Risk Management Standard

BITS Technology Group Pty Ltd

Version 1.0

Published: 20/02/2025

Contents

Purpose and Scope

Purpose of this document

Risk management is an integral part of better practice in business management and effective corporate governance.

Our aim is to use risk management to manage threats and to leverage opportunities so we can:

- protect, sustain, and create long-term shareholder value, and
- minimise the effects of uncertainty on BITS Technology Group achieving its strategic objectives.

The purpose of this document is to outline the minimum requirements and responsibilities for managing risk and the core components of the 'BITS Technology Group Risk Management System' ('RMS').

Scope

This and the other documents comprising the RMS apply to all directors and employees of BITS Technology Group, as well as to our contractors and their employees.

Guiding Principles

The purpose of developing and working within a RMS and adopting the processes detailed in this Risk Standard are to:

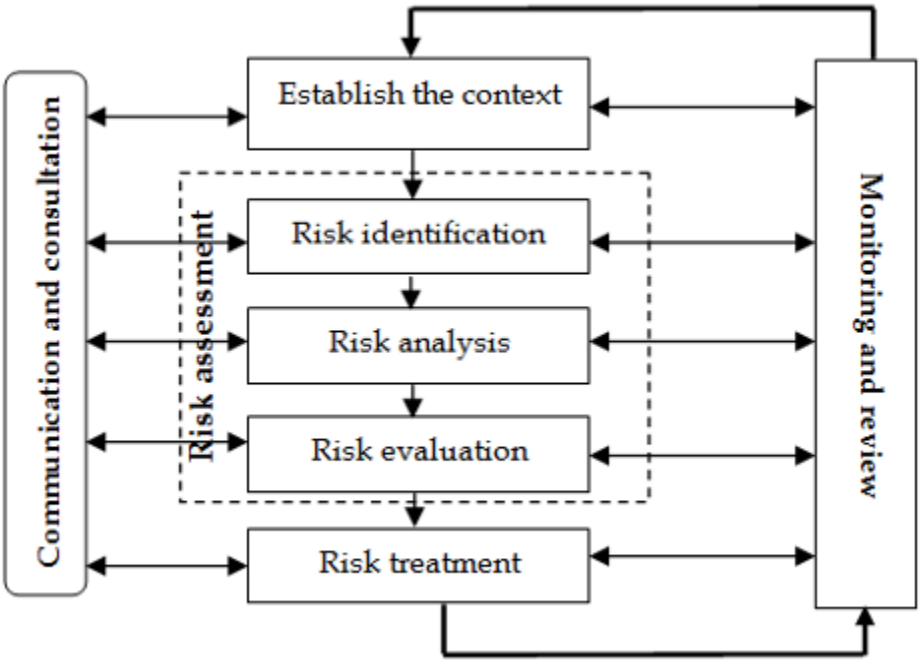
- Safeguard internal and external stakeholders from unacceptable activities and decisions
- Allow the company Directors and management to review and monitor the risk profile of BITS Technology Group through defined risk information channels
- Provide a framework for all employees to identify, manage and make decisions about risk based on both risk and reward
- Provide guidance on management systems to be used to respond to and escalate risks as appropriate.

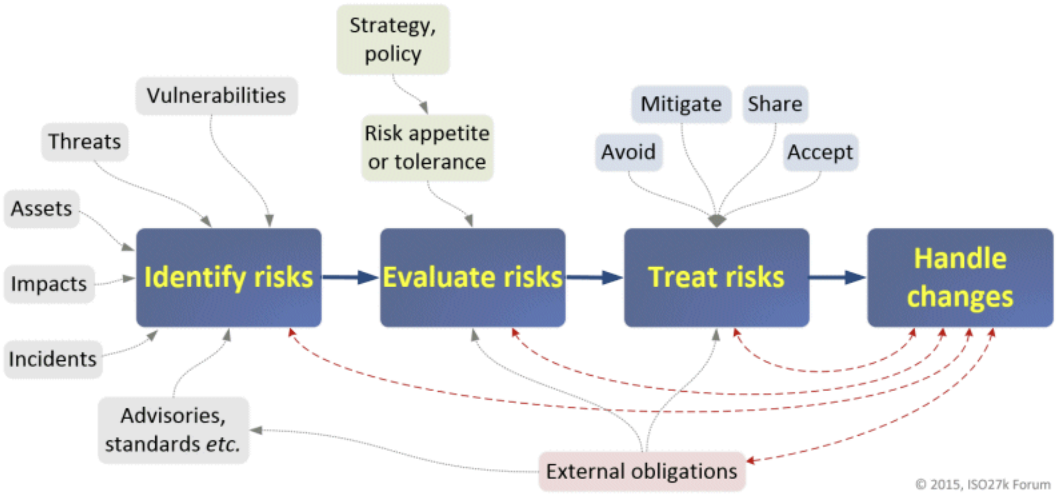
The RMS

The RMS comprises a hierarchy of documents and processes which are depicted in Figure 1. An overview of each of these documents and the role they play in the RMS is provided as Appendix 1 to this document.

Version 1.0
Published: 13/05/2025

Figure 1 – BITS Technology Group RMS





This Risk Standard is the principle document that provides the overarching approach and processes for the management of risk in BITS Technology Group.

Risk Hierarchy

Establishing a hierarchy for risk information (Strategic and Operational risks) ensures that risks are managed at the most appropriate level in the organisation. The hierarchy includes:

- **Strategic**: Risks owned by members of the Exec Team. Should they eventuate, they will impact BITS Technology Group's vision, goals, and/or strategic objectives

- **Operational**: Risks that exist within a stream or functional area of BITS Technology Group such as Finance, Operations, Supply Chain etc.

Risk Assessment Triggers

The Risk Assessment Process can be triggered by any number of business events. The following items are examples of events which may trigger a risk assessment:

- A material change to BITS Technology Group business. This may include: change to business lines/products, geographic operational changes, key personnel change, financial change etc.
- A significant internal project or a significant change in a project.
- A change with a supplier. This may include new suppliers, renewal of supplier contracts, new supply chain requirement.
- A data breach, cyber attack, credible threat intelligence.
  This could originate from Internal, a 3rd party, a supplier or a client.
- Government or regulatory change or change in legal obligations.
- A material change to the ISMS internal or external issues or interested parties.
- Annual risk assessment of the ISMS.
- A Change in the ISMS Controls or material change in the ISMS Scope.

Risk Assessment Process

This section provides the key processes and principles to identify, assess, treat and manage risk in BITS Technology Group.

Establish context

Before assessing uncertainties that could impact our objectives, it is important to recognise the context in which BITS Technology Group operates. To do this we identify and consider the:

- Internal and external environment in which our organisation operates and the factors that have a critical impact on the achievement of our strategic objectives
- Goals and objectives of the risk management activity including how it is to be undertaken and what is in scope.

Identify Risks

The first stage of the process is to Identify potential information risks. Several factors or information sources feed-in to the Identify step, including:

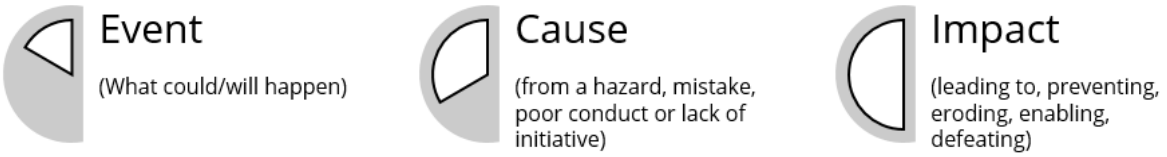
- Vulnerabilities are the inherent weaknesses within our facilities, platforms, technologies, processes, suppliers (including information risk management itself), people and relationships;
- Threats are the actors (insiders and outsiders), natural events, geopolitical events that might cause incidents if they acted on vulnerabilities causing impacts;
- Assets are, specifically, information assets, in particular valuable information content but also, to a lesser extent, the related storage vessels, computer hardware etc.;

- Impacts are the harmful effects or consequences of incidents and calamities affecting assets, damaging the organisation and its business interests, and often third parties;
- Incidents range in scale from minor, trivial or inconsequential events up to calamities, disasters and outright catastrophes;
- Advisories, standards etc. refers to relevant warnings and advice put out by myriad organisations such as AusCERT, ACSC, ISO/IEC, industry specific special interest groups, technology vendors plus information risk and security professionals etc.

The aim of this step is to identify uncertainties that might create, enhance, prevent, degrade, accelerate or delay the achievement of our objectives. This step requires identification and documentation of the risks to be managed, their causes and sources, and potential impacts / consequences. All risks should be captured using the Risk Register.

Clear articulation of the risk title sets the premise for the remainder of the risk assessment. It is critically important the risk title is relevant within the organisational context. The risk description should succinctly articulate the event, cause, and impact, as demonstrated in the figure below.

Figure 2 Risk Description Steps



The example below demonstrates how a work health and safety risk may be described:

'BITS Technology Group employees or contractors performing desk work ('event') could injure themselves due to an inappropriate working environment (desk not ergonomically set) (cause) resulting in back injury ('impact').'

We aim to aggregate substantially similar risks as far as practically possible and eliminate irrelevant risks from the risk register. This is performed with the objective of keeping a relevant and concise risk register to enable agile and focused risk management activities.

Assess Risk

The BITS Technology Group CEO has approved likelihood and consequence criteria to quantify identified risks (refer to Appendix B). At BITS Technology Group we perform the risk assessment twice: once in the absence of existing controls (inherent risk):

(consequence x likelihood) = inherent risk

And again, having regard for the controls in place (residual risk):

(consequence x likelihood) x control effectiveness = residual risk

To estimate control effectiveness the following table should be utilised, i.e.:

Table 1 - Escalation Requirements

Control effectiveness	Description
Fully Effective (100%) = (consequence x likelihood) *0	Controls are well designed for the risk, largely prevent the risk from eventuating, and address the root causes. The controls are operating effectively and are always reliable. Nothing more can be done except review and monitor the existing controls.
Substantially Effective (75%) = (consequence x likelihood) *0.25	Most controls are designed correctly and are in place and effective. Some more work needs to be done to improve operating effectiveness of the controls, or there are doubts about operational effectiveness and reliability.
Partially Effective (50%) = (consequence x likelihood) *0.50	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. There may be an over reliance on reactive controls.
Largely Ineffective (25%) = (consequence x likelihood) *0.75	Significant controls gaps. Either controls do not treat root cause or they do not operate effectively at all. Controls if they exist are just reactive.
None (0%) = (consequence x likelihood) *1	Virtually no credible control. There is little to no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness of controls.

Evaluate the Risks

Risk evaluation is a comparison of the residual risk, as calculated in the previous step, and the target risk to determine both the need for escalation and whether our risk exposure is acceptable or whether further treatment is required.

The residual risk rating forms the basis for this decision making. Escalation of risks should occur as soon as practicably possible using the criteria in Table 2 below.

Table 2 - Escalation Requirements

Residual Risk Rating	Team Lead / Manager	CEO	Directors
Extreme	E	E	A
High	E	A	
Medium	E	A	
Low	E		

E = Escalate R = Review A = Acceptance Authority

Where there is a difference between the Directors risk appetite and the acceptance authority levels, appropriate risk treatments must be introduced to address the disparity, or the issue escalated to the Directors for consideration. People with risk acceptance authority may always elect to implement treatments to reduce a risk under their acceptance authority.

For new risk categorised as:

- Extreme or a risk changing rating to extreme: immediate escalation and notification of the CEO and Directors should be initiated.
- High or a risk changing rating to high: immediate escalation and notification of the CEO should be initiated.

Risk categorised as Extreme or High, should ideally be acknowledged, reviewed and a desired treatment option formulated with in a 24 hour time period.

Treat or Accept the Risk

The target risk level that is acceptable to the organisation will vary according to the situation but will typically be informed by the Director approved RAS and/or risk acceptance by someone with the requisite authority (see section 4.4).

The treatment of risks involves the development and implementation of specific cost-effective strategies and action plans to increase potential benefits and reduce the impact of the risk; some treatment options include:

Table 3 – Treatment options

Control Method	Description
Avoid	Activities with a high likelihood of loss and large financial impact. The best response is to avoid the activity unless there is significant potential opportunity.
Reduce	Activities with a high likelihood of occurring, but financial impact is small. The best response is to use management control systems to reduce the risk of potential loss.
Transfer or share	Activities with low probability of occurring, but with a large financial impact. The best response is to transfer a portion or all the risk to a third party by purchasing insurance, hedging, outsourcing, or entering into partnerships
Accept	If cost-benefit analysis determines the cost to mitigate risk is higher than cost to bear the risk, then the best response is to accept and continually monitor the risk.

Reporting

Risk Reporting

Audiences for risk reporting and associated timeframes are defined in Table 4 below. The content of these reports will be tailored to the needs of each audience.

Table 4 - Risk Reporting Requirements

Report	Report To	Frequency

Operational Risk Register	Business Owners	Quarterly
Operational Security Report	Business Owners	Quarterly

Monitoring and Assurance

Control Assurance

Where high reliance is placed on a control to reduce a material risk to within risk appetite, it should be captured under some form of assurance activity.

An assurance matrix that details and plans how these assurance processes will be maintained within the de.iterate platform and will be reviewed on an annual basis. Assurance activities may include:

- Self-assessment of controls for design, implementation, and operating effectiveness
- Management directed audits which involve completion of a more detailed assessment of a given risk and controls, typically through a focused workshop
- Assurance processes undertaken by external parties.

The outcome of these processes will inform the review of the effectiveness (and rating) for each material risk area.

Continuous Improvement

The effectiveness of the RMS should be monitored on an ongoing basis, with outcomes, such as on the framework's effectiveness and any issues or concerns, presented to the CEO on a periodic basis as part of a formal management review.

The RMS effectiveness may be assessed through the following means:

- Outcomes of any assurance processes by internal and external parties during the review period
- Root cause analysis of events and near misses as required
- Surveys and management team input.

Risk Trigger Monitoring

For each identified risk in the Risk Register, should have an appropriate monitoring methodology implemented to detect the possible inception occurring. The correct notification mythology should also be defined to ensure the Asset Owner, Risk Owner and the appropriate operational response teams are aware.

Where a risk has been classified as Extreme, its advisable to have a Risk Response plan in place.

Risk Management Performance

The BITS Technology Group Directors or their delegates will assess the performance of the Exec Team on its delivery of risk management fundamental outcomes (section 1.3) by taking into account aspects such as:

- The quality and timeliness of risk information or reports provided to the Directors
- The performance of key risk management activities such as strategic and operational risk register updates
- The timely and effective delivery of treatment strategies
- Management effort leading to the reduction of high and extreme risks to the organisation's strategic objectives
- Events, hazards and near misses with root cause analysis.

Consultation

Consultation in relation to risk is not a one-off event, rather it features in all stages of the risk processes described in this document. Many of the key consultation processes are inherent in the design of the risk management processes (e.g. the defined risk escalation processes). However, from a principle based perspective, all stakeholders with a material interest in any risk process should be consulted. Of particular importance are risk and control owners and parties who will be accountable for delivery of key controls.

Roles and Responsibilities

Communicating roles and responsibilities for the management of risk is an essential component of any robust RMS. The risk management responsibilities at BITS Technology Group have been outlined below.

Table 5 – Responsibilities related to the RMS

Position	Responsibility
Company Directors	● Oversight of risk and sole authority to accept extreme risks ● Approve the RMS. ● Oversee and monitor the performance of management in discharging its risk management duties and reporting as set out in the RMS ● Ensure the ongoing adherence of the business to good corporate governance and sound risk management. ● Monitor the internal and external risk environments of BITS Technology Group to identify and report on any changes to the risk profile
Chief Executive Officer	● Ensure the RMS is implemented and operating effectively. ● Ensure that staff are adequately trained in risk management practices. ● Operate within the risk acceptance criteria.

	• Review the effectiveness of the implementation of the RMS and report findings, including risks, as part of the regular updates to the Company Directors
Staff and Contractors	• All employees, contractors and consultants working for or on behalf of BITS Technology Group, are responsible for adherence to the RMS and its supporting procedures, including the identification and escalation of risk.
Risk Owner	• Management of identified risks for which they are the nominated owner, including the following activities: ○ Monitor the risk and its environment for any changes or developments that may affect the level of risk ○ Ensure that the level of risk remains appropriate and trigger/participate in reviews, as necessary ○ Ensure treatment actions are completed by action owners in a timely manner ○ Verify that controls are operating as anticipated ○ Participate in assurance activities, as required.
Risk Treatment Owner	• Execution of identified actions / treatments for which they are the nominated owner, including reporting implementation status to the risk owner as identified within the Risk Treatment Plan (RTP).

Supporting Documents

Description	Detail
External references	• AS/NSZ ISO 31000:2018: Risk management – principles and guidelines

Appendix A - Description of RMS Elements

Description	Detail
Strategy	Risk is defined as the uncertainty on objectives. BITS Technology Group strategic objectives provide the starting point for risk management in the organisation.
Risk Standard	Sets criteria stating minimum performance requirements necessary to ensure effective implementation of the Risk Management Policy, including the processes for assessment, review, escalation, monitoring and reporting of risk. Provides the evaluation mechanism to assess risk which is influenced by the Risk Appetite Statement.
Processes and operational procedures	Reference to or embedding of the requirements of the Risk Management Standard occurs at the process and operational procedure level. For example, the requirement to assess risk using the above guidance is embedded in the business continuity, project management and business case development processes.

Appendix B – BITS Technology Group Risk Assessment Matrix

Consequence (Where an event has more than one 'Loss Type', choose the 'Consequence' with the highest rating)					
Risk Category	**Insignificant (1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Health and Safety	No treatment or first aid treatment only. Returned to full duties.	Minor temporary injury or illness requiring medical treatment. Inability to complete rest of shift or modified duties.	Moderate injury or temporary impairment. One or more entire shifts missed as a result.	Permanent injury or impairment.	Fatality
Strategic	Insignificant impact on Strategic objectives, dealt with through routine operations.	Minimal impact on Strategic objectives. Reversible situation although specific activities required to remedy situation using existing resources.	Moderate impact on Strategic objectives. Reversible situation, additional resources required to remedy situation.	Significant impact on Strategic objectives. Full anticipated benefits will not be realised.	Business and Strategic objectives unable to be achieved
People	Individual staff 'disengagement'. No attrition above baseline levels.	Team 'disengagement' affecting operational processes. Staff attrition 100% higher than baseline.	Functional level 'disengagement' affecting service quality. Staff attrition 150% higher than baseline.	Office/business level 'disengagement', unable to support key services. Staff attrition >200% higher than baseline.	Organisational 'disengagement' (organisational level). Staff attrition >300% higher than baseline.
Regulatory / Compliance / Governance	Compliance, contractual or regulatory non-compliance which can be managed through established processes and is unlikely to result in implications for the organisation.	Compliance, contractual or regulatory breach where specific activities are required to remedy situation but where the incident is unlikely to result in litigation, prosecution, fines or penalties.	Compliance, contractual or regulatory breach with fines or penalties of up to $10,000; enquiry, investigation or complaint from a regulator with threat of or probable litigation or prosecution.	Compliance, contractual or regulatory breach with fines or penalties of under $20,000.	Compliance, contractual or regulatory breach with fines or penalties $20,000 or more.
Financial	Financial impact that can be absorbed in and dealt with at the individual activity level. Or, exposure of <$1k of unfunded financial commitments.	Financial impact that can be absorbed and dealt with at the business unit level. Or, exposure of <$2k of unfunded financial commitments.	Financial impact that can be absorbed and dealt with at the business unit level. Or, exposure of <$10k of unfunded financial commitments.	Financial impact limiting the capacity of the organization to achieve its objectives. Or, exposure of $20k of unfunded financial commitments.	Financial impact jeopardises the business as a going concern. Or, exposure of >$50k of unfunded financial commitments
Customer Experience	Isolated customer complaint regarding service performance.	Service levels for Individual key account customer are impacted but within SLA.	Service levels for Individual key account customer are outside of SLA.	Individual key account customer materially impacted.	Multiple key account customers materially impacted.
Information Security and Privacy	Loss or disclosure of a datum of 'non-sensitive' information.	Loss or disclosure of multiple records of 'non-sensitive' information.	Loss or disclosure of a datum of 'sensitive' information.	Loss or disclosure of multiple records of 'sensitive' information'.	Loss or disclosure of 'sensitive' information' with potential for 'serious harm'.

Consequence Where choosing a rating, remember, it is the likelihood of the event resulting in the consequence. Round up or down to the nearest number as appropriate.							
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Likelihood descriptors			**Risk Rating**				
Almost Certain	The event is expected to occur in most circumstances. Multiple / 12 months	>80%	**Medium**	**High**	**High**	**Extreme**	**Extreme**
Likely	The event will probably occur in most circumstances. Once / 12 months	61 –80%	**Medium**	**Medium**	**High**	**High**	**Extreme**
Possible	The event might occur, but not expected to occur under normal circumstances. Once 1-5 years	>41 –60%	**Low**	**Medium**	**Medium**	**High**	**High**
Unlikely	The event could occur at some time, but only in unusual circumstances. Once / 5 -10 years	21 –40%	**Low**	**Low**	**Medium**	**Medium**	**High**
Rare	The event could occur only in exceptional circumstances. Once / > 10 years	<20%	**Low**	**Low**	**Medium**	**Medium**	**Medium**

Document Control

DESIGNATED POLICY OWNER	Classification	Publication Date	Next Review Date
GM	Business Confidential	01/7/2024	01/7/2025

Revision History

Version	Date	By	Summary of Changes
0.1	20/02/2025	Esther Mangelsdorf	Initial draft
1.0	13/5/2025	Esther Mangelsdorf	Published Copy