk of policies and procedures not followed	1. Ensure that policies are effectively translated into operational standards. 2. Ensure that employment contracts are aligned with policies. 3. Capture explicit acknowledgement from users as to their receipt and understanding of the policies, procedures and standards. 4. Ensure that sufficient and skilled resources are available to support the rollout process. Rollout methods should address resource and awareness needs and implications.
New Users	DS5.3 Identity Management	• Unauthorised changes to hardware and software • Access management failing business requirements and compromising the security of business-critical systems • Unspecified security requirements for all systems • Segregation-of-duty violations • Compromised system information	1. Establish and communicate policies and procedures to uniquely identify, authenticate and authorise access mechanisms and access rights for all users on a need-to-know/ need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved. 2. Ensure that roles and access authorisation criteria for assigning user access rights take into account: • Sensitivity of information and applications involved (data classification) • Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements) • Roles and responsibilities as defined within the enterprise • The need-to-have access rights associated with the function • Standard but individual user access profiles for common job roles in the organisation • Requirements to guarantee appropriate segregation of duties

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			3. Establish a method for authenticating and authorising users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements. 4. Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person. 5. Ensure that a timely information flow is in place that reports changes in jobs (i.e. people in, people out, people change). Grant, revoke and adapt user access rights in co-ordination with human resources and user departments for users who are new, who have left the organisation, or who have changed roles or jobs.
Termination of Users			
Segregation of Duties			

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
Access to Master Data	DS5.11 Exchange of Sensitive Data	• Sensitive information exposed • Inadequate physical security measures • Unauthorised external connections to remote sites • Disclosure of corporate assets and sensitive information accessible for unauthorised parties	1. Determine by using the established information classification scheme how the data should be protected when exchanged. 2. Apply appropriate application controls to protect the data exchange. 3. Apply appropriate infrastructure controls, based on information classification and technology in use, to protect the data exchange.
Reviewing and Monitoring			

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
IT Service Continuity			
IT Disaster Recovery Plan	DS4.1 IT Continuity Framework	• Insufficient continuity practices • IT continuity services not managed properly • Increased dependency on key individuals	1. Assign responsibility for and establish an enterprise wide business continuity management process. This process should include an IT continuity framework to ensure that a Business Impact Analysis (BIA) is completed and IT continuity plans support business strategy, a prioritised recovery strategy, necessary operational support based on these strategies and any compliance requirements. 2. Ensure that the continuity framework includes: • The conditions and responsibilities for activating and/or escalating the plan • Prioritised recovery strategy, including the necessary sequence of activities • Minimum recovery requirements to maintain adequate business operations and service levels with diminished resources • Emergency procedures • Fall-back procedures • Temporary operational procedures • IT processing resumption procedures • Maintenance and test schedule • Awareness, education and training activities • Responsibilities of individuals • Regulatory • Critical assets and resources and up-to-date personnel contact information needed to perform emergency, fall-back and resumption procedures • Alternative processing facilities as determined within the plan • Alternative suppliers for critical resources • Chain of communications plan • Key resources identified 3. Ensure that the IT continuity framework addresses: • Organisational structure for IT continuity management as a liaison to organisational continuity management

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			• Roles, tasks and responsibilities defined by SLAs and/or contracts for internal and external service providers • Documentation standards and change management procedures for all IT continuity-related procedures and tests • Policies for conducting regular tests • The frequency and conditions (triggers) for updating the IT continuity plans • The results of the risk assessment process (PO9)
	DS4.2 IT Continuity Plans	• Failure to recover IT systems and services in a timely manner • Failure of alternative decision-making processes • Lack of required recovery resources • Failed communication to internal and external stakeholders	1. Create an IT continuity plan, including: • The conditions and responsibilities for activating and/or escalating the plan • Prioritised recovery strategy, including the necessary sequence of activities • Minimum recovery requirements to maintain adequate business operations and service levels with diminished resources • Emergency procedures • Fall-back procedures • Temporary operational procedures • IT processing resumption procedures • Maintenance and test schedule • Awareness, education and training activities • Responsibilities of individuals • Regulatory requirements • Critical assets and resources and up-to-date personnel contact information needed to perform emergency, fall-back and resumption procedures • Alternative processing facilities as determined within the plan • Alternative suppliers for critical resources 2. Define underlying assumptions (e.g. level of outage covered by the plan) in the IT continuity plan and which systems (i.e., computer systems, network components and other IT infrastructure) and sites are to be included. Note alternative processing options for each site.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			3. Ensure that the IT continuity plan includes a defined checklist of recovery events as well as a form for event logging. 4. Establish and maintain detailed information for every recovery site, including assigned staff and logistics (e.g. transport of media to the recovery site). This information should include: • Processing requirements for each site • Location • Resources (e.g. systems, staff, support) available at each location • Utility companies on which the site depends 5. Define response and recovery team structures, including reporting requirements roles and responsibilities as well as knowledge, skills and experience requirements for all team members. Include contact details of all team members, and ensure that that they are maintained and readily available (e.g. offsite team, backup managing team). 6. Define and prioritise communication processes and define responsibility for communication (e.g. public, press, government). Maintain contact details of relevant stakeholders (e.g. crisis management team, IT recovery staff, business stakeholders, staff), service providers (e.g. vendors, telecommunications provider) and external parties (e.g. business partners, media, government bodies, public). 7. Maintain procedures to protect and restore the affected part of the organisation, including, where necessary, reconstruction of the affected site or its replacement. This also includes procedures to respond to further disasters while in the backup site. 8. Create emergency procedures to ensure the safety of all affected parties, including coverage of occupational health and safety requirements (e.g. counselling services) and co-ordination with public authorities

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	DS4.3 Critical IT Resources	• Unavailability of critical IT resources • Increased costs for continuity management • Prioritisation of services recovery not based on business needs	1. Define priorities for all applications, systems and sites that are in line with business objectives. Include these priorities in the continuity plan. When defining priorities, consider: • Business risk and IT operational risk • Interdependencies • The data classification framework • SLAs and OLAs • Costs 2. Consider resilience, response and recovery requirements for different tiers, e.g. one to four hours, four to 24 hours, more than 24 hours and critical business operational periods
	DS4.4 Maintenance of the IT Continuity Plan	• Inappropriate recovery plans • Plans failing to reflect changes to business needs and technology • Lack of change control procedures	1. Maintain a change history of the IT continuity plan. Ensure proper version management of the plan, e.g. through the use of document management systems. Ensure that all distributed copies are the same version. 2. Involve the business continuity and IT continuity manager(s) in the change management processes to ensure awareness of important changes that would require updates to the IT continuity plans. 3. Update the IT continuity plan as described by the IT continuity framework. Triggering events for the update of the plan include: • Important architecture changes • Important business changes • Key staff changes or organisation changes • Incidents/disasters and the lessons learnt • Results from continuity plan tests

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	DS4.5 Testing of the IT Continuity Plan	• Shortcomings in recovery plans • Out-dated recovery plans that do not reflect the current architecture • Inappropriate recovery steps and processes • Inability to effectively recover should real disaster occur	1. Schedule IT continuity tests on a regular basis or after major changes in the IT infrastructure or to the business and related applications. Ensure that all new components (e.g. hardware, software updates, new business processes) are included in the schedule. 2. Create a detailed test schedule based on established recovery priorities. Ensure that test scenarios are realistic. Tests should include recovery of critical business application processing and should not be limited to recovery of infrastructure. Make sure that testing time is adequate and will not impact the on-going business. 3. Establish an independent test task force that keeps track of all events and records all results to be discussed in the debriefing. The members of the task force should not be key personnel defined in the plan. This task force should independently report to senior management and/or the council of directors. 4. Perform a debriefing event wherein all failures are analysed and solutions are developed or handed over to task forces. Ensure that all outstanding issues related to continuity planning are analysed and resolved in an appropriate time frame. Schedule a retesting of the changes using similar or stronger parameters to ensure a positive impact on the recovery procedures. 5. If testing is not feasible, evaluate alternative means for ensuring resources for business continuity (e.g. dry run). 6. Measure and report the success or failure of the test and, therefore, the continuity and contingency ability for services to the risk management process (PO9).

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	DS4.6 IT Continuity Plan Training	• Out-dated training schedules • Failure to recover as expected due to inadequate or out-dated training	1. On a regular basis (at least annually) or upon plan changes, provide training to the required staff members with respect to their roles and responsibilities. 2. Assess all needs for training periodically and update all schedules appropriately. While planning the training, take into account the timing and the extent of plan updates and changes, turnover of recovery staff, and recent test results. 3. Perform regular IT continuity awareness programmes for all level of employees as well as IT stakeholders to increase awareness of the need for an IT continuity strategy and their key role within it. 4. Measure and document training attendance, training results and coverage
	DS4.7 Distribution of the IT Continuity Plan	• Confidential information in the plans compromised • Plans not accessible to all required parties • Upgrades of the plan not performed in a timely manner due to uncontrolled distribution strategies	1. Define a proper distribution list for the IT continuity plan and keep this list up to date. Include people and locations in the list on a need-to-know basis. Ensure that procedures exist with instructions for storage of confidential information. 2. Define a distribution process that: • Distributes the IT continuity plan in a timely manner to all recipients and locations on the distribution list • Collects and destroys obsolete copies of the plan in line with the organisation's policy for discarding confidential information 3. Ensure that all digital and physical copies of the plan are protected in an appropriate manner (e.g. encryption, password protection) and the document is accessible only by authorised personnel (recovery staff).

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
Backup Process	DS4.9 Offsite Backup Storage	• Unavailability of backup data and media due to missing documentation in offsite storage • Loss of data due to disaster • Accidental destruction of backup data • Inability to locate backup tapes when needed	1. Provide protection for data commensurate with the value and security classification, from the time they are taken offsite, while in transport to/from the organisation and at the storage location. 2. Ensure that the backup facilities are not subject to the same risks (e.g. geography, weather, key service provider) as the primary site. 3. Perform regular testing of: • The quality of the backups and media • The ability to meet the committed recovery time frame 4. Ensure that the backups contain all data, programs and associated resources needed for recovery according to plan. 5. Provide sufficient recovery instructions and adequate labelling of backup media. 6. Maintain an inventory of all backups and backup media. Ensure inclusion of all departmental processing, if applicable.
Restoration of backups	DS4.8 IT Services Recovery and Resumption	• Shortcomings in recovery plans • Inappropriate recovery steps and processes • Failure to recover business-critical systems and services in a timely manner	1. Activate the IT continuity plan when conditions require it. 2. Maintain an activity and problem log during recovery activities to be used during post-resumption review.
	DS4.10 Post-resumption Review	• Inappropriate recovery plans • Recovery plans failing to meet business needs • Objectives not met by the recovery plans	1. Using the problem and activity log of recovery activities, identify the shortcomings of the plan after re-establishing normal processing, and agree on opportunities for improvement to include in the next update of the IT continuity plan.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
Program Change Control			
Policies and Procedures	AI6.1 Change Standards and Procedures	• Inappropriate resource allocation • No tracking of changes • Insufficient control over emergency changes • Increased likelihood of unauthorised changes being introduced to key business systems • Failure to comply with compliance requirements • Unauthorised changes • Reduced system availability	1. Develop, document and promulgate a change management framework that specifies the policies and processes, including: • Roles and responsibilities • Classification and prioritisation of all changes based on business risk • Assessment of impact • Authorisation and approval of all changes by the business process owners and IT • Tracking and status of changes • Impact on data integrity (e.g. all changes to data files being made under system and application control rather than by direct user intervention) 2. Establish and maintain version control over all changes. 3. Implement roles and responsibilities that involve business process owners and appropriate technical IT functions. Ensure appropriate segregation of duties. 4. Establish appropriate record management practices and audit trails to record key steps in the change management process. Ensure timely closure of changes. Elevate and report to management changes that are not closed in a timely fashion. 5. Consider the impact of contracted services providers (e.g. of infrastructure, application development and shared services) on the change management process. Consider integration of organisational change management processes with change management processes of service providers. Consider the impact of the organisational change management process on contractual terms and SLAs

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
Approval of Changes	AI6.2 Impact Assessment, Prioritisation and Authorisation	• Unintended side effects • Adverse effects on capacity and performance of the infrastructure • Lack of priority management of changes	1. Develop a process to allow business process owners and IT to request changes to infrastructure, systems or applications. Develop controls to ensure that all such changes arise only through the change request management process. 2. Categorise all requested changes (e.g. infrastructure, operating systems, networks, application systems, purchased/packaged application software). 3. Prioritise all requested changes. Ensure that the change management process identifies both the business and technical needs for the change. Consider legal, regulatory and contractual reasons for the requested change. 4. Assess all requests in a structured fashion. Ensure that the assessment process addresses impact analysis on infrastructure, systems and applications. Consider security, legal, contractual and compliance implications of the requested change. Consider also interdependencies amongst changes. Involve business process owners in the assessment process, as appropriate. 5. Ensure that each change is formally approved by business process owners and IT technical stakeholders, as appropriate.
	AI6.3 Emergency Changes	• Inability to respond effectively to emergency change needs • Additional access authorisation not terminated properly • Unauthorised changes applied, resulting in compromised security and unauthorised access to corporate information	1. Ensure that a documented process exists within the overall change management process to declare, assess, authorise and record an emergency change. 2. Ensure that emergency changes are processed in accordance with the emergency change element of the formal change management process. 3. Ensure that all emergency access arrangements for changes are appropriately authorised, documented and revoked after the change has been applied.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			4. Conduct a post-implementation review of all emergency changes, involving all concerned parties. The review should consider implications for aspects such as further application system maintenance, impact on development and test environments, application software development quality, documentation and manuals, and data integrity.
User Acceptance Testing	AI6.4 Change Status Tracking and Reporting	• Insufficient allocation of resources • Changes not recorded and tracked • Undetected unauthorised changes to the production environment	1. Establish a process to allow requestors and stakeholders to track the status of requests throughout the various stages of the change management process. 2. Categorise change requests in the tracking process (e.g. rejected, approved but not yet initiated, approved and in process, and closed). 3. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g. aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition. 4. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.
	AI7.1 Training	• Failure to promptly detect problems with systems or their use • Gaps in knowledge to perform required duties and activities • Errors resulting from new projects	1. For systems development, implementation or modification projects, a training plan is an integral part of the overall project master plan. Ensure that the plan clearly identifies learning objectives, resources, key milestones, dependencies and critical path tasks impacting the delivery of the training plan. The plan should consider alternative training strategies depending on the business needs, risk level (e.g. for mission-critical systems, a formal system of user accreditation and reaccreditation may be appropriate), and regulatory and compliance requirements (e.g. impact of varying privacy laws may require adaptation of the training at a national level).

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			2. Ensure that the training plan identifies and addresses all impacted groups, including business end users, IT operations, support and IT application development training, and service providers. The training plan should incorporate the delivery of the training in a timely manner. It should also identify staff members who must be trained and those for whom training is desirable. 3. Consider alternative training strategies that satisfy the training requirements, and select the most cost-effective approach that aligns with the organisation's training framework. Alternative strategies include train the trainer, end-user accreditation and intranet-based training. 4. Confirm that there is a process to ensure that the training plan is executed satisfactorily. Complete the documentation detailing compliance with the training plan. Examples of information include lists of staff members invited to attend the training, attendees, evaluations of achievement of learning objectives and other feedback. 5. Monitor training to obtain feedback that could lead to potential improvements in either the training or the system. 6. Monitor all planned changes to ensure that training requirements have been considered and suitable plans created. Consider postponing the change if training has not been performed and the lack of training would jeopardise the implementation of the change
	AI7.2 Test Plan	• Insufficient testing by automated test scripts • Performance problems undetected • Lack of cost control over testing activities	1. Develop and document the test plan, which aligns to the project quality plan and relevant organisational standards. Communicate and consult with appropriate business process owners and IT stakeholders. 2. Ensure that the test plan reflects an assessment of risks from the project and that all functional and technical requirements are tested. Based on assessment of the risk of system failure and faults

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
		• Undefined testing roles and responsibilities	on implementation, the plan should include requirements for performance, stress, usability, pilot and security testing. 3. Ensure that the test plan addresses the potential need for internal or external accreditation of outcomes of the test process (e.g. financial regulatory requirements). 4. Ensure that the test plan identifies necessary resources to execute testing and evaluate the results. Examples of resources include construction of test environments and staff for the test group, including potential temporary replacement of test staff in the production or development environments. Ensure that stakeholders are consulted on the resource implications of the test plan. 5. Ensure that the test plan identifies testing phases appropriate to the operational requirements and environment. Examples of such testing phases include unit test, system test, integration test, user acceptance test, performance test, stress test, data conversion test, security test, operational readiness, and backup and recovery tests. 6. Confirm that the test plan considers test preparation (including site preparation), training requirements, installation or an update of a defined test environment, planning/ performing/ documenting/retaining test cases, error and problem handling, correction and escalation, and formal approval. 7. Ensure that the test plan establishes clear criteria for measuring the success of undertaking each testing phase. Consult the business process owners and IT stakeholders in defining the success criteria. Determine that the plan establishes remediation procedures when the success criteria are not met (e.g. in a case of significant failures in a testing phase, the plan provides guidance on whether to proceed to the next phase, stop testing or postpone implementation).

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			8. Confirm that all test plans are approved by stakeholders, including business process owners and IT, as appropriate. Examples of such stakeholders are application development managers, project managers and business process end users.
	AI7.3 Implementation Plan	• Improper resource allocation to ensure effective implementation of changes • Security breaches	1. Define a policy for numbering and frequency of releases. 2. Confirm that all implementation plans are approved by stakeholders, including technical and business. 3. Create an implementation plan reflecting the outcomes of a formal review of technical and business risks. Include with the implementation plan: • The broad implementation strategy • The sequence of implementation steps • Resource requirements • Interdependencies • Criteria for management agreement to the production implementation • Installation verification requirements • Transition strategy for production support Align the implementation plan with the business change management plan. 4. Obtain commitment from third parties to their involvement in each step of the implementation. 5. Identify and document the fall-back and recovery process
	AI7.4 Test Environment	• Insufficient testing using automated test scripts • Performance problems undetected	1. Ensure that the test environment is representative of the future operating landscape, including likely workload stress, operating systems, necessary application software, database management systems, and network and computing infrastructure found in the production environment.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
		• System security compromised	2. Ensure that the test environment is secure and incapable of interacting with production systems. 3. Create a database of test data that are representative of the production environment. Sanitise data used in the test environment from the production environment according to business needs and organisational standards (e.g. consider whether compliance or regulatory requirements oblige the use of sanitised data). 4. Protect sensitive test data and results against disclosure, including access, retention, storage and destruction. Consider the effect of interaction of organisational systems with those of third parties. 5. Put in place a process to enable proper retention or disposal of test results, media and other associated documentation to enable adequate review and subsequent analysis as required by the test plan. Consider the effect of regulatory or compliance requirements
	AI7.5 System and Data Conversion	• Old systems not available when needed • Unreliable system and conversion results • Subsequent processing interruptions • Data integrity issues	1. Define a data conversion and infrastructure migration plan. Consider, for example, hardware, networks, operating systems, software, transaction data, master files, backups and archives, interfaces with other systems (both internal and external), procedures and system documentation, in the development of the plan. 2. Ensure that the data conversion plan incorporates methods for collecting, converting and verifying data to be converted and identifying and resolving any errors found during conversion. This includes comparing the original and converted data for completeness and integrity. 3. Confirm that the data conversion plan does not require changes in data values unless absolutely necessary for business reasons. Document changes made to data values, and secure approval from the business process data owner.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			4. Consider real-time disaster recovery, business continuity planning, and reversion in the data conversion and infrastructure migration plan where risk management, business needs, or regulatory/compliance requirements demand. 5. Co-ordinate and verify the timing and completeness of the conversion cutover so there is a smooth, continuous transition with no loss of transactions. Where necessary, in the absence of any other alternative, freeze live operations. 6. Ensure that there is a backup of all systems and data taken at the point prior to conversion, audit trails are maintained to enable the conversion to be retraced, and there is a fall-back and recovery plan in case the conversion fails. Ensure that retention of backup and archived data conforms to business needs and regulatory or compliance requirements
	AI7.6 Testing of Changes	• Waste of resources • Degraded overall security • Changes impacting system performance and availability	1. Ensure that testing of changes is undertaken in accordance with the testing plan. Ensure that the testing is designed and conducted by a test group independent from the development team. Consider the extent to which business process owners and end users are involved in the test group. Ensure that testing is conducted only within the test environment. 2. Ensure that the tests and anticipated outcomes are in accordance with the defined success criteria set out in the testing plan. 3. Consider using clearly defined test instructions (scripts) to implement the tests. Ensure that the independent test group assesses and approves each test script to confirm that it adequately addresses test success criteria set out in the test plan. Consider using scripts to verify the extent to which the system meets security requirements. Consider the appropriate balance between automated scripted tests and interactive user testing.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			4. Undertake tests of security in accordance with the test plan. Measure the extent of security weaknesses or loopholes. Consider the effect of security incidents since construction of the test plan. Consider the effect on access and boundary controls. 5. Undertake tests of system and application performance in accordance with the test plan. Consider a range of performance metrics (e.g. end-user response times and database management system update performance). 6. When undertaking testing, ensure that the fall-back and rollback elements of the test plan have been addressed. 7. Identify, log and classify (e.g. minor, significant and mission-critical) errors during testing. Ensure that an audit trail of test results is available. Communicate results of testing to stakeholders in accordance with the test plan to facilitate bug fixing and further quality enhancement
	AI7.7 Final Acceptance Test	• Performance problems undetected • Business rejection of delivered capabilities	1. Ensure that the scope of final acceptance evaluation activities covers all components of the information system (e.g. application software, facilities, technology, user procedures, operations procedures, monitoring and support). 2. Ensure that the categorised log of errors found in the testing process has been addressed by the development team. Ensure that the cause of errors has been remediated (e.g. by appropriate changes to the application, configuration or workaround, and/or delayed correction where the error is minor). 3. Ensure that the final acceptance evaluation is measured against the success criteria set out in the testing plan. Ensure that the review and evaluation process is appropriately documented.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			4. Document and interpret the final acceptance testing results, and present them in a form that is understandable to business process owners and IT so an informed review and evaluation can take place. 5. Ensure that business process owners, third parties (as appropriate) and IT stakeholders formally sign off on the outcome of the testing process as set out in the testing plan. Such approval is mandatory prior to promotion to production
	AI7.8 Promotion to Production	• Segregation of duties violations • Systems exposed to fraud or other malicious acts • No rollback to previous application system version possible	1. Ensure that a formal process for application, system and configuration transfer from testing to the production environment exists. Ensure that the process is in accordance with organisational change management standards. 2. Ensure that the approval process clearly identifies effective dates for promotion to production of new systems, applications or infrastructure, as appropriate. Ensure that the approval process clearly identifies effective dates for retirement of old systems, applications or infrastructure, as appropriate. 3. Ensure that the approval process includes a formal documented sign-off from business process owners, third parties and IT stakeholders, as appropriate (e.g. development group, security group, database management, user support and operations group). 4. Consider the extent of parallel processing of the old and new system in line with the implementation plan. 5. Promptly update all copies of system documentation and configuration information, including backup copies stored offsite, for software, hardware, operating personnel and system users before a new or modified system is implemented. Promptly update relevant contingency plan documents, as appropriate.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			6. Ensure that all source program libraries are updated promptly with the version of the program being transferred from testing to the production environment. Ensure that the existing version and its supporting documentation are archived. Ensure that promotion to production of systems, application software and infrastructure is under configuration control. 7. In high-risk environments, consider obtaining from the testing function the media used for implementation to ensure that the software implemented is unchanged from what has been tested. 8. Where distribution of systems or application software is conducted electronically, control automated software distribution to ensure that users are notified and distribution occurs only to authorised and correctly identified destinations. Implement checks in the distribution process to verify that the destination environment is of the correct standard implementation and version prior to the new software being installed and to ensure implementation on the approved effective date. Include in the release process back out procedures to enable the distribution of software changes to be reviewed in the event of a malfunction or error. 9. Where distribution takes physical form, keep a formal log of what software and configuration items have been distributed, to whom, where they have been implemented, and when each has been updated. Implement a procedure to ensure the log's integrity and completeness. Ensure that there are checks in the physical distribution process to ensure implementation on the approved effective date. 10. Update all program copies in use in the production environment with the version being transferred from testing to the production environment in accordance with the implementation plan

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
	AI7.9 Post-implementation Review	• Failure to identify that systems do not meet end users' needs • Return on investments failing to meet management's expectations	1. Establish procedures to ensure that post-implementation reviews identify, assess and report on the extent to which: • Business requirements have been met • Expected benefits have been realised • The system is considered usable • Internal and external stakeholders' expectations are met • Unexpected impacts on the organisation have occurred • Key risks are mitigated • The change management, installation and accreditation processes were performed effectively and efficiently 2. Consult business process owners and IT technical management in the choice of metrics for measurement of success and achievement of requirements and benefits. 3. Ensure that the form of the post-implementation review is in accordance with the organisational change management process. Involve business process owners and third parties, as appropriate. 4. Consider requirements for post-implementation review arising from outside business and IT (e.g. internal audit, enterprise risk management, regulatory compliance). 5. Agree on and implement an action plan to address issues identified in the post-implementation review. Involve business process owners and IT technical management in the development of the action plan
Access of developers and vendors			

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
Facilities and Environment			
Visit to Server Room	DS12.1 Site Selection and Layout	• Threats to physical security not identified • Increased vulnerability to security risks, resulting from site location and/or layout	1. Using the technology strategy, select a site for IT equipment that meets business requirements and the security policy. Take into account special considerations such as geographic position, neighbours and infrastructure. Other risks that need consideration include, but are not limited to, theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals or explosives. 2. Define a process that identifies the potential risks and threats to the organisation's IT sites and assesses the business impact on an on-going basis, taking into account the risk associated with natural and man-made disasters. 3. Ensure that the selection and design of the site take into account relevant laws and regulations, such as building codes and environmental, fire, electrical engineering, and occupational health and safety regulations
Physical access controls	DS12.2 Physical Security Measures	• Threats to physical security not identified • Hardware stolen by unauthorised people • Physical attack on the IT site • Devices reconfigured without authorisation • Confidential information being accessed by devices configured to read the radiation emitted by the computers	1. Define and implement a policy for the physical security and access control measures to be followed for IT sites. Regularly review the policy to ensure that it remains relevant and up to date. 2. Limit the access to information about sensitive IT sites and the design plans. Ensure that external signs and other identification of sensitive IT sites are discreet and do not obviously identify the site from outside. Confirm that organisational directories/site maps do not identify the location of the IT site. 3. Design physical security measures to take into account the risk associated with the business and operation. Physical security measures include alarm systems, building hardening, armoured cabling protection and secure partitioning.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			4. Periodically test and document the preventive, detective and corrective physical security measures to verify design, implementation and effectiveness. 5. Ensure that the site design takes into account the physical cabling of telecommunication and the piping of water, power and sewer. The installation must be concealed, so it is not directly visible. The piping of water and sewer must also be redirected away from the server rooms. 6. Define a process for the secure removal of IT equipment, supported by the appropriate authorisation. 7. Safeguard receiving and shipping areas of IT equipment in the same manner and scope as normal IT sites and IT operations. 8. Define and implement a policy and process to transport and store equipment securely. 9. Define a process to ensure that storage devices containing sensitive information are physically destroyed or sanitised. 10. Define a process for recording, monitoring, managing, reporting and resolving physical security incidents, in line with the overall IT incident management process. 11. Ensure that particularly sensitive sites are checked frequently (including weekends and holidays).
	DS12.3 Physical Access	• Visitors gaining unauthorised access to IT equipment or information • Unauthorised entry to secure areas	1. Define and implement a process that governs the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorised by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			2. Define and implement procedures to ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities. 3. Define a process to log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site. 4. Define and implement a policy instructing all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorisation. 5. Define and implement a policy requiring visitors to be escorted at all times while onsite by a member of the IT operations group. If a member of the group identifies an unaccompanied, unfamiliar individual who is not wearing staff identification, security personnel should be alerted. 6. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. The devices record entry and sound an alarm in the event of unauthorised access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners. 7. Define a process to conduct regular physical security awareness training
Environmental controls (e.g. Aircon)	DS12.4 Protection Against Environmental Factors	• Facilities exposed to environmental impacts • Inadequate environmental threat detection • Inadequate measures for environmental threat protection	1. Establish and maintain a process to identify natural and man-made disasters that might occur in the area within which the IT facilities are located. Assess the potential effect on the IT facilities. 2. Define and implement a policy that identifies how IT equipment, including mobile and offsite equipment, is protected against environmental threats. The policy should limit or exclude eating, drinking and smoking in sensitive areas, and prohibit

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			storage of stationery and other supplies posing a fire hazard within computer rooms. 3. Situate and construct IT facilities to minimise and mitigate susceptibility to environmental threats. 4. Define and implement a process to regularly monitor and maintain devices that proactively detect environmental threats (e.g. fire, water, smoke, humidity). 5. Define and implement procedures to respond to environmental alarms and other notifications. Document and test procedures, which should include prioritisation of alarms and contact with local emergency response authorities, and train personnel in these procedures. 6. Compare measures and contingency plans against insurance policy requirements, and report results. Address points of non-compliance in a timely manner. 7. Ensure that IT sites are built and designed to minimise the impact of environmental risks (e.g., theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, and explosives). Consider specific security zones and/or fireproof cells (e.g. locating production and development environments/servers away from each other). 8. Keep the IT sites and server rooms clean and in a safe condition at all time, i.e., no mess, no paper or card council boxes, no filled dustbins, no flammable chemicals or materials
	DS12.5 Physical Facilities Management	• Non-compliance with health and safety regulations • IT systems failure due to improper protection from	1. Define and implement a process to examine the IT facilities' requirement for protection against environmental conditions, power fluctuations and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g. batteries, generators) to

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
		power outages and other facility-related risks • Accidents to staff members	support business continuity planning. 2. Regularly test the uninterruptible power supply's mechanisms and ensure that power can be switched to the supply without any significant effect on business operations. 3. Ensure that the facilities housing the IT systems have more than one source for dependent utilities (e.g. power, telecommunications, water, gas). Separate the physical entrance of each utility. 4. Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and wiring cabinets have access restricted to authorised personnel. Properly protect cabling against damage caused by fire, smoke, water, interception and interference. 5. Ensure that cabling and physical patching (data and phone) are structured and organised. Cabling and conduit structures should be documented, e.g. blueprint building plan and wiring diagrams. 6. Analyse the facilities housing high-availability systems for redundancy and fail-over cabling requirements (external and internal). 7. Define and implement a process that ensures that IT sites and facilities are in on-going compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications. 8. Educate personnel on a regular basis on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents.

AGSA General Control Review Focus Areas	COBIT 4.1 Control Objectives	COBIT 4.1 Risk Drivers	COBIT 4.1 Control Practices
			9. Define and implement a process to record, monitor, manage and resolve facilities incidents in line with the IT incident management process. Make available reports on facilities incidents where disclosure is required in terms of laws and regulations. 10. Define a process to ensure that IT sites and equipment are maintained as per the supplier's recommended service intervals and specifications. The maintenance must be carried out only by authorised personnel. 11. Analyse physical alterations to IT sites or premises to reassess the environmental risk (e.g. fire or water damage). Report results of this analysis to business continuity and facilities management
Maintenance of equipment	DS13.5 Preventive Maintenance for Hardware	• Infrastructure problems that could have been avoided or prevented • Warranties violated due to non- compliance with maintenance requirements	1. Establish a preventive maintenance plan for all hardware, considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors. 2. Review all activity logs on a regular basis to identify critical hardware components that require preventive maintenance, and update the maintenance plan accordingly. 3. Establish maintenance agreements involving third-party access to organisational IT facilities for onsite and offsite activities (e.g. outsourcing). Establish formal service contracts containing or referring to all necessary security conditions, including access authorisation procedures, to ensure compliance with the organisational security policies and standards. 4. In a timely manner, communicate to affected customers and users the expected impact (e.g. performance restrictions) of maintenance activities. 5. Ensure that ports, services, user profiles or other means used for maintenance or diagnosis are active only when required. 6. Incorporate planned downtime in an overall production schedule, and schedule the maintenance activities to minimise the adverse impact on business processes