Tipo:	Norma de IT
Nome:	Resiliência Cibernética
Nível:	Standard Bank de Angola
Classificação:	Apenas para Uso Interno
Responsável:	Director de Engenharia
Responsável pela Custódia:	Gestor do Departamento de Segurança de IT
Comité de Governança:	Comité de Gestão de Risco
Aprovado por:	Comité de Gestão de Risco do Conselho de Administração
Data da Aprovação:	Fevereiro de 2022
Data da Efectividade:	Fevereiro de 2022
Data da Próxima Revisão:	Janeiro de 2024
Contacto:	Abdul Razac Abdul.Razac@standardbank.co.ao +244 924 970 837

Type:	Technology Standard
Name:	Cyber Resilience
Level:	Standard Bank Angola
Classification:	Internal User Only
Owner:	Chief Engineering
Practice Lead:	Manager of IT Security
Governance Committee:	Risk Management Commitee (RMC)
Approved by:	Board Risk Committee (BRC)
Approval Date:	February 2022
Effective Date:	February 2022
Next Review Date:	January 2024
Contacto:	Abdul Razac Abdul.Razac@standardbank.co.ao +244 924 970 837

Classificação
Este documento foi emitido estritamente para efeitos empresariais internos do Standard Bank Angola

Direitos de Autor

Classification
This document was issued strictly for the internal business purposes of Standard Bank Angola

Copyright

1. Introdução

O Standard Bank Angola (SBA) adota princípios sólidos de governança corporativa, um dos quais é o uso e aplicação de políticas e normas que definem e articulam princípios dentro dos quais o Grupo Standard Bank (SBG) opera.

O SBA usa os guias do SBG para definir e articular as normas mínimas de tecnologia, práticas de suporte, bem como as ferramentas, técnicas e processos. Todas as normas de tecnologia são sustentadas pelos valores, código de ética, estratégia de tecnologia e o exercício de bom senso de indivíduos responsáveis.

2. Aplicabilidade

De acordo com o modelo integrado operacional da organização, as normas de tecnologia são adoptadas e executadas nos países membros do Grupo, unidades de negócios e funções corporativas.

Se houver um requisito do SBG que não está refletido na regulamentação locai, os países deverão cumprir com os requisitos locais. De igual forma, os países devem garantir que cumprem com requisitos regulatórios locais específicos.

Caso as actividades de segurança de tecnologias de informação sejam terceirizadas ou coordenadas por terceiros, os termos desta norma serão aplicados.

3. Funções e Responsabilidades relacionadas com a Norma

Para garantir que esta norma seja implementada, executada e cumprida as seguintes responsabilidades foram alocadas:

3.1. O Comité de Gestão de Risco do Conselho de Administração aprova a norma com base na recomendação do Comité de Gestão de Risco, e inclui a mesma no registo de Normas de IT, nomeia o Responsável pela Norma e confirma uma supervisão de governança adequada;

3.2. O Director de Engenharia é o proprietário desta norma e delega a responsabilidade de implementação da mesma ao Gestor do Departamento de Segurança de IT;

3.3. O Gestor do Departamento de Segurança de IT é o responsável pela custódia e avalia qualquer não conformidade material ou conformidade parcial da norma;

3.4. Os órgãos governança de IT supervisionam a aderência as normas de tecnologia do SBA. Usando uma abordagem de aplicação ou explicação (a aplicação de normas é assumida e uma explicação é fornecida para todas as excepções);

1. Introduction

The Standard Bank Angola subscribes to sound corporate governance principles, one of which is the use and application of policies and standards which define and articulate principles within which the SBG Group will operate.

SBA uses technology playbooks to define and articulate minimum SBG standards, supporting practices, tools and techniques. All technology standards are underpinned by the group values, code of ethics, the group technology strategy and the exercise of good judgement by responsible individuals.

2. Applicability

In keeping with the integrated operating company archetype, group technology standards are taken and executed by legal entities, business lines and corporate functions.

If there is an SBG requirement that is not reflected in local regulations, legal entities must comply with the local requirements. Equally, if there are specific local regulatory requirements with which entities must comply, they must ensure they do so.

In the event that technology security activities have been outsourced or are conducted by third parties, the terms of this standard shall be applied.

3. Roles and Responsibilities related to this Standard

In order to ensure that this standard is implemented, executed and complied with the following responsibilities have been allocated:

3.1. The Board Risk Committee approves the standard based on the recommendation of Risk Management Committee, and includes it in the register of IT Standards, appoints the Responsible for the Standard and confirms adequate governance oversight;

3.2. The Chief Engineering is the owner of this standard and delegates the responsibility for the implementation of this standard to the Manager of IT Security;

3.3. The Manager of IT Security is the practice lead and considers any material non-compliance or partial compliance with the standard;

3.4. Technology governing bodies oversee adherence to SBA technology standards. Using an apply or explain approach (the application of standards is assumed, and an explanation is provided for any exceptions);

3.5. O Gestor do Departamento de Segurança de IT garante que a revisão desta norma seja feita sempre que necessário.

4. Princípios Padrão

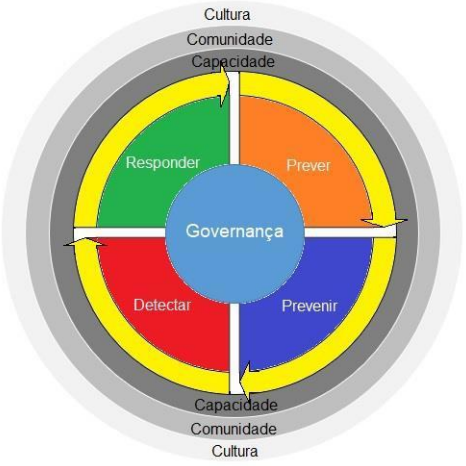
O Departamento de Segurança de IT do Banco é responsável pelo desenvolvimento, implementação e manutenção do programa de resiliência cibernética. O programa está alinhado à estratégia de tecnologia do SBG, matrix de ameaça, apetite ao risco e a framework de segurança tecnológica, garantindo a conformidade com a legislação e os regulamentos relevantes. A framework é necessária para controlar como o Banco protege seus ativos tecnologicos, que incluem sistemas em produção, sistemas em desenvolvimento e sistemas alojados em infraestruturas de terceiros de forma sistemática e consistente.

A segurança de IT do Banco é mandatada para estabelecer e manter uma cultura de segurança em todo o Banco, garantir um ambiente de controle robusto, garantindo que os requisitos das partes interessadas para a proteção de dados sejam atendidos continuamente, com foco na confidencialidade (o risco de acesso não autorizado a sistemas de dados e tecnologia), integridade (risco de manipulação de dados) e disponibilidade (risco de indisponibilidade de sistemas de dados e tecnologia quando necessário).

Essa norma informa e efectiva à direção do Banco em relação a gestão da resiliência cibernética. Os princípios de gestão de resiliência cibernética de tecnologias abaixo são aplicados de maneira proporcional ao tamanho e complexidade do país membro do Grupo, unidade de negócio ou função corporativa.

Caso um dos princípios abaixo não seja aplicado ao nível apropriado, o Gestor do Departamento de Segurança de IT (em conjunto com o Director de Engenharia) tem o mandato de intervir e remediar a seu critério.

A framework de segurança de IT é representada no diagrama abaixo, assim como os princípios de cada componente:



3.5. The Manager of IT Security ensures that a review of this standard is conducted as and when required.

4. Standard Principles

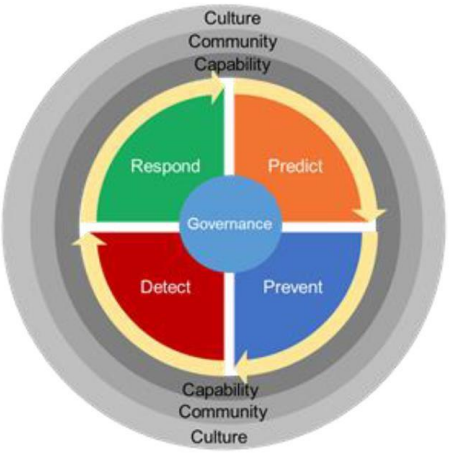
The bank technology security function is responsible for developing, implementing, and maintaining the cyber resilience programme. The programme is aligned to the SBG technology strategy, threat profile, risk appetite and the technology security framework whilst ensuring compliance with relevant legislation and regulations. The framework is necessary to govern how the bank protects its technology assets which include systems in production, systems under development and systems hosted by third parties in a systematic and consistent manner.

The bank technology security function is mandated to establish and uphold a culture of security across the SBG, provide assurance on a robust control environment, ensure that stakeholder requirements for the protection of data are continually met, focusing on confidentiality (the risk of unauthorised access to data and technology systems), integrity (the risk of data being manipulated) and availability (the risk of data and technology systems being unavailable when needed).

This standard articulates and gives effect to the Bank direction regarding the management of technology cyber resilience. The technology cyber resilience management principles below are applied in such a way that is commensurate with the size and complexity of the legal entity, business line or corporate function.

Should any of the principles below not be applied at the appropriate level, the Manager of IT Security (in conjunction with the Chief Engineering) has the mandate to intervene and remediate at their discretion.

The technology security framework is depicted in the diagram below and the principles for each component are articulated below:



4.1. Governança

4.1.1. A framework de segurança de IT informa a forma como o Banco determina seus objetivos de resiliência cibernética e tolerância a riscos cibernéticos, bem como identificar, mitigar e gerir efectivamente riscos cibernéticos.

4.1.2. A framework abrange pessoas, processos e tecnologia e alinha-se às estratégias de gestão de riscos corporativos, bem como as normas internacionais e nacionais.

4.1.3. A framework define claramente as funções e responsabilidades necessárias para gerir o risco cibernético e permite a medição e o relatório precisos do estado do controlo de segurança cibernética.

4.1.4. A framework inclui a gestão de riscos cibernéticos apresentados por provedores de serviços e terceiros.

4.1.5. A adequação da framework de segurança de IT é avaliada e medida anualmente por meio de testes e análises independentes realizados por entidades externas qualificadas.

4.1.6. O investimento em resiliência cibernética é apropriado em valor e priorização e está claramente articulado nos níveis relevantes da organização. O impacto de qualquer *trade-off* é identificado e, quando necessário, escalado.

4.2. Identificação / Previsão

4.2.1. Os sistemas de suporte a operações críticas (sistemas voltados para o cliente / que afetam o cliente) são protegidos contra riscos numa ordem de prioridade.

4.2.2. Os sistemas críticos são determinados com base no perfil de ameaças e no risco cibernético.

4.2.3. Um inventário de activos, configurações do sistema e direitos de acesso são mantidos.

4.2.4. A resiliência cibernética leva em consideração o risco representado pelas interconexões com outros sistemas internos e externos.

4.3. Proteção / Prevenção

4.3.1. Controles de proteção adequados minimizam a probabilidade e o impacto do ataque cibernético.

4.3.2. Os sistemas são projetados para serem resistentes a ataques cibernéticos e incidentes.

4.1. Governance

4.1.1. The technology security framework articulates how the Bank determines its cyber resilience objectives and cyber risk tolerance, as well as how to effectively identify, mitigate, and manage cyber risks.

4.1.2. The framework covers people, process and technology and aligns to enterprise risk management strategies as well as international and national standards.

4.1.3. The framework clearly defines roles and responsibilities for managing cyber risk and allows for the accurate measurement and reporting of the status of cyber security control status.

4.1.4. The framework includes the management of cyber risks posed by service providers and third parties.

4.1.5. The adequacy of the technology security framework is assessed and measured annually through independent testing and reviews carried out by qualified third parties.

4.1.6. The investment in cyber resilience is appropriate in value and prioritisation and is clearly articulated at the relevant levels in the organisation. The impact of any trade-off is identified and where necessary escalated.

4.2. Identification / Prediction

4.2.1. Systems supporting critical operations (customer facing/customer affecting systems) are protected against compromise in order of priority.

4.2.2. Critical systems are determined based on threat profile and cyber risk.

4.2.3. An inventory of assets, system configurations and access rights are maintained.

4.2.4. 4.2.4 Cyber resilience considers the risk posed by interconnections with other internal and external systems.

4.3. Protection / Prevention

4.3.1. Appropriate protective controls minimise the likelihood and impact of cyberattack.

4.3.2. Systems are designed to be resilient to cyber-attacks and incidents.

4.3.3. Um forte ambiente de controle de tecnologia é mantido para oferecer suporte à resiliência cibernética, incluindo proteção de dados, gestão de alterações e requisitos mínimos de segurança.

4.3.4. O acesso físico e lógico a aplicações de negócios, sistemas de informação, redes e dispositivos de computação deve ser concedido com base numa necessidade e de acordo com a política de gestão de acesso lógico.

4.3.5. O acesso privilegiado ao sistema é protegido por fortes controles de autenticação, limitado a uma equipa autorizada específica e registado para atividades maliciosas.

4.3.6. Todos os funcionários recebem formação adequada e são consciencializados sobre a matéria, com base em seu perfil de risco.

4.3.3. A strong technology control environment is maintained to support cyber resilience including data protection, change management and minimum security requirements.

4.3.4. Physical and logical access to business applications, information systems, networks and computing devices must be granted on a need-to-basis and in accordance with the logical access management policy.

4.3.5. Privileged system access is protected through strong authentication controls, is limited to specific authorised staff and is logged for malicious activity.

4.3.6. All staff are provided with appropriate training and awareness based on their risk profile.

4.4. Detecção

4.4.1. Os sistemas são monitorizados continuamente (em tempo real ou quase em tempo real) para detectar atividades e eventos anômalos.

4.4.2. Controlos críticos de segurança são monitorizados continuamente quanto a falhas ou excepções.

4.4.3. Os recursos de monitorização e detecção devem facilitar o processo de resposta a incidentes cibernéticos e apoiar a recolha de informações para o processo de investigação forense.

4.4. Detection

4.4.1. Systems are continuously monitored (in real time or near real time) to detect anomalous activities and events.

4.4.2. 4.4.2 Critical security controls are continuously monitored for failure or exceptions.

4.4.3. 4.4.3 Monitoring and detection capabilities should facilitate the cyber incident response process and support information collection for the forensic investigation process.

4.5. Resposta e Recuperação

4.5.1. O IT é o responsável pela custódia e alinhado com o BCM deverá ter planos de resposta definidos para todos os riscos cibernéticos identificados.

4.5.2. Caso a reposição dos serviços não seja possível, existem planos de contingência, incluindo a reversão para processos manuais.

4.5.3. Os planos de resposta são testados e actualizados regularmente para incluir novas ameaças.

4.5.4. Os sistemas são projectados para facilitar a resposta a incidentes, incluindo o registo de eventos de sistemas e ações do utilizador.

4.5.5. Os backups de dados estão disponíveis de acordo com os objetivos de recuperação, incluindo dados de terceiros.

4.5. Response and Recovery

4.5.1. IT is the sole custodian and should have response plans defined for all identified cyber risks aligned with BCM.

4.5.2. In the event that resumption of services is not possible, there are contingency plans, including reverting to manual processes.

4.5.3. Response plans are regularly tested and updated to include new threats.

4.5.4. Systems are designed to facilitate incident response, including logging of system events and user actions.

4.5.5. Backups of data are available in line with recovery point objectives, including data at third parties.

4.6. Capacidade de Teste

4.6.1. O programa de resiliência cibernética é testado anualmente para validar a sua eficácia.

4.6.2. Os testes incluem campanhas de phishing, avaliações de vulnerabilidades, criação de perfis de risco, simulações com a equipa especializada (Red Team) do Grupo e testes de penetração.

4.7. Consciência / Comunidade

4.7.1. A informação sobre ameaças cibernéticas é recolhida de várias fontes para prever possíveis ameaças a operações críticas (por exemplo, assinaturas de inteligência de ameaças, grupos de partilha de informações locais e globais etc.).

4.7.2. A equipa de Segurança de IT local recebe do Centro de Operações de Segurança Cibernética (CSOC) a informação sobre a análise de ameaças, e tem a responsabilidade de mitigar os riscos cibernéticos.

4.7.3. As lições apreendidas sobre informação sobre ameaças são usadas para definir melhorias no programa de resiliência cibernética.

4.8. Aprendizagem e Evolução / Cultura

4.8.1. A análise da causa de incidentes é realizada após a recuperação dos incidentes e as lições aprendidas informam a prioridade das iniciativas de resiliência cibernética.

4.8.2. As competências de segurança são desenvolvidas continuamente para acompanhar as últimas tendências, ferramentas e técnicas de tecnologia usadas pelos invasores.

4.8.3. A resiliência cibernética é medida usando métricas e modelos de maturidade apropriados.

5. Acção Disciplinar

A adoção dos princípios desta norma é obrigatória e a não conformidade relevante será submetida ao Diretor de Sistemas de Informação pelo Gestor do Departamento de Segurança de IT. Negligência ou má conduta podem resultar na instauração de procedimentos disciplinares.

4.6. Testing Capability

4.6.1. The cyber resilience programme is annually tested to validate effectiveness.

4.6.2. Testing includes mock phishing campaigns, vulnerability assessments, threat profiling, red team exercises and penetration testing.

4.7. Situational Awareness / Community

4.7.1. Cyber threat intelligence is gathered from a number of sources to predict possible threats to critical operations (for example threat intelligence subscriptions, local and global information sharing groups, etc.)

4.7.2. The local IT Security Team receives from Cyber Security Operations Centre (CSOC) the threat intelligence information, with the responsibility to mitigate cyber risks.

4.7.3. Learnings from threat intelligence are used to define improvements in the cyber resilience programme.

4.8. Learning and evolving/culture

4.8.1. Analysis of the root-cause is conducted after recovery from incidents and lessons learnt inform the priority of cyber resilience initiatives.

4.8.2. Security skills are continuously developed to keep up with the latest technology trends, tools and techniques used by attackers.

4.8.3. Cyber resilience is measured using appropriate metrics and maturity models.

5. Disciplinary Action

Compliance with the principles in this standard is mandatory and any material non-compliance will be referred to the Chief Engineering by the Manager of IT Security. Negligence or misconduct could result in disciplinary procedures being instigated.

6. Informação Relacionada

Esta seção inclui informações relacionadas que os responsáveis pela presente norma precisam conhecer para cumprir totalmente com a mesma.

Tipo	Documento / Autoridade	Referência
Norma Internacional	ISO/IEC 27001; 2013; ISO/IEC 27002; 2013	ISO/IEC 27001 international standard CoBIT
Norma Internacional	CPMI-IOSCO	Guidance on cyber resilience for financial market infrastructures
Política	Information risk policy	Group Operational Risk
Política	Logical Access Management Policy	Group Operational Risk
Playbooks	SBG Technology Playbooks	SBG Technology Toolbox

6. Related Information

This section includes related information that the owners of the standard needs to know in order to fully comply with this standard.

Type	Document / Authority	Reference
International Standard	ISO/IEC 27001; 2013; ISO/IEC 27002; 2013	ISO/IEC 27001 international standard CoBIT
International Standard	CPMI-IOSCO	Guidance on cyber resilience for financial market infrastructures
Policy	Information risk policy	Group Operational Risk
Policy	Logical Access Management Policy	Group Operational Risk
Playbooks	SBG Technology Playbooks	SBG Technology Toolbox

7. Administração da Norma

Responsável pela Custódia	
Nome:	Castro Marques
Título:	Gestor
Departamento:	Segurança de IT
Telefone:	+244 924 971 551
Email:	Castro.Marques@standardbank.co.ao

Responsável	
Nome:	Abdul Razac
Título:	Director
Departamento:	Direcção de Sistemas de Informação
Telefone:	+244 924 970 837
Email:	Abdul.Razac@standardbank.co.ao

7. Administration

Practice Lead	
Name:	Castro Marques
Title:	Manager
Department:	IT Security
Telephone:	+244 924 971 551
Email:	Castro.Marques@standardbank.co.ao

Accountable	
Name:	Abdul Razac
Title:	Chief Engineering
Department:	Information Technology
Telephone:	+244 924 970 837
Email:	Abdul.Razac@standardbank.co.ao

8. Histórico de Revisão

Versão:	v1.0
Propósito da Revisão:	Adopção da Norma
Data da Revisão:	Abril de 2020
Sumário dos Pontos Chaves da Revisão:	N/A

8. Revision History

Version:	v1.0
Purpose of Review:	Adoption of the Standard
Date of Review:	April 2020
Summary of Review Key Points:	N/A

Versão:	v2.0
Propósito da Revisão:	• Actualização do Responsável • Actualização da Data de Validade
Data da Revisão:	Fevereiro de 2022
Sumário dos Pontos Chaves da Revisão:	N/A

Version:	v2.0
Purpose of Review:	• Update the Responsible • Update the Expiration Date
Date of Review:	February 2022
Summary of Review Key Points:	N/A