IT RISK MANAGEMENT POLICY

Type of policy:	Information Technology Policy – Risk Management
Executive summary:	The scope of this policy is applicable to Constantia Risk and Insurance Holdings (Pty) Limited and Constantia Life Limited
Area of governance:	Compliance, Legal and Risk
Approving authority:	The Board of Constantia Risk and Insurance Holdings (Pty) Limited
Group Exco support	Operations Manager
Responsible department:	Operations
Date of approval:	September 2023
Review frequency:	Annually
Date of next review:	September 2024
Version:	V2.0
Draft resolution:	The Constantia Group of insurance companies recognises the value as well as the risks associated with outsourcing any of its activities. Whilst legislative requirements form the foundation of this policy, this statement is more practical in its application and utilizes basic business principles and practices as its overall primary standard. This policy has been approved by the Board of Directors of each of the above listed insurers who have duly authorised the signatories to this document. The Board is required to approve the policy in line with regulations with specific reference to Governance and Operational Standards For Insurers (GOI 3)

SIGNED AT Kyalami ON THE DAY 17th OF October 2024

Themba Baloyi

Themba Baloyi (Oct 17, 2024 08:47 GMT+2)

TP BALOYI
CHAIR OF THE BOARD
INDEPENDENT NON-EXECUTIVE

SIGNED AT Cape Town ON THE DAY 2nd OF October 2024

Lu[illegible] Mulaudzi (Oct 2, 2024 18:18 GMT+2)

LK MULAUDZI
CHAIR OF THE JOINT AUDIT & RISK COMMITTEE
INDEPENDENT NON-EXECUTIVE

Table of Contents

1. APPLICATION

1.1. This policy applies to all employees, and is deemed to include:

- Non-Executive Directors
- Executive Directors and Senior Management
- Managers and Senior Officials
- Permanent staff
- Temporary staff

2. POLICY STATEMENT

2.1. This IT Risk Management Policy outlines the framework and guidelines for identifying, assessing, mitigating, and monitoring information technology (IT) risks within the Company. The policy aims to ensure the confidentiality, integrity, availability, and compliance of the IT systems and data by establishing a structured approach to managing IT risks.

2.2. Effective IT risk management is essential for safeguarding the Company's IT assets, reputation, data, and compliance with regulatory requirements. This policy provides the framework for IT risk management, ensuring that the Company remains resilient and secure in the face of evolving threats and challenges.

2.3. Threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the security interests of the Company.

2.4. The Company‘s risk can include many types of risks (e.g. program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk). Security risk related to the operations and use of information systems is just one of many components of organisational risk that senior key persons/executives address as part of their ongoing risk management responsibilities.

3. PURPOSE

3.1. The purpose of this policy is to:

3.1.1. ensure that the Company meets its obligations in terms of the Insurance Authorities’ standards;
3.1.2. define the responsibilities and roles of individuals involved in IT risk management;
3.1.3. establish a systematic process for identifying, assessing, and prioritising IT risks;
3.1.4. define acceptable risk tolerance levels for the Company;
3.1.5. ensure the implementation of appropriate risk mitigation and control measures; and
3.1.6. establish procedures for ongoing monitoring and reporting of IT risks.

3.2. The Group has established a Work-from-Home Policy which sets out the working environment of the Group and therefore this policy has been aligned with the working environment.

4. SCOPE

4.1. This policy applies to all persons with oversight and responsibilities for risk management and IT assets, systems, acquisitions, security, services, monitoring, implementation and processes within the Company, including but not limited to hardware, software, networks, data, cyber-security, internal controls/audits and third-party service providers.

4.2. This policy be read with the **GOI3f. CRIH IT Policy-Oct 2023 v7.0**.

5. POLICY COMPONENTS

5.1. Roles and Responsibilities

5.1.1. Operations Manager (which duties include IT responsibilities)

- The Operations Manager is responsible for overseeing the Company's IT risk management program;
- The Operations Manager must ensure that adequate resources are allocated to manage IT risks effectively; and
- The Operations Manager, together with the Board, is the final authority in approving risk acceptance and decisions that exceed established thresholds.

5.1.2. IT Risk Management Team

- The IT risk management team is responsible for the day-to-day management of IT risks, including risk identification, assessment, mitigation and monitoring;
- The team comprises the Operations Manager, compliance officers, outsourced IT service provider and relevant department heads; and
- Team members should have the necessary expertise and training to perform their roles effectively.

5.1.3. Department Heads

- Department heads are responsible for identifying and reporting IT risks within their respective areas of responsibility; and
- They should collaborate with the IT Risk Management Team to address and mitigate identified risks.

5.2. Risk Assessment Methodology

5.2.1. The Company uses risk assessment to determine the extent of the potential threat, and the risk associated with an Information Asset. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Constantia's risk assessment is conducted at least annually or whenever any significant change occurs in the Company. Information Technology Officer / Manager and all the new identified threats and vulnerabilities are taken into consideration for the treatment.

Previously identified (existing) risks are revisited to see if the controls applied are sufficient or need further treatment.

5.3. Risk Identification

5.3.1. Risk Identification Methodology

The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

- **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, Constantia's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting Constantia's mission.

- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorised disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardising of national security to the disclosure of Privacy Act data. Unauthorised, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against Constantia.

5.3.2. Risk Register

- A central risk register will be maintained to document and track all identified IT risks; and

- The register should include a description of the risk, potential impact, likelihood, and the responsible party for mitigation.

5.3.3. Risk Assessment

- Risks will be assessed based on potential threats and vulnerabilities and their impact on confidentiality, integrity, availability, and compliance;
-
- Risks to information assets are assessed based on their potential impact on confidentiality, integrity, and availability (C, I, A). Each type of risk is calculated by multiplying its impact percentage by its probability percentage:
  - Confidentiality Risk = Impact of Confidentiality % * Probability of Confidentiality %
  - Availability Risk = Impact of Availability % * Probability of Availability %
  - Integrity Risk = Impact of Integrity % * Probability of Integrity %

The combined risk is then calculated using these individual assessments;

- To determine the probability that a potential vulnerability may be exploited, consider the following factors:

  - Threat-source motivation and capability
  - Nature of the vulnerability
  - Existence and effectiveness of current controls

The probability is then rated on a scale of very high, high, medium, low, or very low, as detailed in the accompanying table:

Rating	Description	Probability of Occurrence
1	Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will
2	Unlikely	Not expected, but there's a slight possibility it may occur at some time.
3	Possible	The event might occur at some time as there is a history of casual occurrence at the similar institutions
4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence at similar institutions.
5	Almost certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at similar institutions.

- The adverse impact of losing confidentiality, integrity, or availability of an information asset is assessed based on the asset's sensitivity and required protection level. Information asset owners determine the impact level, which is rated on a scale from 1 to 5. The impact is evaluated from five perspectives: Financial Impact, Client & Staff Health & Safety, Business Interruption, Reputation & Image, and Corporate Objectives as set out in the table below:

Rating	Description	Financial Impact	Clients & Staff Health & Safety	Business Interruption	Reputation & Image	Corporate Objectives
1	Very low	Minimal financial loss; Less than R300,000	No or only minor personal injury: First Aid needed but no days lost	Negligible; Critical System unavailable for less than one hour	Negligible impact	Resolved in day-to-day management
2	Low	R300,000 to R2M; not covered by insurance	Minor injury. Medical treatment & some days lost	Inconvenient. Critical systems unavailable for several hours	Adverse local media coverage only	Minor impact
3	Moderate	R2M to R5M; not covered	Injury. Possible hospitalisation	Client dissatisfaction; Critical systems	Adverse capital city	Significant impact

Rating	Description	Financial Impact	Clients & Staff Health & Safety	Business Interruption	Reputation & Image	Corporate Objectives
4	High	R5M to R10M; not covered by insurance	Single death &/or long-term illness or multiple serious injuries	Critical systems unavailable for 1 day or a series of prolonged	Adverse and extended national media coverage	Major impact
5	Very High	Above R10M; not covered by insurance	Fatality(ies) or permanent disability or ill-health	Critical systems unavailable for more than a day (at a crucial time)	Demand for government inquiry	Disastrous impact

- A risk impact matrix will be used to categorise and prioritise risks as set out in the tables below:

LIKELIHOOD	IMPACT					
		1	**2**	**3**	**4**	**5**
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Qualitative Values	Semi-Quantitative Values	Description
Very High	21-25	Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on Constantia's operations, assets, individuals, other associated companies
High	16-20	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on Constantia's operations, assets, individuals, other associated companies
Moderate	10-15	Moderate risk means that a threat event could be expected to have a serious adverse effect on Constantia's operations, assets, individuals, other associated companies
Low	6-9	Low risk means that a threat event could be expected to have a limited adverse effect on Constantia's operations, assets, individuals, other associated companies

Qualitative Values	Semi-Quantitative Values	Description
Very Low	1-5	Very low risk means that a threat event could be expected to have a negligible adverse effect on Constantia's operations, assets, individuals, other associated companies

- Combined Risk Score is a weighted average considering all conditions from the impact assessment, rather than a simple average of confidentiality (C), integrity (I), and availability (A) values. To calculate the Combined Risk (CR), both the average and worst case are used to balance out extreme values.

- The formula is:

  CR = (Average + Worst Case) / 2

  Where:
  Average = (C + I + A) / 3
  Worst Case = Highest Risk value among C, I and A

5.3.4. Risk Tolerance

- Risks will be assessed based on potential threats and vulnerabilities and their impact on confidentiality, integrity, availability, and compliance.

5.4. Risk Methods

5.4.1. Risk Mitigation Strategies

- To limit the risk and minimise the adverse impact of threats on assets, it is important to implement controls such as anti-virus servers. While installing an anti-virus server in Constantia reduces the risk of known virus attacks, it does not guarantee complete protection;

- Regular updates of virus definitions and frequent backups further mitigate the risk and potential effects of virus attacks, ensuring better security for the assets;

- Mitigation strategies will be developed for high and medium-risk items; and

- Strategies may include implementing security controls, conducting training, or creating backup systems.

5.4.2. Risk Transfer

- Risk Transfer involves shifting the risk to another party, such as by purchasing insurance or outsourcing to third-party vendors through contracts. This can include maintenance contracts or agreements to keep spare hardware available.

5.4.3. Risk Avoidance

- Risk Avoidance entails eliminating the risk by removing its cause or consequences. For example, an outdated system that cannot be patched (e.g., Windows 98) can be taken offline to prevent it from being compromised.

5.4.4. Risk Acceptance

- Reducing risks to an acceptable level might not always be possible or financially feasible. In such cases, it may be necessary to knowingly accept the risk or implement controls to lower it to an acceptable level. Prioritizing business requirements while safeguarding information is essential, and sometimes accepting certain risks is necessary to ensure that business needs are met;

- Risks that fall within predefined acceptable risk tolerance levels may be accepted without further mitigation; and

- Senior management, including the Operations Manager, will review and approve risk acceptance decisions.

5.4.5. Residual Risk

- Residual Risk refers to the remaining risks that exceed the acceptable threshold even after risk treatment measures have been implemented. These risks are presented to and accepted by the management committee, documented, and approved by management. Residual risks are reviewed whenever the risk assessment is updated, or a new threat is identified.

5.5. Threats and Vulnerabilities

5.5.1. Threat Identification

- A threat is the potential for a particular threat-source to successfully exploit a vulnerability. A threat-source can be:

    - intent and method for intentional exploitation of a vulnerability.
    - situation and method that may accidentally trigger a vulnerability.

- A vulnerability is a weakness that can be exploited or triggered. Without a vulnerability, a threat-source does not present a risk. To determine the likelihood of a threat, consider threat-sources, potential vulnerabilities, and existing controls.

- The goal is to identify potential threat-sources and compile a threat statement for the information asset. A threat-source is any circumstance or event with the potential to harm an information asset, including:

    - Natural Threats: Floods, earthquakes, tornadoes, etc.
    - Human Threats: Unintentional acts (e.g., data entry errors) or deliberate actions (e.g., network attacks, unauthorised access).
    - Environmental Threats: Long-term power failures, pollution, chemical leaks, etc.

- For example, while natural floods might be unlikely in a desert, environmental threats like a bursting pipe can still cause significant damage.

- Human threat-sources are driven by motivation and resources, making them potentially dangerous. Common human threats include malicious attacks and negligence. Reviewing historical incidents, security reports, and interviewing relevant personnel helps identify human threat-sources and their potential methods of attack.

5.5.2. Vulnerability Identification

- A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that can be accidentally triggered or intentionally exploited, leading to a security breach or policy violation.

- To analyse the threat to an information asset, it is essential to examine the vulnerabilities within the system environment. The objective is to create a list of these vulnerabilities that could be exploited by potential threat-sources.

- Refer to **Annexure A** for a list of vulnerabilities.

5.5.3. Control Analysis

- The aim of control analysis is to evaluate existing or planned controls to reduce or eliminate the likelihood of a threat exploiting a system vulnerability. This step assesses the overall likelihood that a vulnerability will be exercised, considering current or planned controls.

- Control Methods:

    - Technical Controls: Safeguards in hardware, software, or firmware (e.g. access control, identification and authentication, encryption, intrusion detection).
    - Non-technical Controls: Management and operational safeguards (e.g. security policies, operational procedures, personnel, physical, and environmental security).

- Control Categories:

    - Preventive Controls: Inhibit security policy violations (e.g. access control enforcement, encryption, authentication).
    - Detective Controls: Alert to violations or attempted violations (e.g. audit trails, intrusion detection, checksums).

- Effective implementation of these controls is crucial for mitigating risk, identified through assessing deficiencies in current or planned controls.

5.6. Ongoing Monitoring

5.6.1. Continuous monitoring

- IT risks will be continuously monitored to identify emerging threats and vulnerabilities; and

- Monitoring will include regular security assessments, vulnerability scans and compliance checks.

5.6.2. Reporting

- Regular reports on IT risk status and mitigation efforts will be provided to senior management and relevant stakeholders; and
- Critical risk issues will be reported promptly to facilitate timely action.

5.7. Review and Improvement

5.7.1. Periodic reviews

- The IT risk management policy and procedures will be reviewed at least annually or as needed to ensure their effectiveness; and
- Updates will be made to reflect changes in technology, regulations, or the Company's risk landscape.

5.7.2. Lessons learned

- Lessons learned from risk incidents will be documented and used to improve the IT risk management process.

6. REFERENCES TO IT RISK STANDARDS

6.1. Insurance Authority: The Financial Sector Conduct Authority (FSCA) and Prudential Authority (PA) under section 60 (3) (b) (iv) and section 42 (b) (iv) of the Joint Standard 1 of 2023: Information Technology (IT) Governance and Risk Management

7. CLOSING

7.1. The Group may amend this Policy from time to time and shall be reviewed no less than once within each calendar year cycle. Reasonable efforts will be made to inform all employees of any amendments to the policy. Non-compliance with this policy will be dealt with as described in the Disciplinary Code of Conduct.

8. REVISION HISTORY

Version	Date	Author	Organisation	Revision
1.0	September 2023	R. Kok	Ops Manager	Created policy
2.0	May 2024	R. Kok	Ops Manager	Review and align with FSCA / PA Standards

9. ANNEXURE A

Threat source and their motivations

Threat-Source	Motivation	Threat Actions
Hacker, cracker Challenge	- Ego - Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal Destruction of information	- Destruction of information - Illegal information disclosure - Monetary gain - Unauthorised data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, • impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	- Blackmail - Destruction - Exploitation - Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (Companies, foreign governments, other government interests)	- Competitive advantage - Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (Poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	- Curiosity - Ego - Intelligence - Monetary gain - Revenge - Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Vulnerabilities

Vulnerability	**Threat-Source**	**Threat Action**
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialling into the Company's network and accessing Company proprietary data
Company firewall allows inbound telnet, and guest ID is enabled on XYZ server	Unauthorised users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the guest ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorised access to sensitive system files based on known system vulnerabilities
Data centre uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data centre.

CRIH IT Risk Management Policy

Final Audit Report 2024-10-17

Created:	2024-10-02
By:	Rene Kok (renek@conduitcapital.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAAjXB-HHJezU1AvVN2QbM0VN39eEssx-Cx

"CRIH IT Risk Management Policy" History

Document created by Rene Kok (renek@conduitcapital.co.za)
2024-10-02 - 12:48:42 PM GMT- IP address: 41.193.162.150

Document emailed to Themba Baloyi (thembab@gmail.com) for signature
2024-10-02 - 12:48:47 PM GMT

Document emailed to Lusani Mulaudzi (lusani.mulaudzi@gmail.com) for signature
2024-10-02 - 12:48:47 PM GMT

Email viewed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
2024-10-02 - 12:51:38 PM GMT- IP address: 66.249.93.165

Document e-signed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
Signature Date: 2024-10-02 - 4:18:31 PM GMT - Time Source: server- IP address: 41.147.3.30

Email viewed by Themba Baloyi (thembab@gmail.com)
2024-10-02 - 7:45:59 PM GMT- IP address: 104.28.82.90

Email viewed by Themba Baloyi (thembab@gmail.com)
2024-10-09 - 7:55:03 PM GMT- IP address: 146.75.224.3

Email viewed by Themba Baloyi (thembab@gmail.com)
2024-10-17 - 0:23:21 AM GMT- IP address: 172.224.231.139

Document e-signed by Themba Baloyi (thembab@gmail.com)
Signature Date: 2024-10-17 - 6:47:50 AM GMT - Time Source: server- IP address: 196.192.169.198

Agreement completed.
2024-10-17 - 6:47:50 AM GMT