Northgate Engineering Ltd	Document ID	RSK-001
	Version	1.0
Risk Assessment Methodology	Effective Date	March 1, 2026
	Document Owner	Rachel Okafor
	Approved By	David Whitfield

Table of Contents

1. Introduction

1.1 Purpose

This Risk Assessment Methodology establishes a standardized, repeatable, and defensible approach for identifying, analyzing, evaluating, and prioritizing risks across Northgate Engineering Ltd. The methodology ensures consistency in risk assessment activities, enables meaningful comparison of risks across business units, supports informed decision-making, and demonstrates due diligence to regulators, auditors, and stakeholders.
Risk assessment is a fundamental component of the enterprise risk management framework and informs strategic planning, resource allocation, control design, and continuous improvement activities. This methodology aligns with ISO 31000:2018 (Risk Management Guidelines), ISO 27005:2022 (Information Security Risk Management), NIST SP 800-30 Rev. 1 (Guide for Conducting Risk Assessments), and NIST Cybersecurity Framework 2.0.

1.2 Scope

This methodology applies to all risk assessment activities within Northgate Engineering Ltd, including enterprise-level risk assessments conducted annually, operational risk assessments for business processes and functions, project risk assessments for new initiatives and changes, third-party risk assessments for vendors and partners, information security risk assessments for systems and data, compliance risk assessments for regulatory obligations, and ad-hoc assessments triggered by incidents or emerging threats.
The methodology covers risks across all categories, including strategic, operational, financial, compliance, technology, cyber, reputational, and emerging risks. It applies regardless of whether risks are positive (opportunities) or negative (threats).

1.3 Objectives

The risk assessment process aims to identify risks that could affect achievement of organizational objectives, analyze the likelihood and potential impact of identified risks, evaluate risks against defined criteria and risk appetite, prioritize risks for treatment based on significance, provide actionable information to support risk-based decisions, create an auditable record of risk management activities, and enable trending and comparison of risks over time.

1.4 Principles

Risk assessments conducted under this methodology adhere to the following principles:

- Proportionality: Assessment rigour is proportionate to the significance of the decision being supported
- Consistency: The same methodology is applied across the organization to enable comparison
- Objectivity: Assessments are based on evidence and data where available, not solely on opinion
- Inclusivity: Relevant stakeholders with appropriate knowledge participate in assessments
- Transparency: Assessment criteria, assumptions, and limitations are clearly documented
- Currency: Assessments reflect current conditions and are updated when circumstances change

- Integration: Risk assessment is embedded in business processes, not performed in isolation

2. Risk Assessment Framework

2.1 Framework Overview

The risk assessment framework consists of five phases: Context Establishment, Risk Identification, Risk Analysis, Risk Evaluation, and Documentation and Reporting. Each phase builds upon the previous and produces specific outputs that feed into subsequent activities.

Phase	Primary Activities	Key Outputs
1. Context Establishment	Define scope, objectives, criteria; Identify stakeholders; Gather background information	Assessment scope document; Risk criteria; Stakeholder register
2. Risk Identification	Identify risk sources, events, causes, and consequences; Document in the risk register	Comprehensive risk inventory; Risk statements
3. Risk Analysis	Determine likelihood and impact; Assess existing controls; Calculate risk scores	Inherent and residual risk ratings; Control effectiveness ratings
4. Risk Evaluation	Compare against criteria and appetite; Prioritise risks; Determine treatment needs	Prioritized risk list; Treatment recommendations
5. Documentation	Record findings; Prepare reports; Communicate to stakeholders	Risk assessment report; Updated risk register; Executive summary

2.2 Assessment Types

Different types of risk assessments serve different purposes and employ varying levels of rigour:

Assessment Type	Trigger	Scope	Frequency	Typical Duration
Enterprise Risk Assessment	Annual planning cycle	Organization-wide strategic and operational risks	Annually	4-8 weeks
Operational Risk Assessment	Process changes, incidents	Specific business process or function	Annually or on change	1-2 weeks
Project Risk Assessment	Project initiation	Specific project or initiative	Project phases	2-5 days

Third-Party Risk Assessment	Vendor onboarding, renewal	Specific vendor or partner relationship	Initially and annually	1-2 weeks
Information Security Risk Assessment	System changes, audits	Specific system, application, or data	Annually or on change	1-3 weeks
Compliance Risk Assessment	Regulatory changes	Specific regulation or obligation	Annually or on change	1-2 weeks
Rapid Risk Assessment	Emerging threats, incidents	Specific threat or situation	As needed	1-3 days

3. Phase 1: Context Establishment

3.1 Defining Assessment Scope

Every risk assessment begins with a clear definition of scope, including the organizational unit, process, system, or initiative being assessed, the time horizon for which risks are being considered, the types of risks included (and explicitly excluded), the level of detail required, and the boundaries and interfaces with other areas.
Scope definition prevents scope creep, ensures appropriate resource allocation, and sets stakeholder expectations. The scope statement is documented and approved by the assessment sponsor before proceeding.

3.2 Establishing Risk Criteria

Risk criteria define how risks will be measured and evaluated. These criteria must be established before risk analysis to ensure objectivity. Key criteria include likelihood scale (how probability of occurrence is measured), impact scale (how consequences are measured across dimensions), risk rating methodology (how likelihood and impact combine to produce a risk score), risk appetite and tolerance levels (thresholds for risk acceptance), and aggregation rules (how multiple risks combine).

3.3 Stakeholder Identification

Effective risk assessment requires input from stakeholders with relevant knowledge and perspective. Stakeholders are identified based on their knowledge of the area being assessed, their responsibility for managing identified risks, their authority to make decisions about risk treatment, their interest in the assessment outcomes, and their ability to provide resources for the assessment.

3.4 Information Gathering

Before conducting risk identification, assessors gather relevant background information, including previous risk assessments and audit findings; incident and loss data; industry threat intelligence and benchmarks; regulatory requirements and guidance; business objectives and success criteria; existing controls and their documented effectiveness; and organizational context (structure, culture, strategy).

4. Phase 2: Risk Identification

4.1 Risk Identification Objectives

Risk identification aims to create a comprehensive inventory of risks that could affect the achievement of objectives. The goal is to identify risks before they materialize, enabling proactive management. Effective risk identification answers the questions: What could happen? Why could it happen? What would be the consequences?

4.2 Risk Identification Techniques

Multiple techniques are used to ensure comprehensive risk identification. No single technique captures all risks, so assessors employ a combination appropriate to the assessment context:

Technique	Description	Best Used For	Limitations
Brainstorming Workshops	Facilitated sessions with stakeholders to generate risk ideas freely	New areas; Creative thinking; Team engagement	Can be dominated by vocal participants; May miss technical risks
Structured Interviews	One-on-one discussions with subject matter experts using predefined questions	Sensitive topics; Expert knowledge extraction; Deep dive	Time intensive; Interviewer bias possible
Questionnaires and Surveys	Written questions distributed to larger groups for input	Large stakeholder groups; Baseline data; Consistent input	Low response rates; Superficial responses
Checklists and Taxonomies	Predefined lists of common risks in the domain	Ensuring coverage; New assessors; Compliance	May constrain thinking; May miss novel risks
Process Analysis (FMEA)	Systematic review of process steps to identify failure modes	Operational processes; Quality risks; Technical systems	Requires detailed process knowledge; Time consuming
Scenario Analysis	Development of plausible future scenarios and their implications	Strategic risks; Emerging threats; Long-term planning	Scenarios may be unrealistic; Resource intensive
Historical Analysis	Review of past incidents, losses, near-misses, and audit findings	Known risk types; Trend identification; Evidence-based	Past may not predict future; Data quality issues

SWOT/PESTLE Analysis	Structured analysis of internal and external factors	Strategic planning; Environmental scanning	High level; May miss operational details
Bow-Tie Analysis	Visual mapping of causes, events, and consequences with controls	Complex risks; Control identification; Communication	Requires facilitation skill; Can become complex
Delphi Technique	Iterative expert consultation to build consensus	Uncertain/novel risks; Expert disagreement	Time consuming; Expert availability

4.3 Risk Statement Construction

Risks are documented using structured risk statements that clearly articulate the risk. A well-constructed risk statement includes a risk source (the element that has potential to give rise to risk), a risk event (what could happen), a risk cause (why it could happen), and risk consequences (what the impact would be if it occurred).
The recommended format is: "There is a risk that [EVENT] may occur due to [CAUSE], resulting in [CONSEQUENCE]." For example: "There is a risk that a ransomware attack may occur due to unpatched vulnerabilities and phishing susceptibility, resulting in operational disruption, data loss, and reputational damage."

4.4 Risk Categories

Risk identification shall also consider Strategic Opportunity Risk—the risk of failing to pursue an initiative (e.g., AI adoption, Cloud migration) that could result in loss of market competitiveness.

5. Phase 3: Risk Analysis

5.1 Analysis Overview

Risk analysis determines the level of risk by examining likelihood of occurrence and magnitude of consequences. Analysis is performed for both inherent risk (risk level without considering existing controls) and residual risk (risk level after considering existing controls). The difference between inherent and residual risk demonstrates control effectiveness.

5.2 Analysis Approaches

Three approaches to risk analysis may be employed depending on data availability and assessment requirements:

Approach	Description	When to Use	Advantages	Limitations
Qualitative	Risks described using defined scales (e.g., Low/Medium/High)	Limited data; Rapid assessment; Broad coverage	Quick; Easy to understand; No statistics required	Subjective; Difficult to aggregate; Less precise
Semi-	Qualitative scales with	Moderate data;	Enables	Numbers can

Quantitative	numerical scores assigned	Prioritization needed; Most common	ranking; More rigorous than pure qualitative	imply false precision
Quantitative	Risks expressed in numerical terms (probability, monetary value)	Good data available; Financial decisions; Insurance	Precise; Supports cost-benefit analysis; Actuarial rigour	Data intensive; Complex; May be spuriously precise

Northgate Engineering Ltd primarily uses a semi-quantitative approach for most risk assessments, with quantitative analysis applied to major financial and insurable risks where sufficient data exists.

5.3 Likelihood Assessment

Likelihood represents the probability that a risk event will occur within the assessment time horizon. The following 5-point scale is used:

Level	Rating	Probability Range	Frequency Guidance	Description
5	Almost Certain	>90%	Expected to occur multiple times per year	The risk event is expected to occur in most circumstances. History of frequent occurrence.
4	Likely	66-90%	Will probably occur at least annually	The risk event will probably occur. Has occurred several times in the past.
3	Possible	26-65%	May occur every 1-3 years	The risk event might occur at some time. Has occurred occasionally.
2	Unlikely	10-25%	May occur every 3-10 years	The risk event could occur but not expected. Has occurred rarely.
1	Rare	<10%	May occur less than every 10 years	The risk event may occur only in exceptional circumstances. May have never occurred.

When assessing likelihood, assessors consider historical frequency of similar events, industry data and benchmarks, current threat environment, changes in circumstances since last occurrence, expert judgment where data is limited, and time horizon of the assessment.

5.4 Impact Assessment

Impact represents the magnitude of consequences if the risk event occurs. Impact is assessed across multiple dimensions to capture the full range of potential effects:

Level	Rating	Financial	Operational	Reputational	Compliance/Legal
5	Catastrophic	>$10M loss or >25% revenue	Extended shutdown >1 month; Unrecoverable service loss	International media; Lasting brand damage; Executive departure	Criminal prosecution; License revocation; Major regulatory action
4	Major	$1M-$10M loss or 10-25% revenue	Significant disruption 1-4 weeks; Major service degradation	National media attention; Significant customer attrition	Regulatory investigation; Material fines; Litigation
3	Moderate	$100K-$1M loss or 5-10% revenue	Disruption 1 week; Noticeable service impact	Regional/trade media; Customer complaints	Formal regulatory inquiry; Moderate fines; Audit findings
2	Minor	$10K-$100K loss or 1-5% revenue	Disruption 1-7 days; Limited service impact	Local media; Social media criticism	Regulatory warning; Minor breach notification
1	Insignificant	<$10K loss or <1% revenue	Disruption <1 day; Minimal service impact	Internal awareness only; No external coverage	Internal compliance breach; Informal regulatory feedback

When a risk could have impacts across multiple dimensions, the highest impact rating is used. Financial thresholds should be adjusted based on organization size and risk appetite.

5.5 Risk Score Calculation

To streamline the assessment for operational agility:

- **Current Risk:** Assess the risk level *as it exists today*, considering all currently implemented controls. This is the primary driver for decision-making.
- **Target Risk:** (Optional) Assess the desired risk level after proposed treatments are implemented.

- *Note: "Inherent Risk" (Risk without any controls) is reserved for advanced theoretical modeling and is not required for standard assessments.*

5.6 Risk Matrix

The risk matrix provides a visual representation of risk levels based on likelihood and impact combinations:

Likelihood / Impact	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
5 Almost Certain	5 Medium	10 Medium	15 High	20 Critical	25 Critical
4 Likely	4 Low	8 Medium	12 High	16 High	20 Critical
3 Possible	3 Low	6 Medium	9 Medium	12 High	15 High
2 Unlikely	2 Very Low	4 Low	6 Medium	8 Medium	10 Medium
1 Rare	1 Very Low	2 Very Low	3 Low	4 Low	5 Medium

5.7 Control Assessment

Existing controls are assessed to determine residual risk. Control assessment considers control design (is the control appropriately designed to address the risk?) and control operating effectiveness (is the control operating as designed?).

Effectiveness Rating	Score	Description	Residual Risk Adjustment
Highly Effective	4	Controls are well designed and operating effectively; Strong evidence of effectiveness; No significant gaps	Reduce likelihood and/or impact by 2 levels
Effective	3	Controls are adequately designed and generally operating effectively; Minor gaps exist	Reduce likelihood and/or impact by 1 level
Partially Effective	2	Controls are designed but operating inconsistently; Significant gaps exist	No adjustment to inherent risk rating
Ineffective	1	Controls are poorly designed or not operating; Major deficiencies	Consider increasing inherent risk rating
None	0	No controls exist for this	Use inherent risk rating as

		risk	residual

6. Phase 4: Risk Evaluation

6.1 Evaluation Purpose

Risk evaluation compares analyzed risk levels against established criteria to determine risk significance and treatment priorities. Evaluation answers the question: Which risks require treatment, and in what order?

6.2 Risk Appetite Comparison

Residual risk levels are compared against the organization's risk appetite as defined in the Risk Appetite Statement (RSK-005). Risks are classified as within appetite (acceptable without additional treatment), approaching appetite (monitoring required; treatment may be needed), or exceeding appetite (treatment required to bring within tolerance).

6.3 Prioritization Criteria

When multiple risks require treatment, prioritization considers residual risk score (higher scores treated first), velocity (how quickly the risk could materialize), trend (increasing risks prioritized over stable risks), interconnection (risks that could trigger other risks), treatment feasibility (risks with practical treatment options), and strategic alignment (risks affecting strategic objectives).

6.4 Treatment Determination

For each risk requiring treatment, the evaluation phase determines the appropriate treatment strategy:

Strategy	Description	When Appropriate	Considerations
Accept	Retain the risk without additional treatment	Risk within appetite; Treatment not cost-effective; Opportunity risk	Must be conscious decision by authorized personnel; Document rationale
Mitigate	Implement controls to reduce likelihood and/or impact	Most common strategy; Risk exceeds appetite but can be reduced	Consider control costs vs risk reduction; Avoid over-control
Transfer	Share risk with third party (insurance, contracts)	Financial risks; Insurable risks; Outsourceable activities	Does not eliminate risk; Counterparty risk; Coverage limitations
Avoid	Eliminate the risk by eliminating the activity	Risk exceeds appetite; Cannot be adequately mitigated; Not core activity	May forego opportunity; May not be possible for core activities

Exploit	Take action to realize a positive risk (opportunity)	Upside risks; Competitive advantage potential	Balance against downside risks; Resource requirements

7. Phase 5: Documentation and Reporting

7.1 Documentation Requirements

All risk assessments are documented to provide an audit trail, support decision-making, enable knowledge transfer, and demonstrate due diligence. Documentation includes assessment scope and context, participants and their roles, information sources used, risk identification results, analysis methodology and ratings, evaluation criteria and decisions, assumptions and limitations, and recommendations and next steps.

7.2 Risk Register Updates

Assessment findings are recorded in the Enterprise Risk Register (RSK-003), which serves as the authoritative record of identified risks. The register captures risk identification details (ID, title, description, category, owner), analysis results (inherent likelihood, inherent impact, inherent score), control information (existing controls, control effectiveness), residual risk (residual likelihood, residual impact, residual score), treatment details (strategy, actions, owner, due date, status), and review information (last review date, next review date, trend).

7.3 Reporting

Risk assessment findings are reported to stakeholders through various mechanisms:

Report Type	Audience	Content	Frequency
Risk Assessment Report	Assessment sponsor and stakeholders	Full assessment findings, methodology, recommendations	Per assessment
Executive Risk Summary	Executive leadership	Top risks, trends, treatment status, emerging risks	Monthly
Board Risk Report	Board/Audit Committee	Strategic risks, appetite status, material changes	Quarterly
Risk Dashboard	Risk owners and managers	Risk status, KRIs, treatment progress	Real-time/ Weekly
Regulatory Risk Report	Regulators	As required by regulatory obligations	As required

8. Roles and Responsibilities

8.1 Risk Assessment Roles

Role	Responsibilities
Assessment Sponsor	Approve scope and resources; Receive and act on findings; Ensure appropriate treatment
Assessment Lead	Plan and coordinate assessment; Facilitate sessions; Ensure methodology compliance; Produce report
Risk Manager	Provide methodology guidance; Quality assure assessments; Maintain risk register; Aggregate and report
Subject Matter Experts	Provide domain knowledge; Participate in identification and analysis; Validate findings
Risk Owners	Own identified risks; Implement treatment plans; Report on risk status; Escalate as needed
Control Owners	Provide control information; Support control assessment; Implement control improvements
Internal Audit	Provide independent assurance on risk assessment quality and risk management effectiveness

9. Quality Assurance

9.1 Assessment Quality

Risk assessment quality is ensured through methodology compliance (assessments follow this documented methodology), peer review (assessments reviewed by independent risk management personnel), management review (findings reviewed by appropriate management level), calibration (periodic comparison across assessments to ensure consistency), and continuous improvement (lessons learned incorporated into methodology).

9.2 Common Pitfalls to Avoid

Assessors should be aware of common pitfalls that reduce assessment quality: availability bias (overweighting recent or memorable events), optimism bias (underestimating likelihood of negative outcomes), groupthink (convergence on consensus without critical challenge), anchoring (over-reliance on initial estimates), confirmation bias (seeking information that confirms existing beliefs), and scope creep (expanding scope without corresponding resources).

10. Review and Maintenance

10.1 Methodology Review

This methodology is reviewed annually and updated when there are significant changes to the risk environment, changes in organizational structure or strategy, lessons learned from risk events, changes in regulatory requirements, feedback from methodology users, or industry best practice developments.

10.2 Risk Assessment Refresh

Existing risk assessments are refreshed annually at a minimum, when significant changes occur to the assessed area, following relevant incidents or near-misses, when new threats or vulnerabilities emerge, and when control effectiveness changes materially.

11. Framework Alignment

Framework	Relevant Requirements	Alignment
ISO 31000:2018	Clause 6: Risk Assessment Process	Full alignment with identification, analysis, evaluation phases
ISO 27001:2022	Clause 6.1.2: Information Security Risk Assessment	Methodology applicable to information security risks
ISO 27005:2022	Information Security Risk Management	Aligned risk identification, analysis, evaluation guidance
NIST CSF 2.0	ID.RA (Risk Assessment subcategory)	Supports ID.RA-01 through ID.RA-06 outcomes
NIST SP 800-30	Guide for Conducting Risk Assessments	Aligned threat, vulnerability, impact, likelihood approach
CIS Controls v8	Control 17: Incident Response	Supports risk-based control prioritization

12. Document Control

Version	Date	Author	Description of Changes
1.0	March 1, 2026	Information Security Team	Initial release

Appendix A: Quick Implementation Tips

For Organisations New to Risk Assessment: Start with a focused scope (one business unit or process) rather than enterprise-wide. Use workshops with key stakeholders to build engagement. Focus on the top 10-15 risks initially rather than a comprehensive inventory. Establish clear ownership for each identified risk. Set realistic treatment timelines that can be achieved.
For Mature Organisations: Integrate risk assessment with strategic planning cycles. Implement continuous risk monitoring using KRIs. Use quantitative analysis for material financial risks. Benchmark against industry peers. Consider emerging risk horizon scanning.

This is a customizable template provided by RidgeLine Cyber Defence. It is not legal advice. Organiations should seek qualified professional advice for their specific circumstances and jurisdiction.