RISK MANAGEMENT FRAMEWORK

Updated November 2025

Contents

1. INTRODUCTION

1.1 Purpose

G8 Education Limited and its subsidiaries (together, **G8** or the **Group**) is committed to proactive, consistent, and effective risk management. This Risk Management Framework (the **Framework**) sets out the systems, processes, tools, governance structures, and expectations used across the organisation to identify, assess, treat, monitor, and report risk.

The Framework operationalises the Risk Management Policy (**Policy**) and implements the systems, procedures and governance necessary to meet:

- ISO 31000:2018 *Risk Management Guidelines*
- ASX Corporate Governance Council Principle 7
- National Principles for Child Safe Organisations
- Requirements under the Education and Care Services National Law and Regulations
- Obligations relating to workplace health and safety, privacy, employment, cyber security, financial management and other legislation applicable to the Group.

The Framework supports:

- the protection of children
- the safety and wellbeing of team members
- operational continuity
- quality learning environments
- compliance with legislation and regulations
- financial sustainability
- effective decision-making
- the achievement of strategic objectives

The Framework also supports a constructive risk culture where team members proactively identify and escalate concerns, apply controls, and act in accordance with G8's values, legal obligations and child safety principles.

1.2 Application

This Framework applies to:

- All G8 team members, contractors and volunteers
- All G8 centres, support functions and regions
- All enterprise, functional, operational and project risks

The Framework governs the eleven enterprise risk categories and associated sub-risks, and the requirements for risk registers, reporting, escalation, monitoring and assurance.

1.3 Relationship to the Risk Management Policy

The G8 Risk Management Policy defines Risk Management governance expectations, and this Framework explains how to operationalise those expectations in practice.

The Framework serves as an operational **"how-to" manual** that enables leaders and team members to apply risk management in their daily work. It explains:

- how to identify and assess risks at centre, regional, divisional and enterprise levels
- how to utilise the eleven enterprise risk categories and their sub-risks
- how to evaluate risks using likelihood, consequence and control effectiveness
- when and how to escalate risks that exceed risk tolerances
- how risk registers should be maintained and reviewed
- how centre-based risk management connects to divisional and enterprise risk oversight.

The Framework aims to:

- Build consistent and systematic risk management practices across G8 at an enterprise level.
- Integrate risk management with child safety, team safety, quality, operations, strategy and finance.
- Ensure risks are identified early and managed within G8's risk appetite as set by the Board.
- Support the Board and Executive Leadership Team (ELT) with accurate, timely risk information.
- Provide practical procedures and tools to support effective risk identification, reporting, and escalation.

2. KEY CONCEPTS AND DEFINITIONS

2.1 Definition of Risk

G8 uses the ISO 31000 definition of Risk:

Risk is the effect of uncertainty on objectives.

Uncertainty may affect a variety of aspects of the Group's activities, including child safety, staffing stability, regulatory compliance, continuity of operations, financial health, technology resilience, reputation and strategic outcomes.

2.2 Enterprise Risk Categories

G8 manages risk through eleven enterprise-level categories. The Board has set a Risk Appetite and Risk Tolerances for each of this Enterprise Risks. The Enterprise Risks are the basis of the Group's operational, functional and enterprise risk registers.

Enterprise Risk Categories

	Enterprise Risk	Definition
R1	Child protection	Failure to protect children in our care from sexual, physical, emotional/psychological abuse, exposure to violence, neglect or harm inflicted upon them.
R2	Health, safety and well-being	Failure to provide safe environments, workspaces and systems to support children, team members, contractors and visitor's health, safety and well-being.
R3	Liquidity and funding management	Failure to manage G8's financial position that impacts on G8's ability to pay its obligations on a timely basis and fund the future strategy and business operations.

	Enterprise Risk	Definition
R4	Attraction, retention, and capability of team	Failure to attract, develop, engage and retain appropriate talent, resulting in negative operational and financial impacts.
R5	Cyber, confidential data and IP	Losses arising from theft of G8 physical and digital confidential data and IP through unauthorised internal or external party access.
R6	Business disruption and system failure	Losses arising from disruption of business or system failure such as natural disasters, man-made events, supply chain disruptions, software/hardware outages, and cybersecurity incidents.
R7	Strategy and competitive pressures	Failure to make effective strategic decisions and execute a proactive strategic plan effectively, resulting in poor operational performance and weak financial outcomes, loss of family and stakeholder confidence and inability to adapt to changing market conditions.
R8	Regulatory and legislative obligations	Failure to comply with external regulations, acts, laws or G8 policies and procedures resulting in material penalty or fine or negatively impacting G8's licence to operate.
R9	Government and policy reform	Failure to advocate for, plan for and adapt to early childhood education policy or other government reforms which impact G8's market or diminish the importance of government funding for all children to access quality early learning and care.
R10	Supplier and contract management	Adverse business impacts from supplier/landlord arrangements, including contract management, business interruption, critical non-performance and disputes.
R11	Theft, fraud and malicious acts	Internal or external parties intending to defraud, misappropriate property or circumvent the law.

Each Enterprise Risk has a number of sub-risks which delineate the Enterprise Risk. These are included in the Enterprise Risk Register.

2.3 Risk Appetite

Risk appetite describes the amount and type of risk G8 is willing to accept in pursuit of its objectives. The Board sets risk appetite and risk tolerance ranges for each enterprise risk category.

Risk appetite must be applied in:

- assessing residual risks
- determining risk treatments
- escalating risks outside appetite
- evaluating strategic decisions

- prioritising actions and resources

Risks outside of risk tolerance must be escalated and a treatment plan applied.

G8's Risk Appetite Statement describe the level of risk that the Board have deemed as broadly acceptable, while our risk tolerance is the amount of risk related to a specific objective. The risk appetite statements are reviewed by the Board at least annually.

Appetite Levels	Meaning and required escalation and response
Zero	G8 is **not willing** to accept any instances of this risk occurring. It does accept that sometimes these risks could occur and if they do, they will always be actioned and any weaknesses identified will be rectified.
Low	G8 accepts a **low** amount of this risk occurring. Risks occurring greater than a low level will be risk mitigated and any weaknesses identified will be rectified.
Medium	G8 accepts a **medium** amount of this risk occurring. Risks occurring greater than a medium level will be risk mitigated and any weaknesses identified will be rectified.
High	G8 accepts a **high** amount of this risk occurring. Risk occurring will only be risk mitigated and any weaknesses identified, rectified where they fall outside of the high tolerances.

2.4 Three Lines of Defence

G8 adopts the internationally recognised Three Lines of Defence Model.

G8 Three Lines of Defence Model

Line	Who	Responsibilities
First Line	Centre Managers, Area Managers, Regional Managers, Support office operational teams	Monitor and manage all material risks consistent with the strategic objectives, risk appetite statement and policies approved by the Board. Identify and manage risk within day-to-day operations. Ownership and responsibility for maintaining effective internal controls. Comply with risk management policies and processes. Foster and demonstrate positive risk culture. Implement corrective actions to address process and control gaps.
Second Line	Legal, Quality Assurance, Risk, WHS, Child Protection, ECEC Compliance	Implementation and maintenance of the risk management framework.

		Provide advice to leadership teams regarding the management and reporting of risk. Verification and oversight of the first line, that risks are being managed against agreed processes and controls. Provide transparent reporting on the management of risk to the Board. Provide internal assurance that compliance mechanisms are in place. Monitor risk registers for alignment within the approved risk appetite and strategy. Oversee internal Quality and Compliance Audits and reviews Support escalation.
Third Line	Internal Audit/External Audit	Provide independent assurance on the adequacy and effectiveness of risk management, governance and internal controls (Internal Audit) Provides assurance over Financial Reporting and associated controls and areas of regulatory exposure relevant to financial statements (External Audit).

2.5 Risk Culture

G8 promotes a strong, constructive and open risk culture in which all team members understand their responsibilities for identifying, assessing and managing risk, raising concerns early, and acting in accordance with legal, ethical and professional standards.

Risk culture is reflected in the behaviours, decisions, systems and leadership practices that shape how risk is understood and managed across the organisation.

A positive risk culture at G8 is demonstrated by:

- the prioritisation of child safety and wellbeing in all decisions
- consistent escalation of concerns, hazards and incidents
- transparent and accurate reporting without fear of blame or repercussion
- early identification of emerging risks
- active use of centre, functional and enterprise risk registers
- willingness to challenge unsafe practice or assumptions
- informed decision-making aligned to risk appetite
- learning from incidents, audit findings and systemic issues
- leadership modelling of expected behaviours and standards.

Risk culture is influenced by the environment G8 creates, including structures, governance, training, communication and leadership behaviours. The Framework, associated policies, Three Lines of Defence Model and operating rhythms all reinforce positive risk culture.

G8 recognises that strengthening risk culture requires consistent reinforcement and the alignment of systems, incentives, accountability and information flows.

2.6 Risk Culture Enablers

The following organisational mechanisms support the development and maintenance of a constructive risk culture across all levels of G8.

Enablers	Actions
Leadership and Tone From the Top	Board and Executive demonstrate visible commitment to risk management and child safety. Senior leaders consistently model expected behaviours and decision-making. Leaders reinforce the importance of speaking up and escalation.
Integration With Strategy and Operations	Risk is embedded into planning, budgeting, projects and operational decision-making. Enterprise risks inform strategic decisions at Board and Executive level. Operational risks inform resource allocation and centre practices.
Clear Expectations and Accountability	Roles and responsibilities for risk management are clearly defined through the Framework and Three Lines of Defence. Consequences for failing to follow risk management processes are understood. Teams are recognised for proactive risk identification and effective control management
Training and Capability Building	Mandatory training for all team members on child safety, WHS, privacy, cyber security and core operational risks. Coaching and support for Centre Managers, Area Managers and Regional Managers to develop risk assessment capability. Functional training aligned to specialist risk areas (e.g., cyber, regulatory, HR, finance)
Accessible Processes, Systems and Tools	Simple, usable templates and registers to support consistent risk assessment. Technology that enables accurate documentation, escalation and monitoring.

Enablers	Actions
	Streamlined reporting mechanisms that reduce administrative burden
Open Communication and Safe Escalation	Regular forums for discussing risks, controls and lessons learned. A culture where concerns can be raised without blame or retaliation. Transparent communication of changes to risks, controls and obligations
Continuous Improvement and Learning	Regular reviews of incidents, hazards, complaints and regulator findings. Data-driven decision-making using KRIs, audit results and operational insights. Updates to processes and controls following lessons learned.

2.7 Cultural Safety and Child Safe Principles

G8 is committed to providing culturally safe environments for all children, including Aboriginal and Torres Strait Islander children. Cultural safety must be incorporated into all stages of the risk management process.

Cultural Safety Requirements

Area	Requirements
Environment	Spaces, routines and interactions should support cultural identity and safety.
Educator Capability	Team members should be culturally competent and trained in trauma-informed approaches.
Engagement	Respect for family culture, identity and protocols integrated in communication and decision-making.
Incident Response	Cultural considerations inform responses to risk, harm or disclosures.

3. ROLES AND RESPONSIBILITIES

Risk management requires clear responsibility across centres, regional, functional and enterprise levels. These responsibilities complement, but do not replace, legislative duties.

Roles and Responsibilities

Role	Responsibilities
Centre Manager	Maintains centre risk register Implements daily/weekly/monthly checks

Role	Responsibilities
	Completes hazard and incident reporting Ensures supervision, ratio and WHS compliance Implements treatments Escalates risks outside appetite or with systemic indicators.
Area Manager	Reviews centre risk assessments and registers Validates quality of assessments Identifies systemic risks across area Coaches Centre Managers Conducts spot checks Escalates risk issues to Regional Manager.
Regional Manager	Consolidates regional risks Monitors systemic patterns across centres Ensures leadership capability Supports complex risk treatment actions Escalates significant risks to Chief Operating Officer
Functional Senior Leaders *with risk management responsibilities	Maintains and reviews functional risk register (with support from Risk function) Ensures effective controls Monitors KRIs Escalates high risks to ELT Ensures compliance within their portfolio.
Executive Leadership Team	Owns enterprise risks Approve and monitor treatment plans Assess risk tolerance breaches Allocates resources Reviews risk trends and systemic issues.
Chief Legal, Quality & Risk Officer	Maintains enterprise risk register Oversees risk methodology and systems Monitors and reports emerging risks Prepares reporting for ELT, ARMC and Board.
Internal Audit	Provides independent assurance on the design and operating effectiveness of controls as per the Annual Internal Audit Plan (approved by the ARMC). Allowance is included in the plan for management requests for areas of focus or concern arising throughout the year.

Role	Responsibilities
External Audit	Provides an opinion on the truth and fairness of the half year and annual financial report (including ESG reporting) and assesses the management of risk and key internal control systems in providing their opinion as per the External Audit Plan (approved by the ARMC).

4. G8 RISK MANAGEMENT SYSTEM

The G8 Risk Management System provides the structure and processes that guide how risk is identified, assessed, managed, escalated and monitored across all levels of the organisation. It integrates enterprise governance, operational controls, reporting, business continuity, functional oversight and assurance.

The system comprises:

- Hierarchies of risk management across the Group
- Risk information and escalation flows
- Integration with business continuity, emergency management and disaster recovery
- Governance roles
- Supporting technology and documentation

4.1 Hierarchies of Risk Management

Risk management at G8 occurs at four levels: enterprise, functional, operational and project. These levels ensure risks are appropriately owned and managed at the point of origin while allowing enterprise-level oversight of material and systemic risks.

Levels of Risk Management

Level	Description	Details
Enterprise Level	Organisation-wide risks owned by the Executive Leadership Team and overseen by ARMC and the Board. These risks typically have cross-functional impacts, strategic importance or regulatory materiality.	Enterprise Risks (see section 2.2 above)
Functional Level	Risks specific to a portfolio, team or discipline. Functional leaders maintain registers, operate controls and escalate as required. Typically these risks are sub-risks of an Enterprise Risks	Sub-risks of Enterprise Risks managed at a functional level e.g. Risk of Ineffective Training (P&C), Risk of Poor System Access Controls (Technology), Risk of Incorrect Models (Finance) etc.
Operational Level	Centre and regional risks linked to daily operations. Centre Managers, Area Managers and Regional Managers lead risk identification, assessment, escalation and treatment.	Primarily linked to Child Safety, Health Safety and Well Being and Regulatory and Compliance Enterprise Risks e.g. supervision; ratio compliance; WHS hazards; facility condition; critical incidents.

Level	Description	Details
Project Level	Risks associated with major projects, systems implementations, integrations and transformations. Project teams identify, assess and manage project risks, reporting to the sponsor and governance body.	Examples include major IT implementations; new service rollouts; network optimisation at scale; transformation initiatives.

4.2 Risk Information Flow

A consistent and reliable flow of risk information ensures escalation, accountability, transparency and oversight. Escalation pathways must be followed for risks outside appetite, systemic issues, critical incidents and notifiable events.

Risk Information Flow

Information Flows FROM	Information Flows TO	Purpose
Centre Manager	Area Manager	Communicate centre-level risks, incidents, hazards, treatments and resource needs. Seek guidance on tolerance breaches or systemic issues.
Area Manager	Regional Manager	Validate centre-level risks, consolidate trends, identify patterns and supervise risk quality.
Regional Manager	Chief Operations Officer	Provide regional summaries; escalate systemic issues; raise material operational challenges; seek enterprise support.
Chief Operations Officer	Chief Legal, Quality & Risk Officer	Escalate high or cumulative risks; ensure visibility of systemic issues; support allocation of enterprise resources.
CLQRO	Executive Leadership Team	Provide consolidated enterprise risk reporting; highlight risk tolerance breaches; present control design or effectiveness concerns; identify emerging risks.
ELT	ARMC and Board	Provide strategic risk oversight; ensure major risks, systemic issues and residual exposures are understood and overseen.
Internal Audit	ARMC and Board	Provides independent reporting on management of risks and effectiveness of internal controls
External Audit	ARMC and Board	Provides independent report on management of risks and effectiveness of internal controls in forming an opinion on the truth and fairness of half year and full year financial reports (including ESG reporting)

This flow supports timely escalation, accountability and accuracy of organisational risk insights.

RISK RATING	NEWLY IDENTIFIED RISK OR EXISTING RISK RATING CHANGES	
	NOTIFICATION	**ACTION**
Extreme	**Reported immediately to the CEO and Chief Legal, Quality & Risk Officer who will then notify the Board within 24 hours (as appropriate)**	• Immediate and urgent Executive management action required. • Monitor daily. • Cease activity until risk can be reduced to an acceptable level. Activity shall not be undertaken without the express approval from CEO, ratified by the Board Chair within a reasonable time.
High	**Reported to relevant Executive within 48 hours who will notify the CEO and Chief Legal, Quality & Risk Officer**	• Executive Leadership attention required immediately. • Weekly monitoring. • The activity shall not be undertaken without the express approval of Executive Leadership.
Moderate	**Reported to the Responsible Manager then reported to the relevant Executive**	• Executive Management attention required. • Action plans developed and implemented, and accountability specified. • Manage by routine procedures and business-as-usual processes.
Low	**Reported to the Responsible Manager**	• Manage by routine procedures and business-as-usual processes. • Unlikely to need specific application of resources. • Monitor as appropriate

4.3 Integration with Business Continuity and Emergency Management

G8's risk management system is tightly integrated with:

- Business Continuity Plans (BCPs)
- Emergency Management Plans (EMPs)
- Disaster Recovery Plans (DRPs)
- Crisis Management Framework (CMF)

These frameworks collectively ensure G8 can prepare for, prevent, withstand, respond to and recover from disruptive events affecting operations, technology, workforce or facilities.

Integration of Risk and Continuity Functions

Continuity Component	Description	Integration with Risk Management
Business Continuity Plans (BCPs)	Plans for maintaining critical operations during disruptions such as facility inaccessibility, key system outages or workforce shortages.	Operational risks relating to business disruption reference BCP capability and treated in alignment with BCP priorities and responsibilities. Residual risk informs BCP design.

Continuity Component	Description	Integration with Risk Management
Emergency Management Plans (EMPs)	Centre-level plans addressing emergency procedures including evacuation, lockdown, fire and critical incidents.	EMP controls reflected in centre-level risk registers. EMPs tested and updated following incidents or environment changes.
Disaster Recovery Plans (DRPs)	ICT system recovery strategies governing the restoration of technology capabilities.	Cyber and technology risks reference DRP capabilities, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
Crisis Management Framework (CMF)/Serious Incident Response Team (SIRT)	Enterprise-level response structure for major or complex events that require coordinated leadership and communication.	Residual risks assessed as extreme or outside appetite may trigger assessment under the CMF/SIRT. Escalation to the ELT and Board occurs as per Crisis Management/SIRT framework

4.4 Documentation Requirements

Risk management at G8 is supported by documented templates, processes and tools including:

- Centre risk registers
- Functional risk registers
- Enterprise risk register
- Treatment plan templates
- Escalation pathways
- Incident reporting mechanisms
- Business continuity documentation
- Emergency management documentation
- Disaster recovery documentation
- Key Risk Indicator (KRI) dashboards

Documentation is maintained in approved G8 systems and updated promptly after any operational, environmental or regulatory change.

4.5 Responsibilities for Maintaining the Risk Management System

The ongoing effectiveness of the risk management system relies on coordinated responsibilities across the organisation.

Responsibility for the Risk Management System

Role	Responsibilities
Centre Manager	Maintain up-to-date centre risk registers Ensure documentation reflects operational reality

Role	Responsibilities
	Update after incidents, hazards or changes Ensure alignment with emps.
Area Manager	Validate the quality of centre documentation Ensure consistency across centres Ensure alignment with regional requirements.
Regional Manager	Consolidate operational risks Ensure risks are escalated Ensure documentation supports regional oversight.
Functional Senior Leaders ***with risk management responsibilities**	Maintain functional registers Ensure alignment with enterprise risks Ensure documentation supports internal and external audit requirements.
CLQRO	Maintain enterprise risk documentation Ensure processes align with ISO 31000 and ASX Principle 7 Maintain risk tools and templates.
Internal Audit	Review documentation quality as part of assurance activities.

4.6 Operating Rhythm

Risk management activities occur within an operating rhythm that ensures visibility, oversight and accountability.

Operating Rhythm

Level	Frequency	Required Activities
Centre Level	Daily / Weekly / Monthly	Environment and equipment checks Hazard identification Incident management Risk register updates Monthly review with Area Manager.
Area Level	Monthly	Review and validate centre risk registers Identify systemic risks Coach Centre Managers.
Regional Level	Monthly	Consolidate risk information Escalate systemic trends Review resource needs.

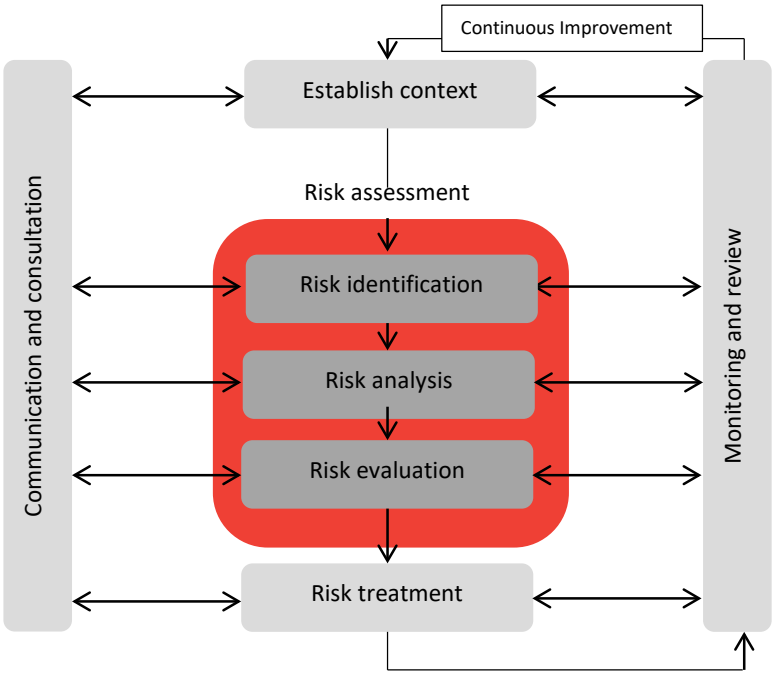
Level	Frequency	Required Activities
Functional Level	Quarterly	Review functional risk registers and KRIs Update mitigation plans.
Enterprise Level	Quarterly	ELT review of enterprise risk profile ARMC oversight Board reporting.

5. RISK MANAGEMENT PROCESS

G8 applies the seven-step ISO 31000 risk management process across all centres, regions, functions and enterprise activities.
This process provides consistency, transparency and disciplined decision-making.

The seven steps are:

1. Establish context
2. Identify risks
3. Analyse risks
4. Evaluate risks
5. Treat risks
6. Monitor and review
7. Communicate and consult



5.1 Step 1: Establish Context

Establishing context ensures risk assessments reflect operational reality, regulatory requirements, and organisational objectives.

Key activities include:

- understanding relevant legislation, standards and obligations
- assessing centre environment, layout and conditions
- clarifying operational or project objectives
- assessing staffing, resources and operating constraints
- understanding technological dependencies

- reviewing past incidents and performance

Establishing Context – Example of Context for Centre Assessment

Activity	Requirement	Responsible Role	Tools / Inputs
Identify relevant obligations	Consider NQF, WHS, privacy, mandatory reporting and other legal obligations.	Centre Manager / Functional Lead	Legislation summaries; regulatory notices.
Assess environment	Review layout, blind spots, equipment condition, outdoor areas, evacuation routes, sleep/rest spaces.	Centre Manager	Environment risk assessment; safety checklists.
Confirm objectives	Understand operational, program or project objectives and performance requirements.	Centre Manager / Functional Leader / Project Manager	Annual operational plans; project charters.
Identify constraints	Assess staffing, resources, budget, system limitations, seasonal pressures.	Centre Manager / Area Manager	Rostering data; workforce plans.
Identify dependencies	Identify reliance on suppliers, IT systems, facilities or other functions.	Centre Manager / Functional Leader	Supplier list; asset registers; IT system dependencies.

5.2 Step 2: Identify Risks

Risk identification must be comprehensive and ongoing.

Risk Identification Methods - – Example of factors for Centre Assessment

Method	Description	Responsible Role
Incidents and near misses	Review causes, context and potential recurrence.	Centre Manager / WHS / Child Protection / Functional Leaders
Hazard reporting	Identify unsafe conditions, faulty equipment, environmental hazards or behavioural indicators.	Centre Manager / All Team Members
Observations	Daily supervisory observations of environment, interactions, routines and safety.	Centre Manager / Area Manager / Regional Manager
WHS and Quality audits	Identify compliance gaps or systemic issues.	Second Line (Quality, WHS, Compliance)
Data and system analysis	Analyse IT logs, system outages, attendance patterns, staffing data, ratios, trends.	Functional Leaders (IT, HR, Safety)

Method	Description	Responsible Role
Regulatory updates	Identify new obligations or changes requiring updated controls.	CLQRO / Legal / Compliance
Project risk reviews	Assess risks during project planning, implementation and review stages.	Project Manager / Sponsor
Feedback from families and team members	Identify emerging concerns impacting safety or operational performance.	Centre Manager

Risk identification must be proactive, not solely reactive.

5.3 Step 3: Analyse Risks

Risk analysis determines how likely the risk is to occur and the impacts if it does.

Analysis must consider:

- causes (immediate and systemic)
- consequences (multiple impact areas)
- existing controls
- control effectiveness
- inherent and residual risk levels

Risk Analysis Components

Component	Requirement	Tools / Inputs
Causes	Identify immediate triggers and underlying systemic causes.	Incident reports; hazard forms; RCA tools.
Consequences	Assess impacts on child safety, WHS, regulatory compliance, financial performance, operations, reputation and environment.	Consequence scale.
Likelihood	Determine how frequently or easily the risk could occur based on data, environment and historical patterns.	Likelihood scale; incident history.
Existing controls	Identify preventative, detective and corrective controls currently in place.	Control library; centre procedures; system safeguards.
Control effectiveness	Assess controls as Effective, Partially Effective or Ineffective.	Audit findings; testing; observations.
Inherent risk	Risk level before applying controls.	Risk matrix.
Residual risk	Risk level after applying controls.	Risk matrix; control effectiveness evaluation.

An assessment of the control's current **operating effectiveness** should be determined using the criteria below.

Rating	Definition	Characteristics
Effective	The control is operating effectively to reduce, mitigate or detect unexpected risk in most circumstances.	• Control is formally documented and understood by all team members. • Control is occurring on a regular basis but less structured. • Control will mitigate an inherent risk to an acceptable level of current risk in most circumstances.
Partial Effective	The control in place is partly functional and needs to be improved for it to mitigate or detect basis risk.	• Control is not formally documented although it is reasonably understood by team members. • Control is informal and tends to occur on an ad hoc basis. • Control will mitigate the inherent risk to some extent.
Ineffective	The control is not operating effectively as such there is no assurance that the risk will be controlled.	• Team members are not aware of or do not understand the control. • There is no control monitoring in place. • The control will not mitigate the current risk to an acceptable level.

5.4 Step 4: Evaluate Risks

Evaluation compares residual risk levels to the Board-approved risk appetite/risk tolerance. This determines whether a risk is acceptable, requires mitigation or treatment or must be escalated.

Risk Evaluation Requirements

Residual Risk Position	Required Action
Within appetite	Accept Record in risk register Monitor routinely.
Approaching appetite	Strengthen controls Increase frequency of monitoring Update treatment plan.
Outside appetite	Escalate immediately to Area Manager (centre risk), Regional Manager (regional/systemic risk) or Functional Leader (portfolio risk). Treatment plan required.
Extreme residual risk	Immediate escalation to ELT and CLQRO Assess for crisis management implications.

5.5 Step 5: Treat Risks

Risk treatment involves deciding how to modify the risk to achieve an acceptable residual level.

Treatment must:

- address root causes
- include clear actions, owners and deadlines

- identify required resources
- include measurable success criteria
- be monitored and reviewed

Risk Treatment Options - Treatment plans are mandatory for risks outside appetite/tolerance.

Treatment Option	Description	Examples
Avoid	Discontinue or avoid the activity causing the risk.	Closing an unsafe play area Discontinuing a high-risk supplier.
Reduce	Modify likelihood or consequence via additional controls.	Training Process redesign Technology safeguards Supervision improvements.
Transfer	Shift responsibility or financial impact to another party.	Insurance Outsourcing Contractual risk allocation.
Accept	No further action required if within appetite.	Document rationale Continue monitoring.

5.6 Step 6: Monitor and Review

Monitoring ensures risks, controls and treatments remain effective over time. It occurs at centre, area, regional, functional and enterprise levels.

Monitor and Review Requirements

Level	Frequency	Required Activities
Centre Level	Daily / Weekly / Monthly	Perform environment checks Update risk register Review incidents Complete WHS and child safety checks Discuss risks with Area Manager.
Area Level	Monthly	Review centre risk registers Validate quality Identify systemic issues Coach Centre Managers Escalate where required.

Level	Frequency	Required Activities
Regional Level	Monthly	Consolidate risk information Identify recurring patterns Escalate systemic issues to GM Operations and functional leads.
Functional Level	Monthly	Review functional risk registers and kris Update treatments Escalate appetite breaches.
Enterprise Level	Quarterly	ELT risk review ARMC oversight Board reporting Emerging risk analysis.

5.7 Step 7: Communicate and Consult

Communication and consultation are integral to each step of the process. They ensure all stakeholders understand risks, controls and responsibilities.

Communication Requirements

Role	Communication Requirements	Frequency
Centre Manager	Incidents, hazards, emerging risks, register updates.	Immediate / Weekly / Monthly
Area Manager	Trends, systemic issues, quality concerns, high-risk cases.	Monthly
Regional Manager	Regional summaries, resource needs, appetite breaches.	Monthly
Functional Leader	Portfolio risks, compliance updates, KRI insights.	Monthly / Quarterly
CLQRO	Enterprise risk updates, appetite breaches, systemic issues, emerging risks.	Quarterly
ELT	Strategic risk analysis, oversight reporting to ARMC and Board.	Quarterly
Internal Audit	Quarterly report to ARMC	Quarterly
External Audit	Half Year and Full Year report and interim reporting to ARMC and Board	Quarterly

Consultation is required when:

- environments change
- new activities commence
- new regulations arise

- treatments require functional support
- system changes or disruptions occur.

6. RISK REGISTERS AND REPORTING

Risk registers form the core documentation for capturing risk assessments, controls, treatments and monitoring activities. All risk registers must be:

- accurate
- current
- complete
- consistently maintained
- aligned across centre, functional, regional and enterprise levels

Risk registers are maintained at:

- Centre level
- Area level (through review and validation)
- Regional level (consolidation)
- Functional level
- Enterprise level

All registers must use G8-approved formats and systems.

6.1 Mandatory Risk Register Fields

Each risk entry must contain the following information.

Mandatory Register Fields

Field	Requirement
Risk ID / Title	Clear, meaningful name reflecting the nature of the risk.
Enterprise Risk Category	Linkage to one or more of the G8 enterprise risk categories.
Sub-risk Classification	Specific operational or functional sub-risk.
Description	Brief explanation of the risk scenario.
Causes	Immediate and underlying systemic causes.
Consequences	Potential impacts across safety, regulation, financial, operational and reputational domains as per the Risk Matrix.
Existing Controls	Preventative, detective and corrective controls currently in place.

Field	Requirement
Control Effectiveness	Rated Effective, Partially Effective or Ineffective.
Inherent Risk Rating	Before considering existing controls.
Residual Risk Rating	After considering existing controls.
Risk Appetite Position	Within, approaching or outside appetite.
Treatment Actions	Required activities, owners, due dates and resources.
Owner	Primary individual accountable for the risk.
Status	Open, in progress, complete or closed.
Review Date	Mandatory review frequency.

6.2 Technology and System Support

Risk documentation must be recorded in G8's approved systems. Technology supports:

- centralised register maintenance (currently via sharepoint)
- secure access control
- workflow and action tracking (manual)
- dashboards showing KRIs (Excel and powerBI)
- version control
- consistent templates
- audit trails

If systems are unavailable, manual temporary records must be maintained and uploaded within **24 hours** of system restoration.

6.3 Escalation Requirements

Risks must be escalated according to severity, trends, appetite position and regulatory requirements.

Example Escalation Pathways

Trigger	Escalation Pathway
Child protection incident / allegation	Centre Manager → Area Manager → Regional Manager → Child Protection → CLQRO
WHS notifiable incident	Centre Manager → Area Manager → Regional Manager → WHS → ELT
Serious data breach or cyber event	IT Security → CLQRO → ELT

Trigger	Escalation Pathway
Supplier failure affecting safety or continuity	Functional Leader → GM Operations → ELT
Risk outside appetite/tolerance	Centre/Functional owner → Area/Functional Manager → CLQRO
Repeated incidents or systemic patterns	Centre Manager → Area Manager → Regional Manager → Functional Leaders
Significant trend shifts (KRIs)	Functional Leader → ELT
Regulator enforcement action	Legal / Compliance → CLQRO → ELT

Escalation must occur immediately when harm, regulatory breach or serious operational disruption is present.

7. ASSURANCE

Assurance activities verify that risk controls and processes are designed and operating effectively. Assurance is delivered through the Three Lines Model.

7.1 First Line Assurance

Operational teams maintain day-to-day controls and perform checks, including:

- supervision and safety checks
- hazard identification
- ratio compliance
- centre environment assessments
- process adherence
- completion of training requirements
- reporting of incidents and near misses

7.2 Second Line Assurance

Second line functions monitor compliance and provide oversight through:

- regulatory compliance audits
- WHS audits
- quality reviews
- child protection case reviews
- cyber security monitoring
- policy and process oversight
- trend analysis and reporting

7.3 Third Line Assurance (Internal Audit)

For topics included in the annual Internal Audit Plan, Internal Audit provides independent assurance over:

- risk management effectiveness
- control design and operation
- compliance with regulatory obligations
- management of high-risk processes
- financial and operational controls

Internal Audit reports directly to the ARMC through the Chief Legal, Quality and Risk Officer.

7.4 External Assurance and Regulatory Oversight

External assurance includes:

- External financial audits
- Early years regulatory authority assessment and rating
- Food safety audits
- Fire and building inspections
- WHS regulator interventions
- Privacy commissioner reviews
- Independent cyber penetration testing
- Specialist reviews commissioned by G8 or the Board

External Assurance Integration Requirements

Assurance Type	Required Risk Management Action
Regulatory assessment or rating	Findings reviewed for systemic risk implications; updates made to relevant registers.
Regulator enforcement action	Immediate escalation to CLQRO and ELT; root cause analysis performed; treatment plan implemented.
External audit report	Material findings linked to enterprise risks; treatments monitored.
Specialist external review	Recommendations added as treatment items and tracked.

8. CONTINUOUS IMPROVEMENT

G8 is committeed to continuous improvement in risk management. Improvements to processes, systems or behaviours contribute to strengthening G8's overall risk culture
Sources of improvement include:

- incident reviews
- hazard trend analysis
- regulator findings
- internal and external audits
- KRI data

- lessons learned from emergencies or continuity events
- system changes
- annual Framework review

Improvements may lead to updates to processes, controls, training, documentation or technology.

9. SUPPORTING DOCUMENTS

This Framework should be read in conjunction with:

- G8 Risk Management Policy
- Risk Matrix (defines consequence, likelihood and risk rating at enterprise level)
- Risk Appetite Statement and Risk Tolerances (defines appetite and tolerances as set by the Board)
- Enterprise Risk Register
- Emerging Risk Assessment Template
- Project Risk Assessment Template
- Centre Risk Assessment Templates (including Environment, Supervision and Safe Sleep)
- Child Protection and Safety Policies
- Incident Management Procedure
- WHS Policy
- Business Continuity Policy and Plan
- Delegations of Authority
- Information Security Policy

10. FRAMEWORK REVIEW

This Framework is reviewed annually by the Audit & Risk Management Committee (ARMC) and updated in response to internal audit findings, regulator review outcomes, emerging risks, sector developments and organisational learning.

11. DEFINITIONS

Term	Definition
Consequence	G8's assessment of the impact or outcome of an event. There can be more than one consequence from one event. Consequences can range from positive to negative. Consequences can be expressed qualitatively or quantitatively. Consequences are considered in relation to the achievement of objectives.
Control	Any process, policy, device, practice, or action taken by management, the Board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

Term	Definition
Cost	Of activities both direct and indirect, involving any negative impact, including money, time, labour, disruption, and goodwill, political and intangible losses.
Contingency	Budget (cost benefit) or time (duration) that may be used in the event of a risk occurrence.
Enterprise risk	Risks which have the ability to impact the achievement of the organisation's strategic objectives.
Event	An incident or situation, which occurs in a particular place during a particular interval of time. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences.
Frequency	A measure of the rate of occurrence of an event expressed as the number of occurrences of the event in a given time. See also Likelihood and Probability.
Hazard	A source of potential harm or a situation with a potential to cause loss.
Incident Management	Systems and processes that provide for an organisational structure capable of responding to all levels of emergency from simple to complex.
Likelihood	Used as a qualitative description of probability or frequency of a risk occurring.
Loss	Any negative consequence financial or otherwise. Can be differentiated as follows: Maximum foreseeable loss – highest possible loss after considering key controls. Maximum possible loss – highest possible loss without considering key controls.
Monitor	To check, supervise, observe critically, or record the progress of an activity, action, or system on a regular basis in order to identify change.
Organisation / Enterprise	Group of people and facilities with an arrangement of responsibilities, authorities, and relationships. In this document, 'organisation' or 'enterprise' refers to G8 Education.
Policy	G8 documented policy including overarching governance principles and approach.
Probability	The likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes, to the total number of possible events or outcomes.
Procedure	G8's documented procedures including flowchart of steps/tasks, timing of steps/tasks, who is responsible for steps/tasks. All G8's procedures are linked to and reference a G8 Policy.
Reasonable Assurance	The concept that enterprise risk management, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met. This is because of inherent limitations in all risk management systems.
Risk	The effect of uncertainty on objectives. Risk may have a positive or negative impact. Risk is measured in terms of impact and likelihood.
Risk acceptance	An informed decision to accept the consequences, and the likelihood of, a particular risk.
Risk acceptance criteria	Management's formal establishment of criteria or boundaries designed so that the residual risk does not exceed the selected range of financial and operating outcomes.

Term	Definition
Risk analysis	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk appetite	The amount of risk, on a broad level, that G8 is willing to accept in pursuit of objectives.
Risk assessment	The overall process of risk identification, analysis and evaluation.
Risk avoidance	An informed decision not to become involved in a Situation or activity that presents risk.
Risk category	Commonly grouped risks, e.g. reputation, operations, financial.
Current risk	The remaining risk after management has taken action to alter the risk's likelihood or impact. The rating of risk once existing controls has been taken into account.
Risk evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk identification	The process of determining what can happen, why, when where and how.
Risk Management	Co-ordinated activities to direct and control an organisation with regard to risk.
Risk Management Framework	The set of elements of an organisation's management system concerned with managing risk. Also, the document established by policy which provides the detailed explanation of processes, tools and roles and responsibilities.
Risk Management Process	The systematic application of policies, procedures, and practices to establish context, identify, analyse, evaluate, treat, monitor and communicate risk.
Risk Management System	The totality of the culture, structures, methodology, procedures, and definitions that an organisation has chosen to use to implement its Risk Management processes.
Risk Register	The summary report of all individual risks within each assessment, which include risk ratings (current and target), level of control, risk decision, risk owner and summary of key controls and/or mitigating actions.
Risk Tolerance	The maximum level of risk that is acceptable to the board or management. This may be set for the organisation as a whole, for different groups of risks or at an individual risk level.
Risk Treatment	Process of selection and implementation of measures to modify risk.
Stakeholders	Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.
Target risk	The level of risk G8 plans to achieve with the implementation of additional or different controls.