America's Cup 36 Programme Risk Management Framework

Version: 0.1

Date Approved: 22 August 2018

Approved by: AC36 Joint Chief Executive Group

Owner: Cecilia Tse, Programme Risk Lead

Approval

Prepared by. (Name)	Position	Signature and date
Shivali Kukreja	Principal Risk Advisor	13/8/18
Reviewed by. (Name)	**Position**	**Signature and date**
Cecilia Tse	Head of Risk	13/8/18
Approved by (Name)	**Position**	**Signature and date**
Joint Chief Executive Steering Group		22 August 2018

Amendments

Date	Revision No.	Amendment Description	Review By	Approved By

Contents

Appendices	Page

1. Introduction

Emirates Team New Zealand Limited (ETNZ), the winners of the 35th Americas Cup, were awarded the rights to select the host location for the 36th America's Cup (AC36). Auckland, New Zealand has been appointed by ETNZ to host the 36th America's Cup.

The America's Cup 36 (AC36) programme includes the delivery of infrastructure, event, legacy and leverage through a collaborative approach between Auckland Council Group (ACG), Ministry of Business, Innovation and Employment (MBIE) on behalf of the Crown, Americas Cup Event Limited (ACE), Wynyard Edge Alliance and Mana Whenua.

The AC36 programme objectives are:

- provision of a safe environment for the public and staff (including contractors and volunteers) to achieve zero harm;
- deliver an exceptional event experience for participants, spectators, public and all other stakeholders to enhance Auckland, New Zealand's reputation as a desirable destination of future major events and a hub for growth and business opportunities;
- community participation from whole of New Zealand, including youth, Maori and Iwi;
- meet or exceed expectations regarding project budget, timeframes, scope, quality and sustainability of infrastructure;
- develop and maintain strong and collaborative relationships;
- maximise social and economic benefits, including innovation and technology, quality jobs, youth pathways and education; and
- leave a legacy that all stakeholders, partners and the people of Auckland and New Zealand can be proud of.

The AC36 Joint Chief Executive Group (JCEG), with representations from ACG, MBIE, ACE and Mana Whenua, will oversee the delivery of the end-to-end AC36 programme, including effective risk management.

The AC36 programme governance structure depicts the interim workstreams, governance and oversight groups and reporting lines (as included in Appendix 1). The interim Risk Workstream, led by Auckland Council (as approved by JCEG in May 2018), is responsible for the development of the risk management framework and to provide leadership, guidance and oversight for risk management activities across the programme.

2. Purpose

Risk management activities are an integral component of programme and project management as it improves decision-making, supports the achievement of objectives and enhances performance and outcomes.

The purpose of this document is to outline the AC36 programmes risk management principles, framework and processes including:

- confirming JCEG's commitment to adopting an integrated, consistent and structured programme-wide approach to effectively manage risks, issues and incidents;
- supporting the development of a positive risk culture;
- requirements for identifying, assessing, managing and reporting risks; and
- clarifying roles and responsibilities regarding the management of risk.

3. Context

The 36th America's Cup, comprising of three key events to be held over the period December 2020 - March 2021, are of great significance to New Zealand and its reputation, has multiple stakeholders and involves substantial funding from Auckland Council and the Crown.

The infrastructure required for AC36 will be delivered under a collaborative alliance model, as detailed under the Interim Project Alliance Agreement (IPAA). The IPAA is between Auckland Council, the Crown through MBIE and Wynyard Edge Alliance (Downer NZ Ltd, McConnell Dowell Constructors Ltd, Beca Ltd and Tonkin & Taylor Ltd). The planning, design and construction of the AC36 venue has many complexities and involves marine works (breakwaters, pontoons and wharf extensions and repairs) and land-based works including the removal of redundant industrial bulk storage tanks and associated infrastructure from Wynyard Point and addressing existing contamination.

ETNZ has established America's Cup Event Limited (ACE) to undertake its event management responsibilities in collaboration with Auckland Council Group. The Host City Appointment Agreement (HCAA) is shared between Auckland Council and MBIE, collectively referred to as the Hosts and ACE.

The HCAA and IPAA sets out each party's obligations in relation to AC36 infrastructure and event deliverables.

All infrastructure works will provide a legacy beyond the event, facilitating the future development of Wynyard Point, by providing and improving berthage in the Wynyard area. The construction period overlaps with several other infrastructure projects in the vicinity, including City Rail Link, private developments in Wynyard Quarter, and the Quay Street development programme.

In addition, there are several statutory and regulatory obligations that must be met. This includes obtaining consents, oversight and review of the emergency services requirements (police, ambulance, fire services, civil aviation). Some of the key legislations applicable to AC36 are set out in **Appendix 2**.

4. Risk Management Principles

JCEG is committed to the following principles of risk management, which are fundamental to achieve the AC36 programme wide objectives:

Risk management	How is it applied?	Why is it important?
1. Creates and protects value	• incorporated into governance framework • considered as part of programme culture	• contributes to the achievement of objectives • assists to improve performance • protects assets and community interests • adds value for sustainable infrastructure development
2. Is an integral part AC36's planning and management process	• integrated into programme planning (strategic, operational, financial) • part of change management processes	• avoids duplication • guides prioritisation • clarifies responsibilities
3. Is part of decision making	• built into approval processes • explicitly incorporated into projects, system design and changes and resource allocation • part of all contractual agreements • part of staff recruitment and employment arrangements	• assists decision makers to make informed choices • assists to prioritise actions • distinguishes among alternative courses of action
4. Explicitly addresses uncertainty	• used to develop descriptions for risk rating criteria (i.e. likelihood and consequence) • linked to assessing objectives	• explicitly identifies uncertainty in the programme's internal and external contexts • promotes a shared view of risks and risk appetite • identifies vulnerabilities and risk treatments

5. Is systematic, structured and timely	• incorporated into the design of all systems rather than a stand-alone process • consistently applied through clear guidance • measured and reported	• contributes to a consistent and efficient approach • facilitates comparability of results and benchmarking • promotes consistent understanding • establishes clear channels for communication and consultation
6. Is based on best available information	• advice and support for risk management is available • specifies the functional requirements of risk framework and processes process • used to accurately define uncertainty and ensure treatments are relevant	• stakeholders require accurate and reliable data to manage risk • risk attestation is supported • evaluates the effectiveness of controls • develops risk monitoring and reporting • risk management framework, tools, processes are fit-for-purpose
7. Is tailored	• the risk framework is designed and operated to fit with the AC36 Programme's context and capabilities	• aligns with AC36 Programme' external and internal context and risk profile • consistent with AC36 Programme's culture • adequate resources are allocated • ensures compliance with legal obligations
8. Takes human and cultural factors into account	• the risk framework considers how people and cultures interact with its functions and how to monitor risk culture and behaviour	• aligns the capabilities and intentions of stakeholders with the AC36 objectives • ensures consistency between culture and behaviour
9. Is transparent and inclusive	• identifies scope and method for risk monitoring and reporting to stakeholders • identifies elements required in the risk criteria • identifies the role of stakeholders in the risk management process	• promotes line-of-sight of risks between all levels of the AC36 Programme • facilitates appropriate and timely involvement of stakeholders • ensures that risk management strategy remains relevant and up to date
10. Is dynamic, iterative and responsive to change	• incorporated into change management strategies • incorporated into programme and project management	• builds AC36 Programme resilience • ensures risk management process takes account of emerging risks • ensures the risk management framework is responsive to changes in context
11. Facilitates continual improvement	• risk management process is incorporated in continual improvement systems • risk attestation and the results of internal audit are used to inform continual improvement • stakeholder feedback is sought to influence continuous improvement of the risk framework and related activities	• improves programme risk maturity • addresses stakeholder expectations to protect assets and community interests • assists AC36 governance group and staff to meet obligations

5. Scope

In view of the above principles, and to enable a consistent and structured approach to risk management, the Risk Management Framework (RMF) is applicable to all employees, management, parties to legal agreements, contractors and volunteers appointed in the AC36 programme to deliver the infrastructure and the event.

6. Defining Risk, Opportunity and Risk Management

6.1. Risk

Risk is an uncertain event or condition that if it occurs has a positive or negative effect on one or more programme and/or project objectives (*AS/NZS ISO 31000:2018)*.

Delivery of AC36 objectives is surrounded by several uncertainties. The effect that uncertainty has on the achievement of AC36 objectives, gives rise to risks. Risk taking should be guided by the risk appetite and managed in accordance with the RMF.

It is important to note that issues and incidents are not risks. An issue is a current problem or concern influencing objectives. A risk can become an issue, but an issue is not a risk. Section 14 provides further details on issue and incident management.

6.2. Opportunity

An opportunity is something (tangible or an "effect") identified within the programme and/or project deliverables that could unlock or otherwise facilitate a positive or beneficial effect.

Managing project opportunities includes (at least) setting goals for projects based on business cases, adjusting project plans to align with overall objectives and working to realize potential benefits that might or might not occur. In all three cases, risk is a significant part of the picture. Opportunity management and risk management are interrelated.

When identifying uncertainties, scan for possible upside benefits, and where possible take actions to make realising the benefits more certain. All opportunities must be captured, assessed, recorded and reported.

6.3. Risk Management

Risk management is the combination of culture, systems and processes undertaken to coordinate the identification, assessment and management of risks and opportunities. This includes:

- adequate oversight, reporting, monitoring and assurance;
- identification and assessment of risks and taking action to manage them at an acceptable level;
- identification and assessment of opportunities and taking action to realising the benefits where possible;
- conducting controls self-assessment to identify weaknesses/gaps in controls and taking action to improve them; and
- the right capability and skills required to manage risks, issues and incidents across the programme.

7. Risk Management Framework

7.1. Risk Management Framework (RMF) Objectives

The objectives of the RMF are to:

Drive consistency	• Provide a comprehensive set of guidlines to ensure that the management of risks, issues and incidents are consistent across the AC36 programme
Enable cross-group collaboration	• Between Auckland Council Group, WEA, MBIE, ETNZ, ACE and other partners for effective management of risks
Support well informed decisions	• Enable stakeholders to implement well informed decisions rapidly
Drive accountability and ownership	• Provide guidance to all staff on their specific risk management responsibilities
Enable a risk aware culture	• Encourages staff to proactively identify risks, issues and/or incidents and associated opportunities, so that they can assess and respond to them.
Embed robust risk management practices	• Across all aspects of AC36 business and decision-making processes
Manage material risks of the AC36 programme	• Ensure that material risks are understood, managed, monitored, and escalated to the appropriate stakeholders
Maintain documents and records	• Specify appropriate documents to support the effective management of risks
Improve stakeholder confidence and trust	• Through regular communication mechanisms and effective, efficient and responsible management of risks

7.2. Framework Components

The RMF is based on the best practice risk management framework *AS/NZS ISO 31000:2018.*

This framework sets out the structure by which risk management should operate within the programme. It guides the management of all types of risk, including specific subjects, such as business continuity management; health and safety, inter-agency and state significant risks. In some cases, separate policies and procedures are in place to manage these specialist risk subjects.

To achieve the objectives outlined in section 7.1, the RMF consists of the following core components:

7.3. Risk Categories

JCEG has identified nine categories or groupings of risk, which may have an impact on the achievement of the AC36 objectives. These categories are intended to provide guidance on the range of potential risks, which may arise and will be used for reporting purposes. Risks, issues and incidents identified are required to be categorised using the following risk categories:

Risk Category	Description
Strategic/Governance	Strategic risks arising from: • deciding on and following incorrect strategies (strategic decision risk), • not executing the strategies successfully (execution risk) • the impact that the strategies will have on the business risk profile once implemented (delivered risk). This risk also considers external changes which may be known, partially known or unknown at the time the decisions are made. Governance risks arising from: • delays in establishing governance structures with clearly defined roles and responsibilities to ensure effective oversight and governance over decision making, fiscal management, project and risk management. • inadequate governance structures
Relationships (Delivery Partners, Customers)	Risks relating to new and existing internal and external stakeholder relationships (Council group, Crown, ETNZ, Mana Whenua, other stakeholder/partners) and customer's satisfaction with delivery.
Information Technology (IT) systems, Business Disruptions and Resilience	Risks arising from IT systems, infrastructure and business disruption due to internal or external events such as system and application failures, cyber security incidents, privacy and confidentiality breaches, terrorism and natural catastrophes. It includes disaster recovery and contingency planning.
Resources (Financial, Human Resources, Assets)	Risks in this category include: • Financial risks arising from insufficient funding, poor budget management, expected or unexpected financial losses including fraud, treasury risks. • Human resource risks arising from staff capacity, skills, recruitment and retention. • Loss/damage/theft of physical assets and information
Operational	Operational risks arising from external or internal processes or from external events, people and systems including procurement, third parties and contract management.
Health, Safety and Well-being	Risks arising from external or internal events, that may have a material impact on the health, safety and wellbeing of employees, contractors and the public (including volunteers).
Legal and Regulatory Compliance	Regulatory and compliance risks arising from failures to implement, or comply with, appropriate laws, regulations, contractual agreements policies and procedures within which AC36 infrastructure and event is required to be delivered.

Risk Category	Description
Programme and project delivery	Delivery risks such as 'failure to deliver the service within agreed/set terms' and 'failure to deliver on time/budget/specification'. These risks could have an impact on meeting the schedule, cost, quality and scope objectives of AC36. This category covers risks in the areas of project planning, project organization, design and quality of construction, stakeholder management, programme interfaces, programme governance, project decision-making.
Environmental Sustainability	Environmental risks arising from AC36 planning, infrastructure, construction and event activities that do not incorporate the management of environmental impacts and climate change, including the development of sufficient infrastructure to keep pace with natural catastrophes and stresses.

7.4. Framework Monitoring, Review and Continuous Improvement

Review and update of the RMF is essential to ensure that it continues to reflect any changes in the AC36 internal and external environment.

The RMF will be assessed on a continuous improvement basis to ensure it remains fit for purpose or when significant changes are made to AC36 programme and governance structure. The first review will occur in November 2018, once the programme and governance structures are confirmed.

The review will assess the following:

- effectiveness of the embedding of the framework; and
- suitability of risk systems and processes in place to record, manage and report on risks, compliance obligations, issues and incidents.

If the RMF review results in material changes, this will require approval by JCEG.

8. Roles and Responsibilities

8.1. Approach to Risk Management

JCEG has adopted a three lines of defence model to ensure that ownership, accountability and responsibility for management of risk is clearly defined and resides at the correct level within the AC36 programme. The following diagram depicts the three lines of defence model:

The table below outlines the specific responsibilities that governance and oversight groups and each line of defence plays in managing risk:

Role	Responsibilities
Governance and Oversight Groups	
AC36 JCEG	• Decision-making body for the programme in line with delegated authorities. • Programme-wide risk management, including oversight of the infrastructure alliance, event, legacy and leverage outcomes. • Approve RMF and associated policies and processes. • Determine, maintain and approve an appropriate, clear and concise risk appetite statement in relation the risk categories outlined in section 7.3. • Provide effective governance and oversight of risk, incident and issue management JCEG will receive risk information/reporting from the Event Steering Group, Interim Project Alliance Board and the work stream leads. • Set the 'tone from top' that promotes a risk aware culture. JCEG will be chaired by Auckland Council, with representatives from ACG, (including Panuku Development Auckland Limited (Panuku), Auckland Tourism, Events and Economic Development Limited (ATEED) and Regional Facilities Auckland Limited (RFA), the Crown (MBIE and the State Services Commission) and four Mana Whenua representatives.
Host City Agreement Group	• Resolve issues escalated by the JCEG. • Convene at the request of any party, but it is expected that the members will keep in contact to ensure the relationships run smoothly. This group is mandated through the HCAA and will comprise of two members from ETNZ and ACE and one each from Auckland Council and the Crown.

Role	Responsibilities
Event Steering Group (ESG)	• Ensure delivery of the AC36 event in accordance with the concept and principles developed in the Event Concept, terms and conditions of the HCAA and Host Venue Agreement. • Provide effective governance and oversight of risk, incident and issue management. This group is mandated through the HCAA to provide support, oversight and review of the emergency services requirements, including police, ambulance and fire services to comply with all health and safety requirements. ESG will be chaired by ACE with representatives from ATEED, Panuku and Crown.
Wynyard Edge Alliance – Interim Project Alliance Board (iPAB)	• Governance, leadership and oversight of the Wynyard Edge Alliance in the formation of the projects design and costs to deliver the America's Cup infrastructure. • Monitor the Alliance team's performance and where appropriate, implement measures to redirect efforts and achieve outstanding outcomes. • Provide effective governance and oversight of infrastructure risk, incident and issue management. • Escalation of risk, issues and incidents to JCEG.
Auckland Council Audit and Risk Committee	• Provide recommendations on behalf of ACG to the Governing Body on the effectiveness of the risk management processes to deliver the programme.
First line of defence – functions that own and manage risks	
Business Owners of the project workstreams (Chief Executives)	• Accountable and responsible for ownership for risks and the ongoing identification, management and reporting of risks, issues and incidents. • Promote a risk aware culture.
Interim Project Workstreams Leads: • Infrastructure • Finance • Legal and Commercial • Procurement • Mana Whenua • Regulatory • Legacy • Leverage • Event Working Group • Waterfront Integration • Inter-agency Steering Group • Security Steering Group	The work stream lead must: • Implement and comply with the risk management framework and supporting processes; • foster a culture where risks, issues and incidents can be identified, managed, reviewed, reported and escalated; • develop and maintain risk registers and continuously improve risk management responses through implementing controls; • escalate risks, issues and incidents per framework requirements; • provide periodic and adhoc reporting of risks, issues and incidents; • create operational, project and contingency plans; and • undertake control self-assessment for key controls on a regular basis. *Infrastructure - Wynyard Edge Alliance have developed a separate risk management plan and are expected to align with the AC36 RMF requirements in relation to reporting and escalation.
Inter-agency Steering Group	• Report to the Event Steering Group. • Coordinate and provide support to ensure risks relating to the provision of state emergency services requirements, including police, ambulance and fire services have been identified and managed effectively. This group with consist of representatives from ACG, including ATEED and Crown Agencies that are required to ensure delivery of a successful event. The Chair of this group is ATEED.

Role	Responsibilities
All Staff and Contractors	• Comply with AC36 RMF, policies and procedures. • Understand accountability for individual risks and controls. • Report systematically and promptly any perceived new risks, issues, incidents and/or failures of existing control measures.
ACE Ltd	• Management and delivery of AC36. • Implement and comply with the risk management framework and supporting processes. • Foster a culture where risks, issues and incidents can be identified, managed, reviewed, reported and escalated. • Develop and maintain risk registers and continuously improve risk management responses through implementing controls. • Escalate risks, issues and incidents per framework requirements • Provide periodic and adhoc reporting of risks, issues and incidents. • Create operational, project and contingency plans • Undertake control self-assessment for key controls on a regular basis.
Second line of defence – functions that provide oversight and challenge	
AC36 Programme Risk Lead – led by Auckland Council	• Develop, maintain and embed the RMF, guidance and tools. • Provide advice and challenge first line of defence risk management activities and outputs. • Conduct quality assurance reviews to challenge the completeness and accuracy of information in the risk registers and risk reports. • Promote a risk aware culture. • Provide training and guidance. • Provide risk leadership and oversight over management of risks, issues and incidents. • Provide regular risk reporting to JCEG, PMO, assurance committees and stakeholders. • Facilitate risk identification workshops as required. • Provide targeted controls assurance. • Chair and facilitate fortnightly AC36 Risk Working Group meetings with risk representatives from each workstream. The objective of the Risk Working Group is to collectively assess and implement remedial actions in relation to the following: o RMF - effectiveness of RMF and how this can be enhanced. o Success measures – define success measures to evaluate the effectiveness of risk management. o Policies - the need to develop policies or guidance material to support the RMF. o Training - staff training and coaching requirements o Risk and compliance - any significant risk and compliance matters, including matters which may require escalation to JCEG.
Programme Management Office	• Collate and report on risks, issues and incidents to JCEG.
AC36 Workstream Risk Representatives: • Panuku • ATEED • Auckland Transport • Wynyard Edge Alliance • Crown (MBIE)	• Provide support and assistance to workstream leads to implement the RMF at an operational level, including risks, issues and incident management, reporting and escalation, via Business Owners. • Undertake targeted controls assurance. • Attend fortnightly Risk Working Group meetings facilitated by AC36 Programme Risk Lead.
Third line of defence – functions that provide independent assurance	

Internal/External Audit	• Provide independent, objective assurance through systematic, disciplined evaluation of the control environment and governance processes. • Develop and implement a flexible audit plan using an appropriate risk-based methodology to ensure risks are being managed effectively and that controls are designed and operating as intended.

9. Governance, Reporting and Escalation

9.1. Risk Governance

Risk governance is an essential part of AC36 JCEG's governance responsibilities and will support JCEG to improve performance and achieve desired outcomes as it will:

- guide required risk management activities and culture;
- establish consistent risk assessment, reporting and escalation processes; and
- drive informed decision making.

JCEG is responsible for programme-wide risk management, including oversight of the infrastructure alliance, event, legacy and leverage outcomes, communications, marketing and stakeholder engagement. Section 8.1 outlines the specific responsibilities of the AC36 governance and oversight groups.

9.2. Reporting

Reporting is an integral part of the AC36 programme governance to enhance the quality of dialogue with stakeholders and support senior management and oversight bodies in meeting their responsibilities.

The purpose of risk reporting is to create awareness of key risks, issues/incidents, improve accountability and the timely implementation of risk treatment plans.

Monthly, each of the workstream leads will be responsible to provide risk reporting, as per the escalation requirements included in Section 9.3.

Risk information will be provided to JCEG as per the escalations requirements noted in Section 9.3. Risk reporting should include (but is not limited to) an update on the following:

- status of risks (including emerging risks), opportunities and controls/treatment plans;
- control self-assessment review outcomes relating to risks rated;
- compliance with required legal, regulatory and contractual obligations, including progress on key milestones and deliverables for the event and infrastructure
- issues and incidents, including root cause analysis and remedial actions; and
- internal and external audit reports and recommendations.

The PMO function is responsible to coordinate the risks, issues and incidents reporting from the interim workstream lead and/or risk representatives. Workstreams should ensure that the information provided is of high data quality standards and provide it in a standard risk reporting template as included in **Appendix 12a.**

The AC36 Programme Risk Lead team will summarise the risk reports provided by workstreams for reporting to the JCEG monthly. A risk Heat Map, as included in **Appendix 12b**, provides a summary of High and Extreme risks and will form part of the monthly reporting.

The formal reporting requirements do not preclude the timely escalation of emerging risks, issues and incidents as they are highlighted. A summary of the reporting requirements, in terms of frequency and levels of escalation, is included in **Appendix 12c.**

9.3. Escalation

Risk, issues and incidents require escalation based on their ratings.

Monthly, the following escalations are required to the Chair of the JCEG, who will determine escalation to business owners, partners, sponsors and/or JCEG:

- Residual risks rated High and Extreme
- Issues and incidents rated High and Extreme
- Controls self-assessment results for all inherent risks rated High and above; and
- Control Effectiveness rating for residual risks rated High and Extreme

The following escalations are required to the interim Programme Risk Lead and Project Management Office, who will determine if it requires further escalation to the business owners and Chair of JCEG:

- Residual risks rated Medium and above;
- Issues and incidents rated Medium and above;
- Controls self-assessment results for all inherent risks rated Medium and above; and
- Control Effectiveness rating for all residual risks rated Medium and above.

All regulatory/legislative non-compliance or health and safety incidents must be reported to Programme Risk Lead, Project Management Office and the Chair of JCEG, irrespective of the rating.

10. Risk Appetite Statement

10.1. Defining Risk Appetite

Risk appetite is defined as the degree of risk that the organisation or a project is prepared to accept in pursuit of its objectives and business plan.

Risk appetite can be expressed in a number of ways to ensure that it is commonly understood and consistently applied across the programme. Generally, the risk appetite is expressed in the form of high-level qualitative statements that clearly capture the programme's attitude and level of acceptance of different risks. Where appropriate, the risk appetite statement may include quantitative measures.

10.2. Objectives of Risk Appetite

Key objectives of Risk Appetite are:

- enables JCEG to exercise appropriate oversight and governance by setting boundaries for the programmes activities and behaviours;

- expresses JCEG's attitude to risk to promote a risk aware culture;
- provides a framework for making business / risk-based decisions;
- expenditure assessments and decisions relating to capital and operational expenditure;
- provides a framework to evaluate and rank risks to allow automatic acceptance or escalation and treatment (including formal acceptance) as required; forms the basis of risk reporting to executive management and Board;
- integral part of programme/project planning;
- empower staff to take more risk; and
- limit staff from taking excessive risk.

10.3. Defining Risk Tolerance

Risk tolerance is the maximum level of risk that JCEG is willing to operate within, expressed as a risk limit and based on its risk appetite. This can be expressed as a dollar, percentage, number.

Risk tolerances translate risk appetite into operational limits for the day-to-day management of material risks.

Tolerances should be measurable and quantifiable as far as possible.

10.4. Risk Appetite Statement requirements

JCEG is responsible for having an approved risk appetite statement in relation the risk categories outlined in section 7.3 and use the risk appetite as a basis for decision making. The approved risk appetite statement at a minimum will convey:

- the degree of risk that JCEG is prepared to accept in pursuit of its strategic objectives and business plan, considering the interests of all stakeholders (risk appetite);
- for each material risk, the maximum level of risk that JCEG is willing to operate within, expressed as a risk limit and based on its risk appetite, risk profile and capital strength (risk tolerance);
- the process for ensuring that risk tolerances are set at an appropriate level, based on an estimate of the impact if a risk tolerance is breached, and the likelihood that each material risk is realised;
- the process for monitoring compliance with each risk tolerance and for taking appropriate action if it is breached; and
- the timing and process for review of the risk appetite and risk tolerances.

AC36 Programme Risk Lead team will facilitate a workshop with JCEG members to develop the Risk Appetite Statement.

11. Risk and Opportunity Assessment and Management

11.1. Top-down and Bottom-up Approach

An integrated top-down and bottom-up approach will be adopted to support the AC36 programme risk assessment process.

Risk identification and assessment, using the top-down approach will occur in the early phase of the AC36 programme to set the tone and direction from the top. In the top-down approach, discussion on overarching risks, including strategic and operational risk will be held at the "top" level (i.e. JCEG). The output of this process will be a top risk register for AC36.

To identify more granular operational risks at tactical level, a bottom-up approach will be used. The top risks register will serve as a useful prompt list for the identification of risks at the project workstream levels.

By integrating the outputs from the top-down and bottom up approaches, the risk assessment outcomes should be aligned and follow on risk management activities will be directionally correct.

11.2. Risk Assessment and Management Process

The risk assessment and management processes are forward looking, focussed on risks, opportunities and associated controls. The AC36 programme risk appetite (how much risk is tolerable and justifiable) is regarded as an 'overlay' across the process to achieve effective risk management.

The outputs of the risk assessment processes should be documented and will be used by management for decision-making, prioritisation and governance.

The following diagram illustrates the core components of the risk assessment and management process. The components are common to top-down and bottom-up risk assessment.

Risk Assessment and Management Process (AS/NZS ISO 31000:2018)

The AC36 Programme Risk Lead team will facilitate the top-down and bottom-up risk workshops, which includes providing guidance on each of the steps identified below. For the workstreams that have a dedicated risk resource, they will be responsible to provide ongoing input and support to identify, assess and manage risks effectively.

The outputs of the risk workshop will include AC36:

- Top Risks Register
- Workstream Risks Register(s).

Approval/sign-off will be required by business owners to confirm that the risk assessment is an accurate reflection of the risk and control environment quarterly and six monthly, as outlined in section 12.4.

The outcome of the Risk Assessment process should be documented in the Risk Register as per section 12. All risks (and issues) will have a unique identifier across the life of the AC36 programme.

11.2.1. Step One - Establish the Context

This step establishes the context in which the rest of the risk assessment process takes place. It involves understanding the AC36 programme structure, objectives, culture and risk appetite of all stakeholders and the internal and external environment within which risk should be managed.

11.2.2. Step Two - Risk Identification

Risk identification is the process of identifying risks and opportunities that may impact achievement of the project and process value chain objectives. The output of the risk identification process is a comprehensive list of risks and opportunities originating from events that may create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. These could be current foreseeable risks or emerging risks.

JCEG should also consider "stress events" that are very unlikely to occur but may have the potential to significantly disrupt the delivery of AC36. By identifying and analysing these events, there is an opportunity to develop mitigation plans and be prepared to deal with unexpected significant events.

11.2.3. Step Three - Risk Analysis

The assessment of risk, whether at the inherent, residual, expected or targeted level, requires an assessment of two major components, that of:

- likelihood of occurrence, and
- impact if the risk were to occur.

To assess the likelihood and consequence of each risk, scales have been developed for each of these two components as outlined in **Appendix 3.** Likelihood and impact should be assessed on an average basis and not on a worst case basis, for e.g. ‘what is the average number of times you would expect this risk to occur within a twelve month period’ or ‘what is the average expected consequence if the risk were to occur’.

The risk analysis step involves an analysis as to the likelihood or occurrence and the impact if the risk were to occur. This leads to an assessment as to the overall size of the risk and its relative importance to other risks. It also involves a detailed consideration of uncertainties, risk sources, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

Risk analysis should be undertaken with consideration to the processes or objectives it

impacts, which may influence the level of detail to which the analysis is conducted. The analysis may be qualitative, quantitative or a combination of these depending on the circumstances.

All risks identified must be categorised according to the nine categories of risk outlined in section 7.3 and assessed using the 5x5 Risk Assessment Matrix included in Appendix 3. The risk rating selection to enable prioritisation is Low, Medium, high, Extreme.

11.2.4. Step Four- Risk Evaluation

Risk evaluation involves reviewing the level of risk established during the analysis stage to determine if it is within risk appetite and if not, what level of escalation and/or mitigation plans/controls are required.

Risk evaluation can lead to a decision to:

- consider risk treatment options, including risk acceptance;
- undertake further analysis to better understand the risk;
- maintain existing controls;
- reconsider objectives.

Decisions should take account of the wider context and the actual and perceived impacts to external and internal stakeholders.

Ongoing actions are required based on the risk rating, as included in Risk Response Table in **Appendix 4**.

11.2.5. Step Five - Risk Treatment Plans/Controls

Once risks have been identified and rated, risk treatment options to consider are:

- **Risk acceptance:** this occurs when no further treatment is implemented, and the current level of risk is formally accepted.
- **Modifying controls:** modifying either likelihood and-or consequence reducing controls. This may either reduce or increase the risk compared to current levels.
- **Risk avoidance:** this involves ceasing the activity that is causing the risk, deciding not to proceed with the activity or choosing an alternative activity which meets AC36 objectives and does not pose the same level of risk; or
- **Risk transfer:** this involves the impacts of the risk being transferred to a third party such as insurance

In considering the risk treatment plans, consider the 'cost v benefit' (both direct and indirect) of treating a risk, to select a response that brings the residual risk within desired tolerance levels as defined in the risk appetite statement.

The four types of controls used to 'treat' and manage the risks are preventative, detective, directional and corrective. These control types are defined in **Appendix 7**.

The controls should be clearly defined and referenced to the risks. A 'control effectiveness rating' is required to be applied to controls as detailed in Section 15.

11.2.6. Step Six- Monitoring and Review

Risks are dynamic and ever changing. This step requires a process of ongoing monitoring and review to ensure risks are continually identified, analysed, evaluated and treated. This is a critical step to ensure that:

- risks are being addressed and for staff and governance groups to maintain a real-time view of changes in the risk assessments;
- risk is integrated into the decision-making processes and there is timely implementation of response plans; and
- promotes a risk aware culture.

Monitoring and review of risks are required to occur through:

- establishment of Key Risk Indicators (as detailed in section 12). These indicators aim to provide performance metrics on key risks in the context of the programme and internal control environment.
- monthly and quarterly review of risk assessments (i.e. risk registers) to ensure the data captured remains a true and accurate reflection of the current programme environment. Risk Register review and approval requirements are outlined in Section 13.
- monthly reporting on risks, controls, issues and incidents, control self-assessments.

11.2.7 Step Seven- Communication and Consultation

Communication and consultation with stakeholders should occur regularly. It is an essential component of the risk assessment process and is required to achieve transparency and effective management of risks.

11.2.8 Step Eight – Recording and reporting

The risk management and assessment processes and its outcomes should be formally recorded and reported through appropriate mechanisms. Recording and reporting aims to:

- communicate risk management activities and outcomes across the AC36 programme;
- provide information for decision-making;
- improve risk management activities; and
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

The outputs from Step 1- 5 should be recorded in the risk register template, all fields in the template should be completed and review and approval requirements must be complied with. These requirements are detailed in Section 12.

Risk reporting requirements and the governance mechanisms in place to provide formal oversight for the outcomes of the risk assessment and management process are documented in Section 9.

12. Risk Register(s)

12.1. Defining Risk Register

A risk register is used to record risks identified through the risk assessment process and provides information to manage them. A risk register should be a true and accurate reflection of risks and mitigations as it will be:

- used for decision making;
- shared with team members;
- escalated to senior leaders;
- used as a core document for all risk reporting requirements; and
- shared with auditors as evidence of risk management.

12.2. Risk Register Template

The risk register template is included in **Appendix 6** and information to complete the various fields in the register is outlined in **Appendix 7.**

Each risk will have a unique alpha numeric identifier across the life of the AC36 programme.

12.3. Risk Register Approval

All risks in the risk register must be reviewed and approved by the Business Owner, who is responsible and accountable for the management of the risks. Evidence of review and approval must be recorded.

12.4. Risk Register(s) Review

The risk registers are required to be reviewed regularly and when significant changes are made to structure, programme activities or objectives. Review and monitoring requirements are described below:

AC36 Top Risks register

AC36 Top Risks Register is required to be reviewed quarterly. The review process will be facilitated by the Programme Risk Lead team and the results will be shared with project workstream leads.

Top risks will be subject to a risk review (deep dive) on a rotational basis to provide assurance that risks are being effectively managed, and the controls are designed and operating as intended. The results of the review will be reported to JCEG.

A ‘deep dive’ template (included in **Appendix 8**) will be used to consistently complete the review, record the results and report on review outcomes across all the risks.

AC36 Workstream Risk Register

The Business Owner, in conjunction with the workstream risk representative is required to review the workstream risk register(s) on a quarterly basis. The review should include the following:

- identification and analysis of any new or emerging risks; and

- confirmation that previously identified risks remain relevant including the overall risk rating, controls and assigned risk and control owner(s).
- confirmation from control owners that the controls are designed and operating as intended. The 'control effectiveness rating' will require updating as detailed in Section 15.

The review outputs should be documented for evidential, reporting and auditing purposes.

13. Key Risk Indicators

13.1. Context

Key Risk Indicators (KRIs) are used to understand and monitor risk behaviour. KRIs are forward-looking metrics that monitor changes in the internal and external project environment as well as the quality of controls, thereby indicating potential changes in the inherent or residual risk. KRIs are a powerful management tool if used appropriately, providing an early warning of when risk events may occur.

Note: the term 'KRI' used within the AC36 Framework encompasses both 'risk indicators' and 'control indicators'.

13.2. Objectives

The key objectives of KRIs are to:

- monitor control, risk causes/drivers and impacts as close to the real time mode as possible;
- provide an early signal that triggers a review, escalation, or management action before further impacts occur; and
- Translate risk appetite into quantifiable metrics.

13.3. The KRI process

The KRI process comprises of the following steps:

The detailed KRI process is included in **Appendix 5**.

14. Issue and Incident Management

14.1. Context

The control environment for the AC36 project is critical to the mitigation of key risks. Any weaknesses, deficiencies or gaps in this environment may lead to risk events occurring. Therefore, it is important to identify and fix any issues before an incident occurs.

14.2. Objectives

Incidents and issues should be captured to ensure that:

- there is a consistent approach for collecting data to facilitate transparency across the programme;
- impacts are managed effectively to minimise losses and/or potential future losses;
- root cause analysis is completed to understand what happened, why it happened and how it happened;
- appropriate and timely actions are taken to mitigate any exposure minimise future occurrence;
- weak or missing controls, ineffective processes or poor system performance are identified and remediated in a timely manner;
- training and communication opportunities are identified and addressed
- issues and incidents are reported including analysis and inferences, to JCEG, risk committees and relevant stakeholders for oversight and to facilitate decisions required to manage risks.

14.3. Issue Definition

An issue is defined as a current problem or concern influencing objectives that highlights a deficiency in:

- the mitigation of an identified key risk in terms of:
  - absence of an appropriate control(s) i.e. controls do not exist
  - an ineffective or poorly designed control(s) i.e. controls not designed or designed appropriately for the identified risk
  - non-performance of a control(s), i.e. not being applied or not performing as designed
- processes for meeting regulatory or compliance obligations.

14.4. Incident Definition

Incidents should not be confused with issues.

An incident is defined as situation where a risk has occurred, and one or more impacts have been felt due to inadequate or failed processes, people, systems and external events. This includes compliance incidents, operational losses, and internal and external fraud.

An incident may be a ‘near miss’ where it didn’t result in an impact but had the potential to result in one or more impacts.

14.5. Issue and Incident Management Process

The issue and incident management processes ensure that:

- all relevant issues and incidents are identified, captured and managed effectively;
- negative consequences are minimised;
- improvements are put in place to fix the issue or prevent recurrence of incident; and
- timely and accurate communication to business owners and governance and oversight groups.

The issue and incident management process comprise of the following steps:

Detailed issue management process can be found in **Appendix 10**

15. Control Effectiveness Rating

15.1. Control Evaluation

Control evaluation allows the business to gauge the effectiveness of applied controls in terms of reducing the impact and/or likelihood of risk. This can help management assess whether the risk exposure is within an acceptable level or whether further controls or control improvements are required.

15.2. Control Effectiveness (CE) Rating

Individual controls are required to be assessed based on design and operating effectiveness.

Control Design Effectiveness *Do the controls make sense?*	Consider how well the control should work in theory, if it is always applied as intended. Controls are designed to reduce the level of risk (and will not necessarily eliminate the risk altogether)
Control Operating Effectiveness *How well are the controls operating?*	Consider the way in which the control is operating in practice, if it is applied when it should be and as intended

Control Design Effectiveness and Control Operating Effectiveness assessments are combined to give an overall rating, using 3x3 Control Evaluation Matrix. Control effectiveness rating and 3x3 evaluation matrix are included in **Appendix 11**

The initial CE rating should be assigned as part of the risk assessment process using a combination of understanding of the design of control and evidence of supporting material.

The CE rating should be updated quarterly by the control owners and reviewed by the Business Owner. To update the CE ratings, control owners must refer to the control self-assessment review outcomes, audit recommendations and issue and incident reports.

Justification of final Control Effectiveness ratings and assessments should be documented.

16. Control Self-Assessment

16.1. Definition of Control Self-Assessment

Controls are designed and implemented to reduce either the likelihood and/or impact of a risk. To understand the effectiveness of their controls, risk and control owners must test both the

design and operating effectiveness of each key control. This program of work is known as a Control Self-Assessment (CSA).

16.2. Objectives

The objectives of CSA are:

- ensure the integrity of the control environment through periodic testing of the design and operating effectiveness of key controls;
- identify control gaps and initiate remediation and action plans as required; and
- provide assurance to risk and control owners, senior management and governance and oversight groups on the effectiveness of the control environment.

16.3. Scope

The controls that need to be tested will be identified during the risk assessment process. However, not all controls need to be tested, only those which are considered key to mitigating the risk.

A key control is a control that provides reasonable assurance that material errors or events will be prevented, detected or impact mitigated in a timely manner. The Risk Owner in collaboration with the Control Owner(s) determines which controls are key and therefore in scope for control testing.

As a minimum, key controls associated to inherently High or Extreme risks are to be included in the CSA to quarterly test their design and operating effectiveness. The balance of key controls should be reviewed every six months by the Risk Owners.

16.4. Exemptions

There are two types of CSA exemptions available:

i) Key controls currently undergoing remediation activities (i.e. subject to issue management).
ii) Key controls that are in the processes of being developed and are not yet fully implemented.

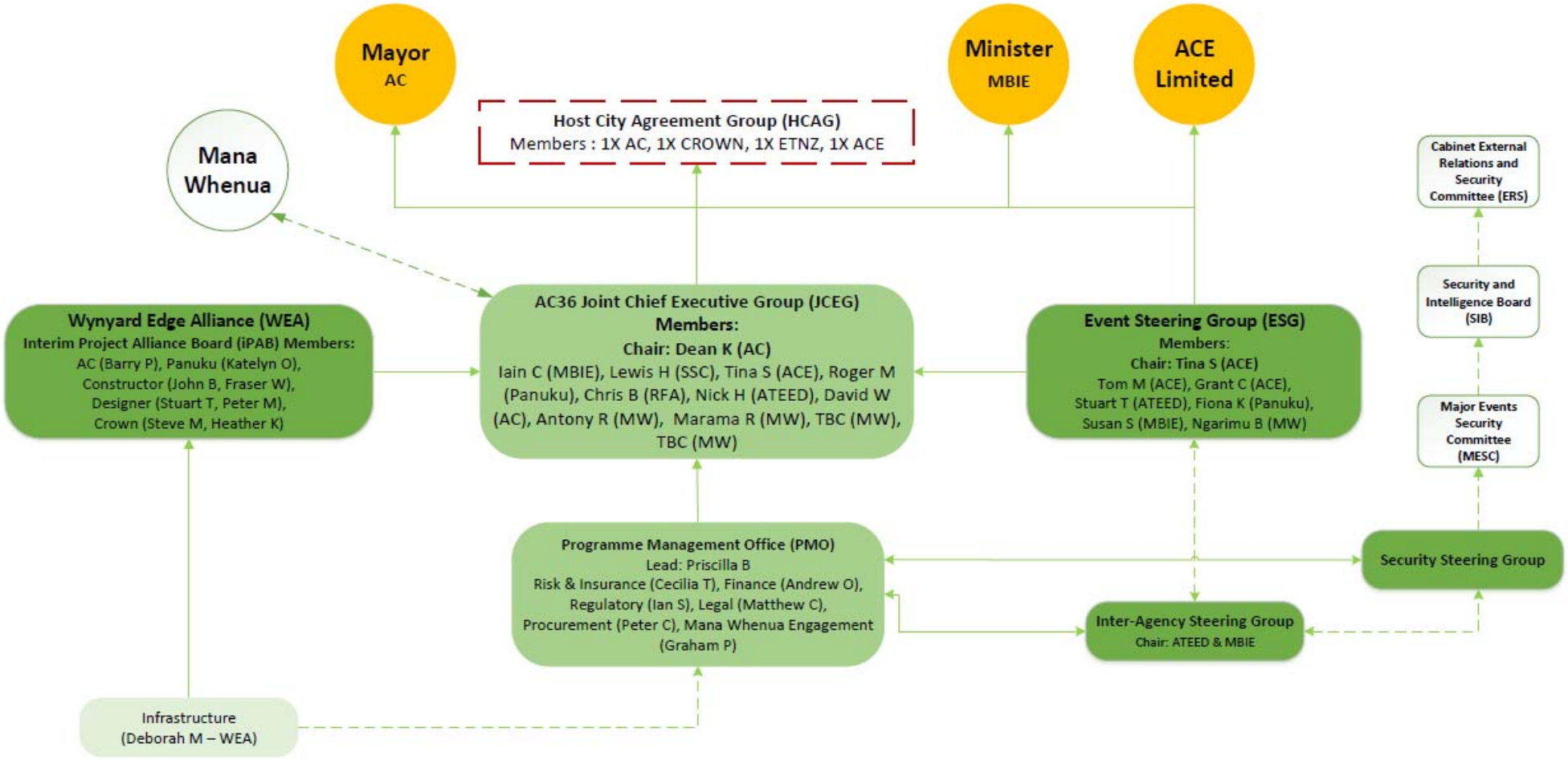
16.5. CSA Process

The CSA process involves the following key steps and the detailed requirements and is included in **Appendix 9**.

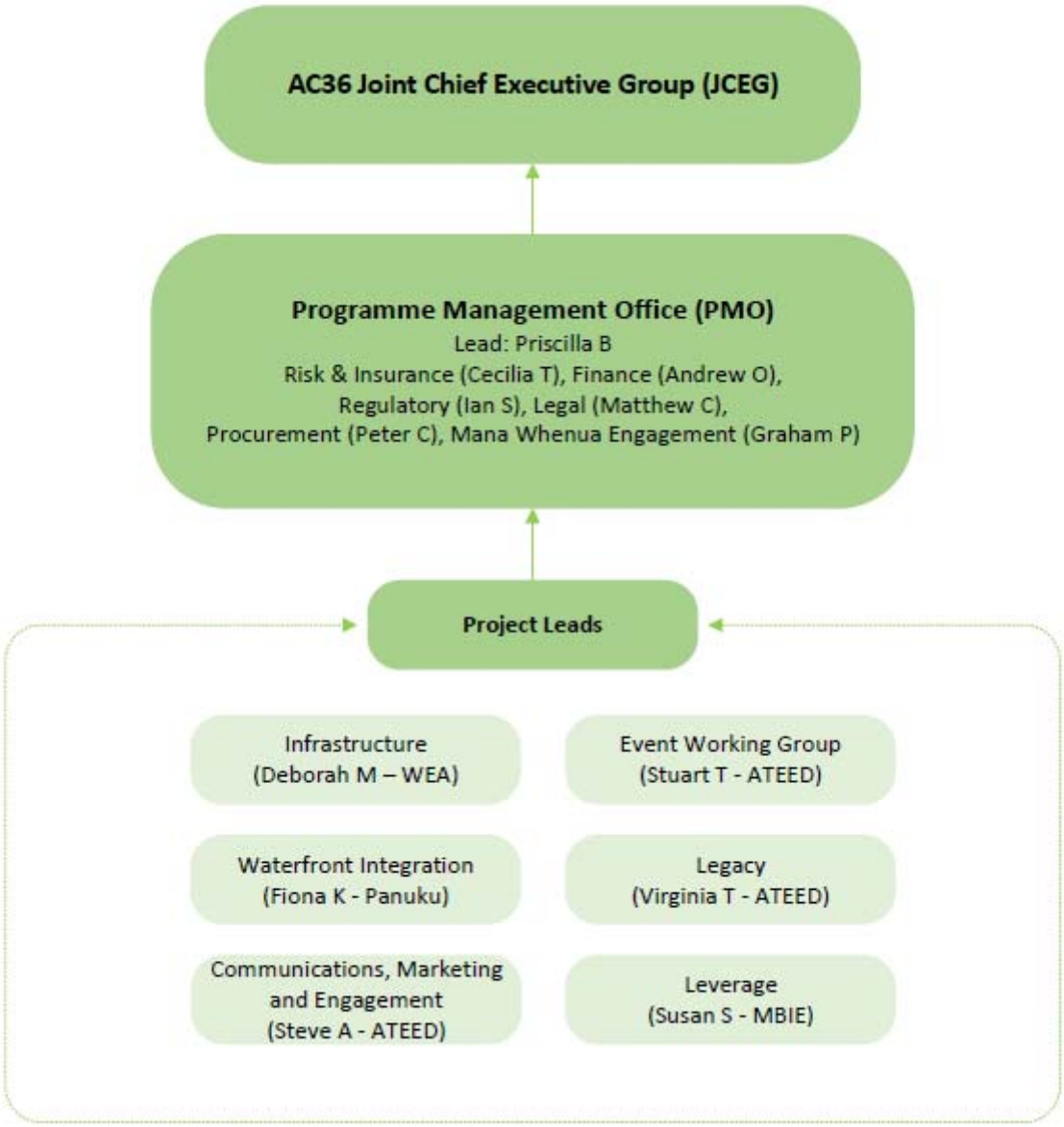
17. References and related documents

Associated policies	There are no associated policies.
AC36 RMF guidance notes and templates	Appendix 1 AC36 Governance Structure Appendix 2 Applicable Legislation Appendix 3a 5x5 Risk Assessment Matrix Appendix 3b Impact Table Appendix 4 Risk Response Table Appendix 5 KRI process (to be created) Appendix 6 Risk Register Template Appendix 7 Risk Register Template guidelines Appendix 8 Risk Deep Dive Template Appendix 9 Control Self-Assessment Process (to be created) Appendix 10 Issue and Incident Management Process (to be created) Appendix 10a Issue and Incident Register Template Appendix 10b Issue and Incident Template Appendix 11 Control Effectiveness Rating and 3x3 Evaluation Matrix Appendix 12a Monthly Risk Report Template Appendix 12b Risk Heat Map Template Appendix 12c Risk Reporting Requirements
References	*Auckland Council Risk Management Framework, Policy* *AS/NZS ISO 31000:2009 – Risk management - Principles and guidelines (20 November 2009)*

Appendix 1 – AC36 Programme Governance Structure



Appendix 1 – AC36 PMO Structure



Appendix 2 – Applicable Legislation

There are a number of legislations applicable to AC36 Programme. Some of the key legislations relevant to the programme include:

- Health and Safety at Work Act 2015
- Crimes Act 1961
- Resource Management Act 1991
- Local Government Act 2002
- Conservation Act 1987
- Maritime Transport Act 1994
- Marine Reserves Act 1971 Civil Aviation Act 1990

Appendix 3a – 5x5 Matrix

Using the 5x5 risk assessment matrix to rate risks involves the subjective assessment of a risk event's likelihood and impact over the next 12 months or within the project timeline. The likelihood and impact are combined to arrive at an overall 'risk rating' (i.e. Low, Medium, High, Extreme). The risk rating is the assessment used to plot where each risk sits on the 5x5 risk assessment matrix.

5x5 Matrix

LIKELIHOOD	RISK RATING					
	5 - Almost Certain	Medium	High	High	Extreme	Extreme
	4 - Likely	Medium	Medium	High	High	Extreme
	3 - Possible	Low	Medium	Medium	High	High
	2 - Unlikely	Low	Low	Medium	Medium	Medium
	1 - Very Unlikely	Low	Low	Low	Medium	Medium
	IMPACT	INSIGNIFICANT	MINOR	MODERATE	MAJOR	EXTREME

Likelihood Table

The likelihood assessment involves estimating the likelihood of a risk occurring. The likelihood table below outlines the five levels of probability/likelihood of occurrence and is articulated qualitatively and by percentage chance of occurrence.

	LIKELIHOOD DESCRIPTION	Percentage
5 - Almost Certain	The event will occur in the foreseeable future or within the project timeframe	>90%
4 - Likely	The event will probably occur in the foreseeable future or within the project timeframe	51-90%
3 - Possible	The event might occur in the foreseeable future or within the project timeframe	16-50%
2 - Unlikely	The event is not likely to occur in in the foreseeable future or within the project timeframe	5-15%
1 – Very Unlikely	The event will only occur in exceptional circumstances	<5%

Appendix 3b – 5x5 Matrix

Impact Table

The range of impact types below are based on AC36 programme and project objectives. Impacts may be assessed for each of the impact categories in the 5x5 risk matrix. A risk event may have multiple impacts, ranging from financial/non financial loss to reputational damage. When there are multiple impacts, we should select the highest impact value for the overall rating.

	IMPACT				
	INSIGNIFICANT	MINOR	MODERATE	MAJOR	EXTREME
OBJECTIVE IMPACTED					
Social and Cultural / Community	• No significant community issues. • Localised short term reversible disruption to the community, resulting in no noticeable damage. • No significant impact on the achievement of a social or cultural legacy outcome	• Local community concerns that can be dealt with. • Localised minor reversible damage and disruption to the community, with no potential public safety issues or long term effect • Minor impact on the achievement of social or cultural legacy outcomes	• Significant community concerns causing delays and modifications to plans. • Localised medium term (1 to 3 weeks) reversible damage and disruption, to the community, with some potential safety issues. • Moderate impact on the achievement of social or cultural legacy outcomes	• Widespread significant community concerns causing significant delays and modifications to plans. • Localised or widespread long term (greater than 3 weeks) reversible or irreversible damage; disruption to community • Major impact on the achievement of social or cultural legacy outcomes; or adverse impact on social or cultural legacy outcomes.	• Extensive community concerns causing major re-think or complete failure of plans. • Localised or widespread damage and disruption to the community (any duration), with potential for loss of life. • Social or cultural outcomes leave Auckland's cultural relationships or New Zealand society in a worse state than before AC36.
Programme Delivery	• A delay, cost increase or scope change for a specific deliverable that doesn't impact on overall delivery. • Negligible negative impact to internal milestones • Compromise or corruption of information held that is otherwise available in the public domain. • Disruption to service delivery and debate on approach. • Minor disagreements with stakeholders	• < 2-week delay to internal milestone but no impact on public milestones OR • Additional resource required for up to 1 month to accelerate programme (≤3FTE in site office). • Minor negative impact on expectations e.g. short term restrictions on pedestrian access. • Compromise of information that could impact upon internal or workstream interests. • Disruption to service delivery and disagreement on approach. • Relationship issues between key parties' cause delays to major decisions	• ≥ 2-week delay to internal Milestone OR • ≤ 2-week delay to delivery for Wynyard Wharf bases OR • Additional resource required for up to 3 months to accelerate programme (≤3FTE in site office OR • additional crew OR extended working hours) • Moderate negative impact on expectations e.g. reduced design life of structural elements or notably reduced aesthetics • Compromise of information that could impact upon the organisations' daily operations. • Disruption to service delivery and strained relationships. • Significant one off or ongoing relationship issues that impact on achievement of objectives	• 2 - 4-week delay to delivery for Wynyard Wharf bases OR • ≤ 2-week delay to delivery for Hobson bases OR • Additional resource required for 3+ months to accelerate programme (>3FTE in site office OR additional crew OR extended working ours) • Delays necessitate significant adjustment to the overall goals, objectives and/or plans. • Major negative impact on expectations e.g. one or more teams based at alternative location. • Compromise of information sensitive to organisational interests. • Serious disruption to service delivery and fracturing of relationships. • Severe breakdown of relationships resulting in changes in appointments	• > 4-week delay to delivery of any base. • Would have permanent impact on the achievement and delivery of objectives making it no longer viable. • Extreme negative impact on expectations e.g. event cancelled, delayed or hosted at an alternative venue. • Compromise of information with significant ongoing impact. • Halt to service delivery and termination of relationship. • Public severance of relationships

Appendix 3b – 5x5 Matrix

	IMPACT				
	INSIGNIFICANT	MINOR	MODERATE	MAJOR	EXTREME
Environmental (Natural and Built)	• Small localised and reversible environmental impact resulting in: o Slight, short term damage to use of land and/or water o Slight short-term damage to land and/or water ecosystems o No noticeable species reduction. o Occasional inconsistency with the intent of environmental legislations. o No significant impact on the achievement of an environmental legacy outcome.	• Contained and reversible (minimal) environmental impact resulting in: o Localised minor reversible damage to (use of) land and/or water o Localised minor reversible damage to land and/or water ecosystems. o Temporary reduction in one species. o Minor erosion and/or damage to property. o Minor inconsistency with the intent of environmental legislations. o Minor impact on the achievement of environmental legacy outcomes.	• Measurable damage to the environment; significant corrective action resulting in: o Localised, medium term reversible damage to land and/or water ecosystems. o Moderate reduction in one or more species. o Moderate erosion and/or damage to property. Recovery time 1 month. o Repeated inconsistency with the intent of environmental legislations. o Moderate impact on the achievement of environmental legacy outcomes	• Irreversible localised damage (major) to the environment resulting in: o Widespread, long term reversible damage to land and/or water ecosystems. o Significant reduction in one or more species. o Severe erosion and/or damage to property. o Recovery time up to 6 months. o Repeated and significant inconsistency with the intent of environmental legislations. o Major impact on the achievement of environmental legacy outcomes; or adverse impact on environmental legacy outcomes.	• Extensive irreversible damage (widespread) to the environment resulting in: o Widespread, irreversible damage to land and/or water ecosystems. o Permanent loss of one or more species. o Destruction of property / widespread flooding. o Recovery time exceeding 6 months o No recognition of the intent of environmental legislations. o Environmental outcomes leave Auckland's environment in a worse state than before AC36.
Reputation	• One-off negative national newspaper coverage • Individual/isolated complaints received	• Sustained negative national TV or newspaper coverage. • One-off negative international television or newspaper coverage • Scrutiny by Executive, internal committees or internal audit to prevent escalation. • Isolated dissatisfaction / complaints from customers.	• Significant one-off event or series of events resulting in sustained negative international media coverage and perception. • Persistent national concern, Scrutiny required by external agencies. • Sustained dissatisfaction / complaints from customers/	• A number of key personnel replaced • A one-off event or series of events that result in loss of confidence from one or more key stakeholders. • Persistent intense national public, political and media scrutiny. • Major operations severely restricted. • Sustained dissatisfaction / complaints from customers.	• International concern, Governmental inquiry or sustained adverse national / international media. • Relentless / sustained reputation issue. • Scandal. • Widespread loss of confidence by customers
Health, safety & wellbeing	• First aid treatment required. No down time. Near misses.	• Injury or illness requires treatment by a medical or other registered practitioner.	• Injury or illness results in lost time. • Notice issued by regulator or Health and Safety Representative.	• Injury of individuals, extensive injury and hospitalisation. • Organisation breaches law resulting in prosecution and penalties	• Permanent disability or one or more fatalities • Considerable penalties and prosecutions. Multiple law suits and jail terms.
Strategic	• Minor complaints about New • Zealand's event capability or infrastructure • Deliver 5% below benchmark economic impact targets • No significant deviation from delivering the desired legacy benefit of the event. • Isolated negative impact to NZ and Auckland brand.	• An aspect of New Zealand's event capability or infrastructure is deemed unsuitable to host a major event. • Deliver 5-20% below benchmark economic impact targets. • Minor deviation from delivering the desired legacy benefit of the event. • Infrequent negative impact to NZ Inc's and Auckland Inc's brand	• Certain aspects of New Zealand's event capability or infrastructure are deemed unsuitable to host a major event • Deliver 20-35% below benchmark economic impact targets • Moderate deviation from delivering the desired legacy benefit for the event.	• New Zealand deemed unsuitable to host future major event • Deliver 35-50% below benchmark economic impact targets • Major deviation from delivering the desired legacy benefit of the event	• Failure to deliver Crown objectives relating to "ability to run a major event and making New Zealanders proud of their achievements as a nation • Deliver less than 50% of benchmark economic impact targets • Significant deviation from delivering the desired legacy benefit of the event

Appendix 3b – 5x5 Matrix

	IMPACT				
	INSIGNIFICANT	MINOR	MODERATE	MAJOR	EXTREME
			• Sustained negative impact to NZ and Auckland brand	• Sustained negative impact to NZ and Auckland brand at a national level	• Significant negative impact to NZ and Auckland brand at a national and international level.
Financial	• Slight financial issue managed by reprioritisation within financial baseline. • Financial loss < $10k. • Event costs over budget by less than 0.5% • Minor breach of compliance with public sector procurement and probity requirements.	• Adverse financial impact requiring financial reprioritisation. • Financial loss $10k - $100k. • Event costs over budget by more than 0.5% and less than 1%. • Minor breaches of compliance with public sector procurement and probity requirements.	• Significant financial impact requiring central (internal) resource funding. • Financial loss $100k - $1m. • Event costs over budget by more than 1% and less than 2.5%. • Moderate breach of compliance with public sector procurement and probity requirements.	• Serious financial implications requiring significant financial reprioritisation. • Financial loss $1m - $10m. • Event costs over budget by more than 2.5% and less than 5%. • Significant breach of compliance with public sector procurement and probity requirements.	• Grave financial implications necessitating new Crown funding or major service cutbacks. • Financial loss > $10m. • Event costs over budget by more than 5%. • Grave breach of compliance with public sector procurement and probity requirements.
Legal and Regulatory	• Isolated contractual disagreements or compliance issues. • Inability to negotiate favourable agreements with parties.	• Significant contractual disagreements with stakeholders • minor penalties for non-compliance to statutory regulations.	• Litigation with Crown or other key parties. • Breach of the Host City Appointment Agreement (HCAA) or Host Venue Agreement (HVA). • Complaint to the Ombudsman or other statutory offices	• Litigation over breach of HCAA • Legislative non-compliance; prosecution or potential for a fine or significant criticism by Judiciary or Ombudsman • Adverse ruling by the Ombudsman or other statutory officer with power to investigate or make rulings.	• Loss of hosting rights. • Legislative noncompliance involving the potential for imprisonment of a Councillor or Senior Officer. • Judicial review of a Council decision on a matter relating to funding.

Appendix 4 – Risk Response Table

Risk Rating	What does it mean	Risk response required	What needs to be done?
Extreme	**Immediate and imperative failures** Significant risk to the achievement of business objectives, making it imperative to have strategies for managing consequences.	**Urgent management (UM)**	**Urgent management** A risk treatment plan must be established and implemented. Regular reporting requirement and immediate appropriate escalation
High	**Major extraordinary events** A risk that can interrupt what we are doing. High risk to business objectives. High potential consequences and/or high frequency of occurrence make management strategy essential.	**Active management (AM)**	**Active management and regular review** A treatment process should be adopted, primarily focused on paying close attention to the maintenance of excellent/good controls.
Medium	**Delivery, operating and compliance** Interferes with the quality of what we are doing. Repetitive risk, low individual consequence.	**Monitor and review (MR)**	**Monitor and review** Requires effective internal controls and monitoring due to occurrence frequency. A treatment process should be adopted, primarily focused on monitoring and reviewing existing control procedures.
Low	**Minor or insignificant occurrence** Low risk to the achievement of our business objectives. Low significance and seldom occurs.	**Well Managed (WM)**	**Routine procedure sufficient to deal with the effects** Significant management effort should not be directed towards these risks. Normal controls monitoring measures should be sufficient.

Appendix 5 – KRI process

1.1 Identify risks to be recorded

KRIs are focused primarily on monitoring risks that have been identified through the risk assessment process. KRIs, at a minimum, should be developed for inherently high or extreme rated risks within the project workstreams.

1.2 Identify and define KRIs

Identify and define meaningful KRIs by first deciding on the objectives which may be pursued with KRIs. The KRI should ideally have a strong relationship to the risk being tracked. For a KRI to be meaningful, a change in the KRI should be strongly correlated to a change in the tracked risk rating. Where this relationship is weak, the KRI is less reliable.

For example, the level of employee complaints may be considered a strong indicator of poor staff morale, while the level of staff turnover may be considered weaker as there is a wider range of other factors that could cause this.

The focus should be on creating leading KRIs that preempt a risk materialising.

1.2.1Types of KRIs

It is generally accepted that the following are four types of indicators that help to monitor current risks and controls:

- Leading risk indicators, which are aligned to the causes of a risk
- Lagging risk indicators, which are more likely to be aligned to the impacts of the risk event.
- Leading control indicators which are aligned to preventative controls
- Lagging control indicators, which are aligned to detective and corrective controls

These indicators can be either:

- Single number KRIs – for example, the number of customer complaints
- Composite KRIs – these KRIs consist of two or more single number KRIs combined using an algorithm. For example, combining the number of customers with the number of customer complaints to produce customer complaint ratio (number of customer complaints divided by number of customers)
- Qualitative KRI – these are KRIs such as ‘Audit Rating’, which may have qualitative values of high, medium and low.

Once the list of potential KRIs has been developed, an assessment of the viability of each metric should be conducted. The following questions should be considered in this assessment:

- Is the KRI leading or lagging?
- How effective will the KRI be at detecting the changes in the risk?
- Can the KRI be used for more than one risk?
- Is the KRI sustainable?

Appendix 5 – KRI process

This assessment will help identify which KRIs should be eliminated from the list. Be careful not to fall into the trap of "If you can measure it, monitor it". Just because information is available, does not mean it is meaningful for monitoring a risk.

Note: The focus should be on developing key *risk* indicators, and not on key *performance* indicators. KPIs monitor the performance of activities, not the underlying risk causes.

1.3 Source Data

Once there is an agreed set of KRIs, the ease of sourcing information should be assessed. It is important to consider:

- Is the KRI data currently reported?
- How frequently is the information available?
- Can the data be regularly and consistently extracted from the same source?
- Is the data in the same format as required for the KRI?
- Can reliance be placed on the data? Who is the data owner / supplier?
- Determine KRI tolerances

The data must be validated by the Business Owner and Workstream Lead prior to setting tolerances to assess its integrity and accuracy.

1.4 Determine Tolerances

Business Owners and work stream leads are responsible for:

- identifying KRIs and associated tolerances, and for the ongoing review and managing actions for KRIs outside of tolerance levels.
- Determining the point at which management are made aware of tolerance breaches and the actions required

Three tolerances for the KRIs must be set: **red**, **amber** and **green**. The purpose of each tolerance is to enable a comparison with the data values recorded and to determine an overall KRI status, including the potential escalation of tolerance breaches.

Tolerances should reflect the level at which Business Owners consider a KRI as acceptable (green), when an attention flag for the KRI is required (amber) and when the KRI performance/behavior is unacceptable (red). Based on the status of the KRI escalated will be required through to the Programme Risk lead team, Chair of JCEG and relevant governance and oversight groups.

The red, amber and green tolerance levels are outlined in the table below:

KRI Tolerance Level and Escalation Matrix

KRI Tolerance Level	Description	Escalation/Management Response
Green	**Acceptable:** normally no action required. However, if an indicator is 'green' but trending towards 'amber' then additional monitoring may be appropriate.	No Action

Appendix 5 – KRI process

Amber	**Raised concern:** KRI must be closely monitored and appropriate stakeholders should be notified, where necessary remediation action should be taken.	Management attention flag. Escalation to Programme Risk Lead team, PMO and Chair of JCEG. Action plans developed: - to bring KR status back to an acceptable level. Action plans must be documented. Or - explanation of why action plans are not considered necessary for a breach of tolerance and therefore have not been formulated.
Red	**Unacceptable:** KRI must be escalated to Programme Risk Lead team, reported to the appropriate governance forum, and actions implemented to manage the KRI back to the accepted tolerance level.	

1.5 Monitor and report

KRIs must be reported by the Business Owner to the Programme Risk lead team as part of their monthly risk reporting.

Depending on level of tolerance breaches and escalation/management response outlined in KRI escalation matrix above, Business owners and project workstream leads are responsible for escalating to the Chair of the JCEG, who will then determine if any further escalations are required.

The following needs to be established as part of the monitoring and reporting of KRIs:

- Determine the frequency of collecting KRIs (for example weekly, monthly, quarterly etc.). The minimum frequency will be limited by the frequency of data availability and driven by the required frequency of the KRI reporting.
- determine the frequency and required timelines for reporting, including tolerances breaches. Most commonly KRIs are required to be reported monthly.

Appendix 6 – Risk Register Template

AC36 RISK REGISTER

Prepared by: _____
‹insert designation›
Signed off by Risk Register Owner: _____
‹insert designation›
Date: _____
‹insert date›

Objective: Objectives of your workstream that contribute to the delivery of the AC36 event.

Ref ID #	Risk and Impact Description	Causes	Risk Category	Risk Owner	Inherent Risk (Untreated)			Existing Controls	Control Owner	Control Effectiveness			Residual Risk (Treated)			Additional Controls Required?	Risk Response	Previous Residual Risk Rating	Review Date	Open / Closed
					Likelihood	Consequence	Inherent Risk Rating			Design	Operating Effectiveness	Control Effectiveness Rating	Likelihood	Consequence	Residual Risk Rating					
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								
												Not Rated								

Appendix 7 – Risk Register Guidance

Risk Register Guidance

The following sections provides guidance on completion of the various fields within the AC36 Risk Register template (**Appendix 6**).

Column	Guidance
Risk ID Number	The risk ID numbers are used to easily distinguish each risk. These numbers do not need to be used to rank risks in order of severity. You can simply number the risks or use letters and numbers to identify the risk.
Risk and Impact Description	Once you have identified the risks in your area you will need to write a description that accurately describes them. An easy way to distinguish the risk is to put it in the following sentence: *'Because of ….(cause)…., there is the risk that …. (risk) …. resulting in …. (impact/effect).'* When identifying the impact, consider the consequences of the risk materialising into an incident. As there are often many causes to the risk event occurring, all possible causes must be captured in the separate column on 'Causes' in the risk register.
Causes	In this column, the underlying potential causes / drivers of the risks need to be noted. This should identify items that would lead to / drive the risk materialising. An example of a Risk Driver could be "Inadequate communication of policies and updates to staff" **Note**: To effectively manage risks, each of the drivers \ causes should be addressed through controls.
Risk Category	Risk categorisation allows grouping of risks, which is useful for reporting. Risks must be categorised using the categories listed and described within the AC36 Risk Management Framework. Select a category that best suits the risk. If you are unable to find an exact fit, choose the next best.
Risk Owner	The risk owner is the person responsible for approving, managing, reviewing and monitoring the risk to ensure that it is accurately captured and that the risk is being managed within the approved appetite level.
Inherent Risk	Under the inherent or "pre-controls" assessment, the severity of the risk is determined if there were no controls in place. When analysing inherent risk, we look at the consequences and likelihood. The register has 2 drop down boxes where the likelihood and consequence can be ranked. Likelihood refers to the possibility of the risk, and its impacts to materialise. The consequence rating refers to the level of impact that the risk will have on the AC36 objectives. When determine the consequence rating, determine the objective that will be most impacted and assign the rating that matches the level of impact expected as per the 5x5 matrix (**Appendix 3**). This matrix also indicates how the two ratings given correspond to the risk score and risk rating.

Appendix 7 – Risk Register Guidance

Column	Guidance
Existing Controls	A control is something that modifies (hopefully decreases) the level of risk. In most cases, preventative controls are the most efficient. When documenting the controls, the following questions are required to be answered: - ***What*** *is the control being performed (control type) – e.g. review, approval, monitoring, etc?* - ***Who*** *performs the control?* - ***When*** *is the control performed (control frequency) – daily, weekly, monthly, etc. or following a certain trigger (e.g. project milestone)?* - ***How*** *is the control performed (control procedures)?* - ***Why*** *is the control performed (control objective)?* Please note that controls that are in the process of being developed \ enhanced should be included in the separate field "Additional Controls Required" and until implemented they will generally not reduce the level of risk.
Control Owner	The control owner is the person/team that is accountable and/or responsible for executing the identified control(s). On a quarterly basis, control owners are required to review and monitor controls to confirm that the controls are designed and operating as intended for effective management of the risks. This program of work is known as a Control Self-Assessment (CSA). The Control Owner(s), in collaboration with the Risk Owner determines which controls are key and therefore in scope for control testing.
Control Effectiveness	Control evaluation allows the business to gauge the effectiveness of applied controls in terms of reducing the impact and/or likelihood of risk. This can help management assess whether the risk exposure is within an acceptable level or whether further controls or control improvements are required. Individual controls are assessed based on design and operating effectiveness to assign a Controls Effectiveness (CE) rating: - **Design**: how well the control should work in theory, if it is always applied as intended. - **Operating Effectiveness**: Consider the way in which the control is operating in practice, if it is applied when it should be and as intended. Control Design Effectiveness and Control Operating Effectiveness assessments are combined to give an overall CE rating, using 3x3 Control Evaluation Matrix, as detailed in the Risk Management framework.
Residual Risk Assessment (after treatment)	This second assessment is to look at the residual risk after the existing controls are taken into consideration, including that they are implemented and working as expected. If you consider the residual risk rating to be too high, look at what other controls or risk treatment can be added and include this under "Additional Controls Required". Refer to the Risk Response table in **Appendix 4** to identify the recommended approach to manage the risk based on the residual risk rating.
Additional Controls Required	If it is determined that the current residual risk is not within acceptable risk appetite, additional controls may be required to lower the residual risk rating. This section allows for these additional controls to be documented and tracked in terms of implementation. Additional controls should be documented in sufficient detail, similar to the existing controls, to ensure that their intended purpose is understood.
Risk Response	The risk treatment plan provides information on how the risk will be treated going forward. This may be through regular reviews or monitoring activities. Refer to the Risk Response table (**Appendix 4**) for guidance on the recommended risk treatments based on the risk rating.
Previous Risk Rating	Through the regular review of risks, controls and their ratings, it is likely that risk ratings will change during the project. To keep track of changes of risk ratings, this field should indicate the risk rating as at the previous review date. If there is no change in risk rating, simply note “No change” in the field.
Review Date	This field indicates the date that a risk was last reviewed. This field should be updated each time a risk is reviewed or modified.

Appendix 7 – Risk Register Guidance

Column	Guidance
Open / Close	A risk should be noted as “Open” if the risk is still present and being managed. A risk can be marked as “Closed” when: - A risk is no longer applicable due to changes in the internal / external environment, or - the scope of a project is amended, and a risk becomes irrelevant (avoided). The Risk team will review any closed risks to verify if the risk has been mitigated.

Appendix 8 – Risk Deep Dive Template

<table>
<tr><th colspan="4">Risk Deep-Dive Review Template</th></tr>
<tr><td>Risk Theme <Risk Theme></td><td colspan="3">Date of review</td></tr>
<tr><td>Risk Reference <Risk Number and description></td><td colspan="3"><Risk Number and description></td></tr>
<tr><td>Overall, current risk rating</td><td>Inherent
<Rating></td><td colspan="2">Residual
<Rating></td></tr>
<tr><th colspan="4">Risk Analysis</th></tr>
<tr><td>Underlying causes
How do you see those causes now – have they changed, are there any internal / external factors impacting the current operating environment?</td><td colspan="3"></td></tr>
<tr><th colspan="4">Risk Assessment</th></tr>
<tr><td>Current controls
Are the controls effective, sustainable and evidenced? Do you need any further controls, or has the risk reduced so that resources can be redirected?</td><td colspan="3"></td></tr>
<tr><td rowspan="2">Updated risk scores
Are there any changes to the ratings?</td><td>Inherent Likelihood
Prior: <xx>
Update: <xx></td><td>Inherent Consequence
Prior: <xx>
Update: <xx></td><td>Inherent Rating
<Rating></td></tr>
<tr><td>Residual Likelihood
Prior: <xx>
Update: <xx></td><td>Residual Consequence
Prior: <xx>
Update: <xx></td><td>Residual Rating
<Rating></td></tr>
<tr><td>If you've changed the scores, provide comments.</td><td colspan="3"></td></tr>
<tr><td>Additional controls
If more needs to be done, what do you suggest – and what are the limitations or constraints?</td><td colspan="3"></td></tr>
<tr><td>How will the implementation of planned controls be effective in improving our ability to mitigate the risk?</td><td colspan="3"></td></tr>
<tr><td>Date actions to be delivered
Is that date realistic in your view? Should the deadline be brought forward, or even relaxed? Why?</td><td colspan="3"></td></tr>
</table>

Appendix 8 – Risk Deep Dive Template

Management Attestation How do you obtain assurance that the identified controls are operating effectively and as intended?	
Emerging Issues	
Are there any issues related to the risk identified that your department is currently managing?	
Risk Assurance	
List **a**ny assurance or independent reviews conducted to assess the control effectiveness in mitigating the risks. Include date, outcomes and actions completed or underway.	
Conclusion	
Summarise approach and findings and conclude the design and/or operating effectiveness of the controls.	
Management Comments	
Provide comments on recommendations made.	
Prepared by	
Reviewed by	
Reporting date	

Appendix 9 – Control Self-Assessment Process

Control Self-Assessment (CSA) Process

1. Identify and document the controls

Controls are identified in the AC36 risk registers. At a minimum, key controls associated to inherently High or Extreme risks are to be included in a CSA to periodically test their design and operating effectiveness.

2. Define the testing approach

2.1. Overall Test Approach

When considering an overall test approach, the following factors should be carefully considered:

The timing, frequency and extent of testing: The timing, frequency and extent of testing should enable an appropriate level of testing results to be made available to the Control Owner to complete periodic control evaluations.

The number and experience of resources required: Consideration should be given to who will be performing the testing and their level of experience. The complexity of the testing approach and level of instruction and documentation supplied will dictate the required experience of the testing resources.

Control design elements:

- Preventative vs. detective vs. corrective type controls
- System vs. manual controls
- The type and materiality of risk(s) the control is applied against

Control effectiveness history: Historical measures such as Issues, Incident Management, External Loss Data or Key Risk Indicators or past testing results should be taken into consideration when determining the frequency and extent of testing.

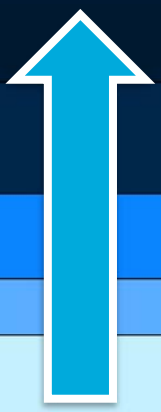
Test failure tolerances: The acceptable level and type of test failures (e.g. design failures, number in a sample, evidence requirements, etc.) noted during a test, that still achieve an overall pass should be considered and guidance provided to the test performer. Where appropriate guidance cannot be entered, it is recommended a key contact(s) be documented to provide further guidance should the test performer require advice on failures

Appendix 9 – Control Self-Assessment Process

2.2. Testing Techniques

The table below provides an overview of testing techniques and an indicative guide to the level of assurance obtained by each technique:

Testing Technique	Description	Level of Assurance
Re-performance	The test performer performs the same control steps as the control performer	High
Detailed examination/inspection	The test performer checks to source data or source documents to confirm the quality of the control.	
Evidentiary	The test performer sights evidence that the control has been performed.	
Observation	The test performer observes the performance of the control.	
Enquiry	The test performer enquires and documents how the control functions.	Low



3. CSA is scheduled

The frequency that a control is subject to CSA is determined by the overall inherent risk rating of the risks associated with the control. This is the overall risk rating in the absence of controls.

Where controls are relied upon to prevent, detect or correct AC36 most significant risks, those controls are subject to more frequent assurance. The following control frequencies apply.

Inherent risk rating	Frequency of CSA
Extreme	Quarterly
High	Quarterly
Medium	Six-monthly
Low	Six-monthly

Where a control is associated with risks of different risk ratings, the highest risk rating determines the CSA frequency. For example, if a control is associated with one risk that has a high inherent rating and one risk that has a low inherent rating, a six-monthly CSA will be required.

Appendix 9 – Control Self-Assessment Process

4. Complete CSA

4.1. Notification of CSA

Control owners will receive a notification from Programme Risk Lead team notifying them of the CSA's due. A completed CSA template and demonstration of control effectiveness is required to be returned to the Programme Risk Lead team within the timeframe specified in the CSA request.

4.2. Document and update Control Effectiveness ratings

When control testing is complete, test results are documented, and the Control Owner advised. The Control Owner will decide whether to update the Design Effectiveness or Operating Effectiveness results to arrive at a new overall Control Evaluation Effectiveness rating as per the 3x3 Controls Evaluation Matrix included in Appendix xx.

4.3. Review, Report, Manage

Programme Risk Lead team to review and ensure that key controls have been correctly identified in the AC36 risk registers and timely CSA's are in place over these controls.

Programme Risk Lead team will monitor resolution of exceptions identified through the CSA process. The CSA test results will be reviewed by the Programme Risk Lead team.

Testing results will be communicated to risk owners in a timely manner to determine the appropriateness of the associated risk ratings.

PMO and JCEG will receive a monthly CSA report. The report will include information regarding CSAs that have been completed, and the resolution of any exceptions identified.

Appendix 10 – Issue and Incident Management Process

1. Identifying the Issue

Everyone is responsible for reporting issues and incidents.

Incidents should not be confused with issues. An issue is defined as a control weakness or gap that highlights a deficiency in the mitigation of an identified key risk or meetings compliance obligations.

An incident is defined as a situation where a risk has or may have materialized due to inadequate or failed processes, people, systems and external events. This includes compliance incidents, operational losses, and internal and external fraud.

1.1. Assigning Roles

For every issue / incident there are three key roles that must be fulfilled:

- Issue / Incident Owner - is the person who is accountable for the issue / incident. This includes accountability for progression and closure.
- Issue / Incident Manager - is the person responsible for managing the issue through to completion on behalf of the Issue / Incident Owner and may be the same person as the Issue Owner / Incident Owner. Management activities include notifying the Issue/Incident and Action Owner on status reporting/updates, managing date extensions and rating change requests, etc. Any changes to issue or action detail must be reflected in the issue/incident register.
- Action Owner - is the person responsible for executing a given action. This may be the same person as the Issue / Incident Owner. This person is responsible for updating the Issue Manager with the action progress/status. Action Owners can be from different workstreams depending upon the nature of the action required. The Action Owner is also responsible for providing appropriate periodic status updates on actions to the Issue / Incident Manager.

2. Recording

2.1. When and how are issues required to be recorded?

Workstream leads and risk representatives must ensure that issues and incidents, irrespective of how they are identified, are captured in the Issues and Incident register (included in Appendix 10a) and are reported, rectified and closed in a timely manner. An issue / incident assessment report (included in Appendix 10b), must be completed for all issues / incidents.

Issues and incidents are required to be recorded and reported on after being identified - this should be within 5 business days of identification.

Every issue must be categorised by issue type, which includes:

- Control weakness/gap
- Loss incident remediation

Appendix 10 – Issue and Incident Management Process

- Compliance incident remediation
- Process improvement
- Non-compliance with internal policies

Every Incident should be categorized by incident type, which includes:

- Operational risk (loss or gain)
- Near miss (including rapid recovery)

2.2. Who Identified the issue / incident?

The issue / incident date raised must be accurately recorded, including the origin of the issue (individual that identified the issue), as follows:

- Line 1 identified – any issue identified in Line 1 during BAU activities
- Line 2 identified – any issues identified by Line 2.
- Internal Audit identified – any issue identified by line 3 during an Internal Audit review.
- External Audit Identified – any issues identified by external audit in conducting external audit activities.

2.3. What risk does the issue / incident relate to?

All issues / incidents are required to be associated to the control(s) and/or risk(s) to which they relate to in the risk registers. Associations should also be made to an incident(s) where an issue is raised for remediation activities or incident analysis has identified a control weakness or gap.

Identify the risk reference and the risk category this risk relates to. It is possible to have more than one Risk reference and Risk Category for each issue / incident, i.e. the issue / incident may apply to more than one risk or risk category.

2.4. How to rate an Issue

Once identified, an issue / incident rating must also be assigned. This rating ranks the significance of the issue / incidence and the importance of its remediation, which is determined by the 4-point scale: Extreme, High, Medium and Low.

For most issues / incidents, the rating of the issue should be assessed based on the risk that the issue / incident represents. That is, as a result of the issue / incident, what is the likelihood of the risk event happening and what would be the impact?

This impact will be based on the 5x5 Risk Assessment Matrix. It should be noted that when rating an issue / incident, the financial and non-financial impacts also need to be considered. In many cases, the larger impacts could in fact be non-financial.

These ratings should be discussed and agreed upon by the Workstream Leads. The Programme Risk Lead team may challenge the rating applied and recommend a different rating through discussions with the Issue / Incident Owner. Where agreement cannot be achieved the issue / incident will be escalated to the internal governance arrangements.

Appendix 10 – Issue and Incident Management Process

The rating of an issue / incident will determine the level of escalation and reporting, as defined in section 4 below.

3. Monitoring and review

Continuous monitoring and reviews of issues / incidents and action status throughout the life of an issue / incident is important. The Issue / Incident Manager should provide periodic updates and reporting to the Issue /Incident Owner on the status of actions. This should include commentary on issue / incident status to be provided to the Issue / Incident Owner.

4. Escalation and Reporting

All issues / incidents rated Medium and above must be reported to the AC36 Programme Risk Lead and PMO. Updates on the issues / incident management, including remedial actions taken will be provided to JCEG and other assurance committees.

5. Remediation

5.1. What is an action?

A remedial action is a task to rectify the underlying factors that lead to an issue / incident.

Each issue / incident must have one or more action(s) to remedy it, each action should be recorded in the issue / incident register.

5.2. Issue and Action Due Dates

Issue / incident due dates will be dictated by the date of the last action to complete. Due dates are required to be agreed and documented.

Each action must be completed by the assigned due date unless a due date extension request is sought and approved by the issue / incident owner.

When agreeing action plans and setting due dates, care should be taken to ensure these:

- Are realistic and practical to implement
- Are achievable within the agreed time
- Take Into consideration the scope of any exiting work plans and relative priorities
- Align with the broader AC36 initiatives at either a strategic or operational level.

6. Closure

The Issue / Incident Manager is responsible for viewing all appropriate evidence and performing quality assurance to ensure the action(s) has been appropriately completed as agreed.

Appendix 10 – Issue and Incident Management Process

Following completion of the final action, the Issue / Incident Manager is responsible for collating all appropriate evidence and presenting it to the Issue / Incident Owner to obtain approval to close the issue / incident.

The Issue / Incident Owner must review evidence that all required actions have been completed satisfactorily and approve closure. Evidence of this approval is required to be recorded.

The issue / incident Closed Date is the date that the evidence has been reviewed by the issue / incident owner and approval for closure has been provided.

Approval to close the issue / incident confirms that all actions have been satisfactorily completed and the root cause of the issue (i.e. control weakness or gap, incident remediation, etc.) has been addressed.

Programme Risk Lead team may review and challenge data quality, ratings and resolution progress and have oversight over the appropriate closure of all issues / incidents rated Medium and above. Programme Risk Lead team will, on a sample basis, validate the closure of issues of lower criticality rating.

Appendix 10a – Issue and Incident Register Template

AC36 ISSUE /
INCIDENT REGISTER

Prepared By: _____ Date: _____
Approved By: _____ Date: _____

ID #	Issue / Incident Description	Issue / Incident Category	Root Cause	Rating	Action(s)	Action Owner	Due Date	Risk Reference	Identified By	Issue / Incident Owner	Issue / Incident Manager	Open/Closed	Closure Approval

Appendix 10b – Issue and Incident Template

Incident / Issue Assessment Report

Prepared by: enter text. **Reviewed By:**enter text.

Incident / Issue Name	This is the name that will be included in reports and should provide a clear indication of the incident / issue. e.g. “Damage to wharf asset”
Incident Summary	Please provide a summary of the event, including: • What lead to the event occurring? • How was the event discovered? • Who discovered the event?
Process	Which process \ activity does the event relate to? • Briefly explain the process. • At which stage of the process did the event occur.
Impact	What was the resulting impact of the incident / issue, such as: • Financial (gain or loss) • Delays while remedying the event • Health and Safety • Regulatory
Root Cause	What underlying control failure or gap lead to the event occurring. These could include circumstances around: • Human error • System limitations • External events • Non-compliance to processes • inadequate processes
Remedial Actions Taken	What actions are planned or have been taken to remedy and prevent future occurrences of the event? Each action should include an owner (person responsible for implementing the remedial action) as well as the expected completion date.
Risk Reference	Include reference to the risk(s) in the risk register that this event relates to.
Existing Controls	Define the controls that are currently in place to manage the risks reference.
Control Effectiveness Rating	Following an event occurring, risk and control owners need to review the risks related to the event and reassess the effectiveness of the controls. The results of this assessment should be updated on the risk register and included here.

Appendix 11 – Control Effectiveness Rating and 3x3 Evaluation Matrix

Design Effectiveness

Design Effectiveness	Criteria
Weak	The control design does not meet the control objective
Sufficient	The control design mostly meets the control objective
Strong	The control design meets the control objective

Operating Effectiveness

Operating Effectiveness	Criteria
Not effective	The control is not applied or applied incorrectly
Partially Effective	The control is normally operational, but on occasion is not applied when it should be, or not as intended.
Effective	The control is operational the majority of the time and in the way intended by design.

Control Self-Assessment 3x3 Matrix

		Operating Effectiveness		
		Ineffective	Partially Effective	Effective
Design Effectiveness	Strong	Unsatisfactory	Marginal	Satisfactory
	Sufficient	Unsatisfactory	Marginal	Satisfactory
	Weak	Unsatisfactory	Unsatisfactory	Unsatisfactory

Appendix 12a – Monthly Risk Report Template

The following report template must be used for risks, issues and incident reporting to provide the JCEG a complete view of risk and compliance management across the programme.

1. Content and Purpose
1.1 Monthly risk update to JCEG for period

2. Recommendations
2.1 To note the paper or make a decision

3. Summary of Risk Activities
3.1 Summary of risk activities completed/underway

4. Risk Profile
4.1 Commentary
4.2 Summary of risk registers, attachments including risk heat map

5. Issues
5.1 Summary of issues, status update and remedial action

6. Incidents
6.1 Summary of incidents, status update and remedial action

7. Controls Self-Assessment (CSA)
7.1 Summary of control self-assessment results and remedial actions

8. Key Risk Indicators (KRI)
8.1 Summary of trends, KRI exceptions etc, commentary for KRI exceptions.

9. Risk Appetite
9.1 Summary of risk appetite monitoring, approval, risks within/outside appetite.

10. Risk Dashboard
10.1 Summary of results of defined measures that can assess how effectively the risk framework is embedded across the programme.

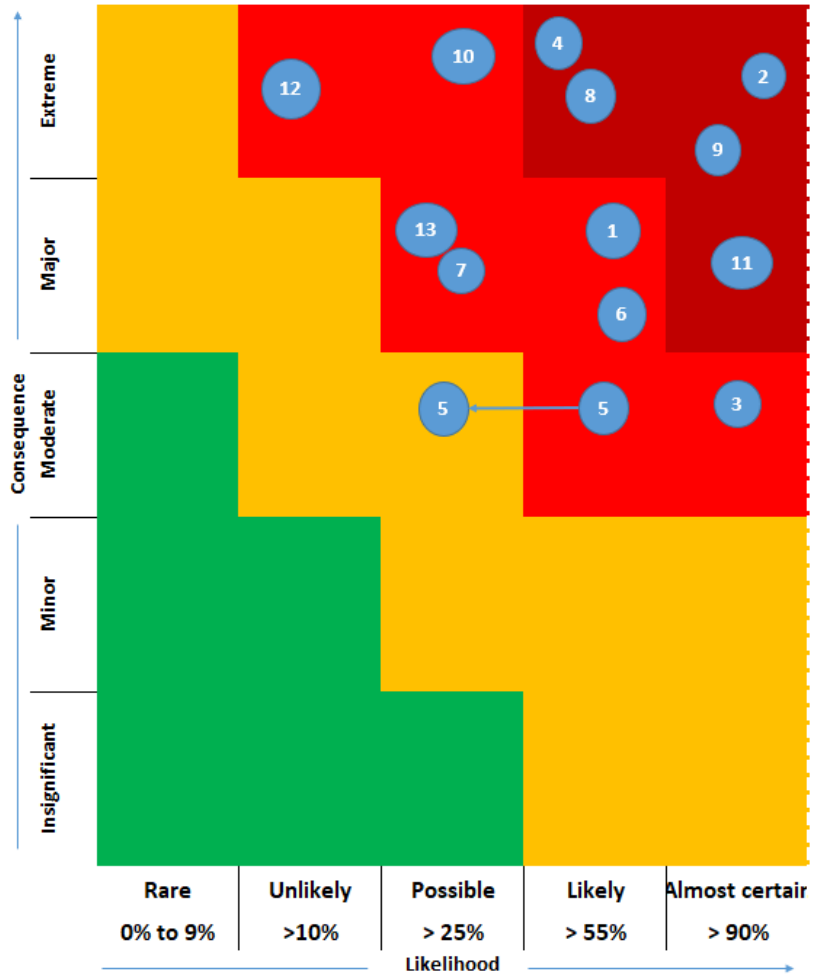
11. Assurance Reviews and Issues Raised
11.1 Summary of reviews - ratings, issues raised, material observations etc

12 Health and Safety
12.1 Summary of actions taken or any issues arising during the period of reporting

Prepared by: xxx
Date: xxx

Appendix 12b – Risk Heat Map Template

Inherent (Prior to Controls) Risk Heat Map Template



ID	Risk Item	Overall Rating
1	Environmental Sustainability	High
2	Relationships	High
3	Brand and Reputation	High
4	Health and Safety	Extreme
5	Fraud and Corruption	Moderate
6	Legacy	High
7	Procurement	High
8	Financial Management	Extreme
9	Programme and Project Delivery	Extreme
10	Assets	High
11	Infrastructure and Event Consents	Extreme
12	Significant Disruptions	High
13	Governance	High

Arrows on a Risk Dot indicate the Trend of the risk (i.e. increasing or decreasing) for the period

Any changes to ratings need to include reasons for the change.

Appendix 12c –Risk Reporting Requirements

From	Frequency	What	Levels of Escalations
Workstreams • Finance • Legal and Commercial • Procurement • Mana Whenua • Regulatory • Legacy • Leverage • Event Working Group • Waterfront Integration • Inter-agency Steering Group • Security Steering Group	Monthly	Risks	High, Extreme
	Monthly	Issues	High, Extreme
	Monthly	Incidents	High, Extreme
	Quarterly	Control Self-Assessments/Control effectiveness	High, Extreme
Wynyard Edge Alliance	Monthly	Risks, issues and incidents	High, Extreme
Event Steering Group	Monthly	Risks, issues and incidents	High, Extreme