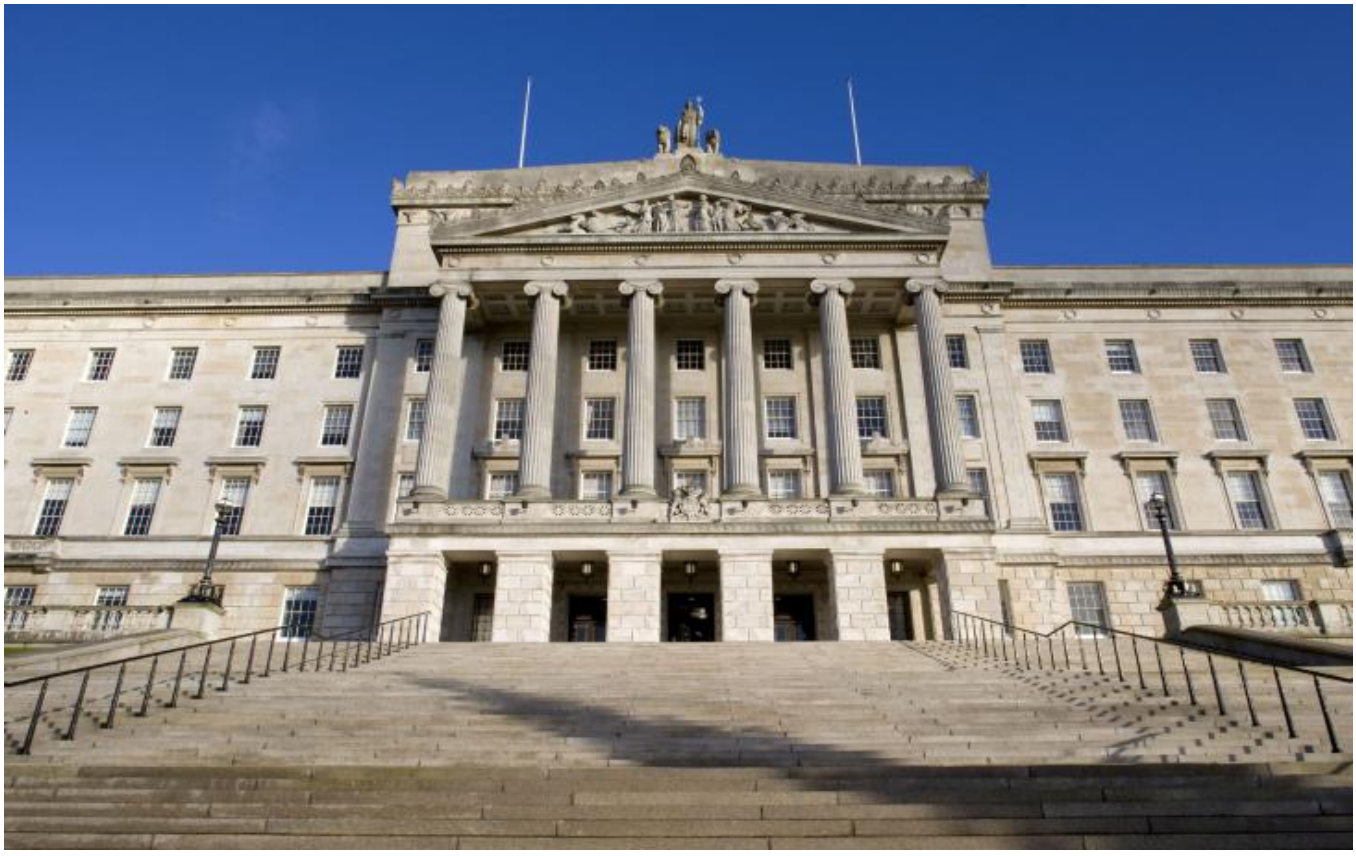
Northern Ireland Assembly

Risk Management Strategy

Directorate of Legal, Governance & Research Services

Revised April 2019



To receive this strategy in alternative formats contact Governance Officer on ex 21242

CONTENTS

1 Introduction to Risk Management

1.1 The Northern Ireland Assembly Commission ("the Assembly Commission") is the corporate body which provides the Assembly, or ensures that the Assembly is provided with the property, staff and services required for the Assembly's purposes. The Assembly Secretariat is the body of staff employed by the Commission which on a day-to-day basis delivers those services. Throughout this document references will be made to both the Commission and the Secretariat in this context. Good governance leads to good management, good performance, good stewardship of public money, good public engagement and, ultimately, good outcomes for the public and service users. Good governance enables the Assembly Commission to pursue its vision effectively and underpins that vision with mechanisms for control and management of risk.

1.2 An essential aspect of good governance is the way the Assembly Secretariat manages the risks that the Assembly Commission faces.

1.3 Risk is any event or uncertainty that may enhance or impede our ability to achieve our current or future aims. This definition makes a direct connection between risk and the Corporate Aims of the Assembly Commission as set out in the Corporate Strategy and Corporate Plan.

1.4 Risk Management is an essential part of good management and governance, which well-run business units will already perform on a day-to-day basis.

> Risk Management is defined as: "the process of identifying risks, evaluating their potential consequences and determining the most effective methods of controlling them and / or responding to them".

1.5 When risks are managed effectively, objectives are more likely to be achieved. Conversely, when risk management fails, the consequences can be significant and high profile and can threaten the achievement of both the business and corporate objectives and ultimately have an impact on the level of service delivery.

1.6 When Risk Management processes are in place in an organisation:

- There is regular and ongoing monitoring and reporting of risk including early warning mechanisms;
- An appropriate assessment is made of the risk appetite and the cost of operating particular controls relative to the benefit obtained in managing the related risk;
- The organisation conducts annually a review of the effectiveness of the system of internal control in place by way of a Governance Statement; and
- Corporate and Directorate Risk Registers are aligned to allow the escalation and de-escalation of Risks.

1.7 Risk Management should be ongoing, embedded in the culture of the organisation, and have the potential to re-focus the whole organisation around

performance improvement. It is used to complement the normal corporate and business planning processes, at a strategic level or at a project, function or site level. However, it is not a process for avoiding risk. When used well, it can actively encourage an organisation to take on activities that have a higher level of risk, because the risks have been identified and are being well managed and the exposure to risk is both understood and acceptable.

1.8 A comprehensive and sound Risk Management Strategy will bring the following benefits:

- A clear assessment of the risks affecting the achievement of Assembly Commission business aims, providing a supporting role to the corporate and business planning process;
- Enhanced communication within and between Directorates through a greater appreciation and understanding of the risks facing the organisation;
- Better use of resources, by directing these to areas of most need;
- The promotion of a culture of continuous improvement;
- More effective tailoring of internal audit programmes;
- A reduction in unwelcome surprises / shocks; and
- Reassurance to the Accounting Officer, the Assembly Commission, the Secretariat Audit and Risk Committee (SARC) and stakeholders that the Secretariat is continually reviewing the operational environment and actively identifying and managing risk.

1.9 The Risk Management Framework consists of the following key elements:

- This Risk Management Strategy;
- Quarterly review of the Corporate Risk Register by the Secretariat Management Group (SMG);
- Six-monthly presentation of the Corporate Risk Register to the Commission;
- Corporate Risk Register reviewed at SARC meetings;
- Monthly review of Directorate Risk Registers by Directors; six-monthly review by SMG; and annual review by SARC;
- Stewardship Statements, provided by Risk Owners to the Clerk/Chief Executive twice yearly (Standard template at Annex B);
- Stewardship Statements submitted to SARC twice yearly;
- Internal risk-based audit by Internal Audit Unit;
- External risk-based audit by the Northern Ireland Audit Office (NIAO);
- The Annual Governance Statement;and
- Annual completion of NIAO's Risk Management checklist

2 Purpose of this document

2.1 It is essential that the approach of SMG towards risk is communicated to all staff in the Assembly Secretariat and that it is applied in decision making regarding the prioritisation of policies, workstreams, programmes, projects, operational service delivery and the funding that goes with them.

2.2 If managers in business areas have insufficient guidance on the levels of risk that are legitimate for them to take, or are not seizing important opportunities due to a perception that taking on additional risk is discouraged, then performance will not be maximised, and opportunities will not be taken. At the other end of the scale, an organisation constantly erring on the side of caution (or one that has a risk averse culture) is one that is likely to stifle creativity and is not necessarily encouraging innovation, nor seeking or exploiting opportunities.

2.3 It is acknowledged that the public sector reward and assessment systems may well emphasise the adverse impact of failure rather than the gains from success and so encourage excessive risk aversion. However, it is also acknowledged that innovation and opportunities to improve public services require **well-managed** risk taking.

2.4 This Risk Management Strategy forms a central part of the Assembly Secretariat's internal control and corporate governance arrangements. It defines the Secretariat's approach to Risk Management throughout the organisation. It ensures a consistent approach to dealing with risks which may have an impact on the Secretariat's ability to achieve the Commission's vision, strategic goals and aims. It also facilitates compliance with current governance requirements and guidelines:

- DAO (DFP) 10/12: Accounting Officers to complete a Governance Statement to be published with the Accounts each year, reflecting the organisation's governance, risk management and internal control arrangements and how they operate in practice;
- HM Treasury's "Management of Risk – Principles and Concepts" ("The Orange Book"), 2004;
- The Department of Finance's Corporate Governance in Central Government Departments: Code of Good Practice (NI) 2013;
- The Department of Finance's Audit and Risk Assurance Committee Handbook NI 2018;
- NIAO's "Good Practice in Risk Management" 2011; and
- Management of Risk in Government – A Non-Executives Review - January 2017.

2.5 The strategy defines the key roles and responsibilities in managing risk within the Assembly Secretariat and the working processes that are to be used.

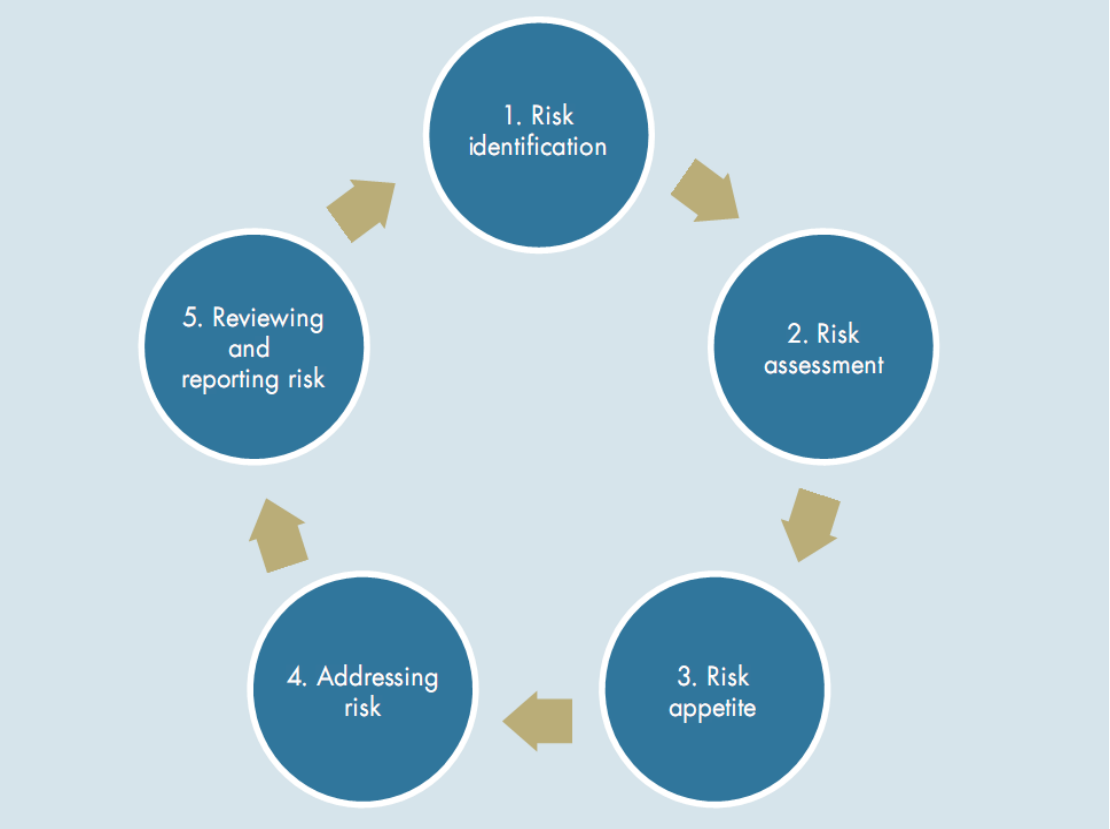
2.6 This document also sets out the Assembly Commission's approach to defining risk appetite and describes how risk appetite is to be used in the management of risk.

3 Risk Management Process & Procedures

3.1 The Risk Management process is adapted from a standard model. It incorporates five phases:

- Risk identification;
- Risk assessment;
- Risk appetite;
- Addressing risk; and
- Reviewing and reporting risk

Risk Management Cycle



Step 1 - Risk Identification

3.2 In the first phase, you identify risks which may impact, positively or negatively, on the Assembly Commission's ability to achieve its aims.

The aim is to identify what, when, where, why and how events occur that could prevent, degrade, delay or enhance the achievement of aims.

What is meant by risk?

3.3 Risk is any event or uncertainty that may enhance or impede our ability to achieve our current or future aims.

When should I do this?

3.4 **Initial** risk identification should be undertaken when the Secretariat undertakes substantial new activity — for example, on the establishment of a new business plan, or on the initiation of a project. Risk assessment and management is a routine element of all policy or project development.

3.5 **Continuous** risk identification should then be undertaken. Regularly review so as to identify new risks as they arise, to make changes to existing risks, or to discount risks which are no longer relevant.

How should I do this?

3.6 Have an open mind, consider all issues and be creative. It can help to focus on three main categories of risk.

External risks, arising from the external environment, not wholly within our control. For example, these might arise in relation to	
political events financial change external fraudulent activity	technological development legal change environmental impact

Operational risks, arising internally from existing operations, including current delivery, or building and maintaining our capability. For example, these might arise in relation to	
service failure project delivery resources constraint human relationships	internal governance internal fraudulent activity resilience security

Change risks, arising internally from decisions to pursue new activities beyond current experience or capability. For example, these might arise in relation to:	
change programmes and projects new projects	new policies new work strands

3.7 You should approach Risk Identification in a methodical way to ensure that all significant activities have been identified and all risks flowing from these activities have been defined.

3.8 Risk must always be related to Assembly Commission Corporate Aims, to be found in its Corporate Strategy, its Corporate Plan and in Business Area Plans. But a risk is different from a failure to achieve an existing aim. So the risk you identify should not be, for example, 'failure to deliver aim x'. Instead the risk should identify the event or uncertainty that may enhance or impede your ability to achieve that aim.

3.9 Other than having an open mind and ensuring that you look to the future, there is no single method that you should use. You could, for example, use:

- Workshops;
- Directorate meetings;
- Past experience; and
- Audit reports (by Internal Audit and the Northern Ireland Audit Office).

Who becomes responsible?

3.10 Once the risk is identified and understood, you should allocate it to a specific post-holder. Ownership of key Corporate Risks is usually assigned at Director level. The risk owner must ensure that the risk is managed and monitored appropriately, so that assurance on the management of the risk can be provided to the Accounting Officer and to the Secretariat Audit and Risk Committee.

3.11 Ownership of Directorate-level risks may be allocated to Heads of Business or other responsible officers, depending on the nature of the identified risk and the potential impact on business. Ownership of risk should be included in Performance Conversations, and risk owners should receive the necessary support and resources to manage key risks.

Step 2 - Risk assessment

3.12 The second phase is to assess the **inherent** risk to the activities of the Assembly Commission. Inherent risk is the exposure arising from a specific risk before any action is taken to manage it. This involves assessing the probability of a risk occurring and its potential impact on the relevant business objective.

The aim is to understand the scale of the risk.

Two Dimensions

3.13 You should do this on a scale of 1 to 5 in each dimension, remembering that this is a management art, not a precise science. In respect of impact, it may help to consider the following indicators:

Rating	Achievement of Objectives	Financial	Reputation	Business Interruption
5 - Critical	Failure to deliver the majority of key aims	Financial loss / damage > £100k NIAO qualification of accounts	Severe adverse media attention likely to significantly affect long-term public perception of the Assembly, the Assembly Commission or the Assembly Secretariat and political affairs	Interruption during a critical period leading to extended loss of service (greater than 1 week) Interruption due to short or long term critical system failure
4 - Major	Failure to deliver more than one key aim	Financial loss / damage between £50k - £100k NIAO "technical" qualification of accounts	Adverse media attention likely to affect medium to long-term public perception of the Assembly, the Assembly Commission or the Assembly Secretariat	Interruption during a critical period leading to loss of service (2 to 5 days) Interruption due to short term critical system failure
3 - Significant	Failure to deliver one key aim	Financial loss / damage between £25 - £50k NIAO criticism	Adverse media attention likely to affect medium-term public perception of the Assembly, the Assembly Commission or the Assembly Secretariat	Interruption during a critical period leading to temporary disruption (1 day or less)
2 - Moderate	One or more key aim is only just delivered	Financial loss / damage between £10k - £25k NIAO lesser criticism	Adverse media attention likely to affect short to medium-term public perception of the Assembly, the Assembly Commission or the Assembly Secretariat	Interruption during a non-critical period leading to temporary disruption (greater than 1 week)
1 - Minor	No risk to demonstrating the delivery of key aims	Financial loss / damage < £10k	Adverse media attention likely to affect short-term public perception of the Assembly, the Assembly Commission or the Assembly Secretariat	Interruption during a non-critical period leading to temporary disruption (less than 1 week)

3.14 In respect of probability, it may help to consider the following indicators:

Rating	Description
5 - Almost Certain	85% chance of occurrence Is expected to occur in most circumstances Has occurred frequently within the Assembly Commission or comparable public authority
4 - Probable	60% - 84% chance of occurrence Will probably occur in most circumstances. More likely to occur than not to occur Has occurred recently within the Assembly Commission or comparable public authority
3 - Possible	31% - 59% chance of occurrence Could occur at some time Has occurred recently within a comparable public authority
2 - Unlikely	11% - 30% chance of occurrence Might conceivably occur at some time. More likely not to occur than to occur Has not occurred recently within a comparable public authority
1 - Remote	10% or less chance of occurrence May occur only in exceptional circumstances Has never been known to occur before within a comparable public authority

The Matrix

3.15 The scores will also be visualized in a 5x5 risk matrix. The closer the risk is to the top right, the more attention is required to be given to mitigating the risk. A **gross risk score** is calculated by referencing the Impact score against the Probability score.

Impact							
	Critical	**5**	G	Y	A	R	R
	Major	**4**	G	Y	A	A	R
	Significant	**3**	G	Y	Y	A	A
	Moderate	**2**	G	G	Y	Y	Y
	Minor	**1**	G	G	G	G	Y
			Remote (<10%)	**Unlikely (11-30%)**	**Possible (31-59%)**	**Probable (60-84%)**	**Almost Certain (>85%)**
			1	**2**	**3**	**4**	**5**
	Probability						

Step 3 - Risk appetite

3.16 The third phase is to determine risk appetite. Risk appetite is defined by HM Treasury as being: "The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time". Risk appetite can be thought of as our level of willingness to let the event occur.

3.17 Understanding appetite then allows you to decide whether your controls in relation to the risk are strong enough, and, if not, what controls to put in place.

3.18 **When considering threats**, risk appetite clarifies the level of exposure which is considered tolerable and justifiable, should it be realised. It relates to comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance; or

3.19 **When considering opportunities**, risk appetite clarifies how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. It relates to comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).

The aim is to set clear guidance to all staff, and set a common understanding, on the degree to which staff can limit the organisation's exposure to the consequences of an event or situation.

3.20 Risk appetite is about thinking through the risk against the rewards that may be realised. The significance of a risk will be an important factor in determining risk appetite. The appetite will also be influenced by the nature of the risk.

3.21 In the HM Treasury publication on "Managing your Risk Appetite", five levels of appetite are defined:

Risk Appetite

Classification	Description
1 - Averse	Avoidance of risk and uncertainty is a key organisational objective
2 - Minimalist	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward
3 - Cautious	Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward
4 - Open	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc.)
5 - Hungry	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk

3.22 The HM Treasury guidance outlines example behaviours when taking key risk appetite decisions across four categories of risk. This is set out in Annex A.

3.23 The categories are:

i. Reputation and credibility;
ii. Operational and policy delivery;
iii. Financial/VFM; and
iv. Compliance-legal/regulatory.

3.24 In defining the Assembly Commission's risk appetite, SMG has adopted these broad categories, although they have been adapted to reflect key elements of the Corporate Strategy. It is important to note, however, that these are broad categories for guidance purposes and there may be individual risks within any of these categories which could warrant a lower or higher tolerance. It is also important to note that individual risks should be carefully considered in each business area as they will not always fall neatly into a single category.

3.24 SMG has set levels of risk appetite for the categories of risk. These are outlined in the table below and will be reviewed annually.

Risk Category / Type	Risk Appetite Classification	Comment
Reputation: Commission & Corporate	3 Cautious / 4 Open	The Assembly Commission is willing to consider all options and has a desire for successful delivery. *Corporate Aims DEVELOPING and BUILDING apply**
Reputation: Assembly & Parliamentary	1 Averse / 2 Minimalist	The Assembly Commission's goal to provide effective and high quality support to the Assembly is predicated upon the Assembly Commission and its Secretariat having a sound reputation and credibility. There is therefore a low tolerance for risks that could lead to adverse scrutiny. Risk taking is limited to events where there is no chance of any significant impediment to the achievement of this goal. *Corporate Aim DEVELOPING applies**
Operational & Policy Delivery	4 Open	Assembly Commission and its Secretariat are willing to consider all options, including systems / technology to enable operational delivery; decisions made at most appropriate level, as set out in framework of delegation. *Corporate Aims INVESTING, BUILDING and STRENGTHENING apply**
Financial	4 Open	Assembly Commission and its Secretariat are willing to consider value and benefits, not just cheapest price, within context of MPMNI and extant guidance. *Corporate Aim BUILDING applies**
Legal / Environmental	1 Averse / 2 Minimalist	The Assembly Commission and its Secretariat will comply with all legal and regulatory requirements and the risk appetite is averse in this area; for example, in relation to compliance with health and safety requirements. In relation to potential legal challenges, the Assembly Commission and its Secretariat prefer business delivery options that have a low degree of inherent risk. Actions will be consistent with the Assembly Commission and its Secretariat being confident of winning any challenge. *Corporate Aims BUILDING and DEVELOPING apply**

*Corporate Aim: INVESTING in the development expertise and well-being of our people
**Corporate Aim: BUILDING excellence and innovation in our services
*Corporate Aim: STRENGTHENING engagement with the public
*Corporate Aim: DEVELOPING a confident legislature with a strong parliamentary culture

Step 4 - Addressing the risk

3.26 The fourth phase is the most important. You decide how to address the risk.

The aim is to respond to the risk in an appropriate way.

3.27 By addressing the risks identified, we constrain threats and take advantage of opportunities. There are four approaches to addressing a risk. The choice will depend on factors such as appetite, cost, feasibility, probability and impact.

Terminate
Decide not to take the risk, or cease the activity which causes the risk Where the risks outweigh the possible benefits, risk can be terminated by doing things differently and thus removing the risk, where it is feasible to do so. This is not always possible in our provision of services to the Assembly, or when required by law or regulatory measures. But the option of closing down a project or programme where the benefits are in doubt as a result of risk factors must be a real one.

Tolerate
Accept the risk This may be where the risk is external and therefore the opportunity to control it is limited, or where the probability or impact is so low that the cost of managing it would be greater than the cost of the risk being realised. This option may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

Transfer
Transfer the risk to another party who can take on some or all of it more economically or more effectively For example, this could be achieved through another organisation undertaking the activity, or through obtaining insurance. It is important to note that some risks may not be fully transferable – in particular, it is generally not possible to transfer reputational risk even if the delivery of the service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure successful transfer of risks.

Treat
Mitigate the risk In practice, this is the most common response to risk. It is achieved by eliminating the risk or reducing it to an acceptable level by prevention or another control action.

3.28 You should expect that, in relation to many risks, you will already have many controls in place. For example, in a procurement exercise, by abiding by the Secretariat's procurement procedures you will benefit from the controls already established therein. You will, however, also need to consider what further controls are necessary. In practice, it can help to consider four different types of controls.

Preventative controls
Designed to limit the possibility of an undesirable outcome being realised The majority of controls implemented belong to this category. For example, password access to computers, supervisory checks and independent authorisation on payments made to suppliers. Effective communication and training provision, in relation to risk management, are also preventative controls.
Directive controls
Designed to ensure that a particular outcome is achieved For example, requiring that staff are trained before being allowed to work unsupervised, or developing an office procedures manual.
Corrective controls
Designed to correct undesirable outcomes which have been realised Applied after the event, these may consist of contractual remedies to recover overpayments or obtain damages or a detailed contingency plan that will be triggered by an event (e.g. disaster recovery or business contingency plans).
Detective controls
Designed to identify occasions of undesirable outcomes having been realised Applied after the event, so these are only appropriate when it will be possible to accept the loss or damage incurred. Examples of detective controls include stock or asset checks, reconciliations and post-implementation reviews.

Risk Response should not be disproportionate to the risk

3.29 It is important that the response put in place is proportional to the risk. Apart from the most extreme undesirable outcome, it is normally sufficient to respond in a way that gives reasonable assurance of confining likely loss within our risk appetite. Every response has an associated cost, and it is important that the response offers value for money in relation to the risk that it is controlling.

Assessing the target risk scoring

3.30 When assessing a risk, and your risk appetite towards that risk, you should set a target risk score – the level to which you eventually want to reduce the risk.

Assessing the residual risk

3.31 Once you have decided on how to address the risk, assess the **residual** risk, in the same manner as you did for inherent risk. This reflects how the risk exposure has changed as a result of our response. This is referred to as **residual** risk and can be described as the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.

3.32 It is possible that, due to there being only a five-point scale in each dimension, the residual assessment may show the same levels or gross rating as the inherent assessment. If that occurs, then pay close attention to whether the controls are suitable and proportionate. Consider whether the controls are adequate, and whether any resultant gap in control is acceptable; that is, whether it is compatible with appetite.

3.33 Two questions can assist you in using appetite to determine whether further actions are required: 'Is the risk owner content [given the risk appetite] that the controls are adequate?' And 'If no, is the risk owner content that the gap in control is acceptable?'

3.34 If the answer to the second question is no, then you should decide on actions to improve control, and plan and deliver those actions. See "Achieving the target risk scoring".

Achieving the target risk scoring

3.35 Once you have assessed the residual risk score, and considering the **target** risk score that has been set, you should assess whether further actions are required to achieve the target risk score. Responses yet to be put in place are now taken into account and are recorded as "Additional actions to manage the risk" in the Risk Register, with standard Action Planning details of by whom and by when they will be delivered and how often they will be performed and how they will be evidenced. Actions and targets should be SMART.

Step 5 - Reviewing and reporting risk

3.36 The fifth phase is to record the risk management process through the maintenance of a risk register. Risk registers are maintained at strategic level (Corporate Risk Register) and operational (Directorate Risk Registers and Project Risk Registers). The standard Secretariat template is set out in Annex C and should be used at all levels of Secretariat operation. Note however that projects are managed in accordance with Guidance on the use of PRINCE2 project management methodology in the Northern Ireland Assembly.

The aim is to maintain and monitor information on the risk and the associated control actions that we have or plan to put in place in response to the risk. The register is the record and is not the purpose of the process.

Regular review

3.37 **Risk registers are living documents and every aspect of them, including appetite, should be reviewed regularly.** Each Director must review his or her Directorate Risks monthly and record changes on the relevant Register. As the nature of individual risks, along with their treatment, may change over time, this review will facilitate an ongoing assessment of the appropriateness of the manner in which each risk is managed.

3.38 Risk registers can get cluttered with out-of-date risks. While it is important that you identify any new risks, you should also remove any risks which are no longer valid or which have been fully addressed.

Escalation

3.39 If a risk on a sub-Directorate Risk Register achieves a residual amber risk score then it should be reported to the Director for consideration (and possible inclusion in the Directorate Risk Register).

3.40 **If a risk on a Directorate Risk Register achieves a residual red risk score then it should be reported, by exception, to SMG for consideration (and possible inclusion in the Corporate Risk Register) as it arises and in advance of the next scheduled quarterly review of the Corporate Risk Register at SMG. Directors should also consider drawing SMG's attention to Directorate Risks achieving an amber risk score.**

The Reporting of Risk

3.41 Directorate Risk Registers will be considered twice a year by SMG. The Corporate Risk Register is reviewed quarterly at SMG.

3.42 The process of regularly updating and reviewing Risk Registers will be monitored by SARC and will form part of its annual report to the Accounting Officer. SARC should reflect on whether any of the following matters need to be included in the Annual Report:

- Any significant change in the nature and extent of the risk profile of the organisation since the last report;
- The scope and quality of management's ongoing monitoring of risks and of the system of internal control, and, where applicable, the work of internal and external audit;

- Any significant gaps in the provision of Stewardship Statements; and
- The incidence of significant control failings or weaknesses that have been identified at any time during the reporting period.

4 Roles and Responsibilities

Clerk/Chief Executive

4.1 The Clerk/Chief Executive is the Accounting Officer under the Managing Public Money Northern Ireland framework. He/she has ultimate responsibility for managing the risks faced by the Assembly Commission and Secretariat. As Accounting Officer, he/she is required to sign the annual Governance Statement as part of the preparation of the Annual Report and Accounts. In order to fulfil this responsibility, he/she will ensure that risk management is promoted, embedded and operational within the Assembly Commission and the Assembly Secretariat.

Secretariat Audit and Risk Committee

4.2 SARC supports the Clerk/Chief Executive in his/her role as Accounting Officer and the Commission and SMG in monitoring their responsibilities for issues of risk, control and governance. Membership consists of two independent members, one of whom chairs SARC, and a member of the Commission.

4.3 Prior to the Clerk/Chief Executive signing the accounts, SARC reviews the adequacy of all risk and control-related disclosure statements, any accompanying Internal Audit statement, and the structures, processes and responsibilities for identifying and managing key risks facing the organisation. SARC reviews the Corporate Risk Register at its meetings and Stewardship Statements twice yearly.

Secretariat Management Group

4.4 SMG members are responsible for ensuring risk management is considered fully at SMG, and also for maintaining a culture of Risk Management within their area of responsibility. This includes:

- Ownership and approval of the Corporate Risk Register through quarterly review at SMG;
- Considering risks escalated from Directorate Risk Registers;
- Considering contents of all Directorate Risk Registers twice yearly at SMG;
- Determining what types of risks are acceptable and the level of risk that the Assembly Commission will carry in relation to specific major activities or projects across the organisation as a whole;
- Corporately agreeing risk appetite;
- Ensuring that line management and staff are aware of their risk and control responsibilities;
- Approving major decisions affecting the organisation's risk profile or exposure;
- Identifying risks and monitoring their management and control;
- Satisfying themselves that the less significant risks are being actively managed, with the appropriate controls in place and working effectively;

- Annually reviewing the Risk Management Strategy and approving changes or improvements to key elements of its processes and procedures;
- Ownership of Directorate Risk Registers for their area of responsibility through monthly review;
- Submission of Stewardship Statements to the Clerk/Chief Executive twice yearly;
- Alerting the Clerk/Chief Executive to any risks which arise within the reporting cycle; and
- Alerting the Clerk/Chief Executive of any 'near miss' incidents as they occur and reviewing and implementing controls to address weaknesses.

Director of Legal, Governance & Research Services

4.5 The Director of Legal, Governance & Research Services is responsible for maintaining and reviewing the Corporate Governance Framework, including the Risk Management Strategy. The Director supports the Clerk/Chief Executive in ensuring that risk management is promoted, embedded and operational within the Assembly Commission and the Assembly Secretariat.

Senior Information Risk Owner (SIRO)

4.6 In recognition of the need to protect corporate information and to manage it effectively, the Clerk/Chief Executive, as Accounting Officer, has appointed the Director of Legal, Governance & Research Services as SIRO. The SIRO has overall authority in relation to decisions about protective marking and ensuring information risks are assessed and mitigated to an acceptable level.

Information Standards Officer (ISO)

4.7 The ISO, in conjunction with Information Asset Owners, is required to review the type and use of information held in each directorate. An Information Governance Framework is in place, including strategies and policies relating to Information Management, Information Security and Information Technology. An Information Security Group is also in place.

Line management and staff

4.8 All line management and staff are expected to:

- Work to the Assembly's Risk Management Strategy;
- Alert management to emerging risks or control weaknesses;
- Participate fully in the regular risk review process; and
- Assume responsibility for risks and controls within their own areas of work.

Internal Audit

4.9 Internal Audit will take the Assembly Commission's corporate risks into account and plan an audit strategy based on a risk-based approach.

4.10 Although Risk Management and internal control are the responsibility of management throughout the Secretariat, Internal Audit clearly has an interest in supporting the maintenance of effective internal control. Internal Audit's primary objective is to provide an independent opinion on the effectiveness of the risk management, internal control and governance framework to the Clerk/Chief Executive in his/her role as Accounting Officer, and to SARC. It

does this by carrying out audits across the Directorates, focusing on the key risks in each business area.

4.11 Internal Audit also has a role to play in:

- Acting as an independent advisor by providing advice on the management of risk, especially those issues surrounding the design, implementation and operation of systems of internal control;
- Monitoring, reporting and providing opinion on the effectiveness of the risk and control mechanisms in operation; and
- Promoting Risk Management and control concepts across the Assembly Commission.

Partner Bodies

4.12 The Assembly Commission has relations with five "partner bodies", namely:

- The Northern Ireland Assembly and Business Trust;
- Politics Plus;
- The Northern Ireland Assembly Members' Pension Scheme Trustees;
- The Northern Ireland Assembly Commissioner for Standards; and
- The Independent Financial Review Panel (IFRP).

4.13 All are separate entities with their own governance arrangements. The purpose of each, and the current governance of each relationship with the Assembly Commission, is summarised below:

Name	**Purpose**	**Governance of Relationship**
Northern Ireland Assembly and Business Trust	Northern Ireland Act 1998 s.40(4): "provide the Assembly, or ensure that the Assembly is provided, with the property, staff and services required for the Assembly's purposes."	MOU
Politics Plus	Northern Ireland Act 1998 s.40: provide Assembly with what it requires	MOU
Northern Ireland Assembly Members' Pension Scheme Trustees	Northern Ireland Act 1998 s.48: deliver pensions of members as determined by IFRP	Administration Agreement
Northern Ireland Assembly Commissioner for Standards	Assembly Members' (Independent Financial Review and Standards) Act (Northern Ireland) 2011 Part 2: self-regulation of conduct	Statute, and statutory directions issued
IFRP	Assembly Members' (Independent Financial Review and Standards) Act (Northern Ireland) 2011 Part 1, NI Act 1998 s.47 and 48: determine pay/ pension etc. of members	Statute, and Service Level Agreement

5 Annual Risk Management Timetable

5.1 The annual risk management timetable is as follows:

Corporate Risk Register reviewed quarterly at SMG

Directorate Risk Registers reviewed monthly by Directors

*SARC meeting – late January / early February

Interim Accounts submitted to NIAO – mid February

NIAO audit process begins – mid February

Interim Report to those Charged with Governance – mid March

Internal Audit Annual Activity Report – end March

Stewardship Statements (see Annex B) – completed end March

Directorate Risk Registers reviewed by SMG – March

Review of Risk Management Strategy – April

*SARC meeting – mid May

Directorate Risk Registers reviewed by SARC – May

Draft Annual Accounts (including Governance Statement) – mid May

SARC self-assessment – May

*SARC meeting – mid June

Assembly Accounts signed and laid – before Summer recess

Certificate from Comptroller and Auditor General – late June

Report to those Charged with Governance – mid July

Directorate Risk Registers reviewed by SMG – September

Stewardship Statements – completed end September

Annual Risk Management self-assessment – end September

*SARC meeting – early October

Annual review of SARC terms of reference – October

**includes review of any outstanding audit actions*

6 Further Reading and Assistance

6.1 The Governance Officer, and the Head of Internal Audit are available to assist in the application of this guidance. You may also like to see:

- NIAO's Good Practice in Risk Management 2011
- HMT's Orange Book - Management of Risk – Principles and Concepts 2004
- Management of Risk in Government – January 2017
- Guidance on the use of PRINCE2 project management methodology in the Northern Ireland Assembly.

6.2 To receive this document in alternative formats contact Governance Officer on ex 21242.

7 Annual Review

7.1 This strategy will be reviewed annually by SMG. Any changes will be brought to the attention of SARC.

Annexes

Annex A: HM Treasury's Risk Appetite Framework

Annex B: Stewardship Statement Template

Annex C: Risk Register Template

Annex D: NI Assembly Secretariat Risk Management Flowchart

ANNEX A

HM Treasury's Risk Appetite Framework

	1 **Averse**	2 **Minimalist**	3 **Cautious**	4 **Open**	5 **Hungry**
	Avoidance of risk and uncertainty is a key Organisational objective	**Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward.**	**Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.**	**Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc.).**	**Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk).**
Category of Risk	**Example behaviours when taking key decisions…**				
Reputation and credibility	• Minimal tolerance for any decisions that could lead to scrutiny of the Government or the Department.	• Tolerance for risk taking limited to those events where there is no chance of any significant repercussion for the Government or the Department.	• Tolerance for risk taking limited to those events where there is little chance of any significant repercussion for the Government or the Department should there be a failure.	• Appetite to take decisions with potential to expose the Government or Department to additional scrutiny but only where appropriate steps have been taken to minimise any exposure.	• Appetite to take decisions that are likely to bring scrutiny of the Government or Department but where potential benefits outweigh the risks.
Operational and policy delivery	• Defensive approach to objectives – aim to maintain or protect, rather than to create or innovate. • Priority for tight management controls and oversight with limited devolved decision making authority. • General avoidance of systems / technology developments.	• Innovations always avoided unless essential. • Decision making authority held by senior management. • Only essential systems / technology developments to protect current operations.	• Tendency to stick to the status quo, innovations generally avoided unless necessary. • Decision making authority generally held by senior management. • Systems / technology developments limited to improvements to protection of current operations.	• Innovation supported, with demonstration of commensurate improvements in management control. • Systems / technology developments considered to enable operational delivery. • Responsibility for non-critical decisions may be devolved.	• Innovation pursued – desire to 'break the mould' and challenge current working practices. • New technologies viewed as a key enabler of operational delivery. • High levels of devolved authority – management by trust rather than tight control.
Financial/VFM	• Avoidance of financial loss is a key objective. • Only willing to accept the low cost option. • Resources withdrawn from non-essential activities.	• Only prepared to accept the possibility of very limited financial loss if essential. • VfM is the primary concern.	• Prepared to accept the possibility of some limited financial loss. • VfM still the primary concern but willing to also consider the benefits. • Resources generally restricted to core operational targets.	• Prepared to invest for reward and minimise the possibility of financial loss by managing the risks to a tolerable level. • Value and benefits considered (not just cheapest price). • Resources allocated in order to capitalise on potential opportunities.	• Prepared to invest for the best possible reward and accept the possibility of financial loss (although controls may be in place). • Resources allocated without firm guarantee of return – 'investment capital' type approach.
Compliance – legal / regulatory	• Avoid anything which could be challenged, even unsuccessfully • Play safe.	• Want to be very sure we would win any challenge.	• Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	• Challenge will be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	• Chances or losing are high and consequences serious. But a win would be seen as a great coup.

ANNEX B

STEWARDSHIP STATEMENT FORMAT (SAMPLE)
ASSEMBLY SECRETARIAT

STEWARDSHIP STATEMENT

RISK OWNER:

DIRECTORATE:

REPORTING PERIOD:

1. ACKNOWLEDGEMENT OF OWNERSHIP OF RISK

I acknowledge my responsibility for managing the risks allocated to me as detailed in

the Corporate Risk Register dated:	
the Directorate Risk Register dated:	

(Note checklist at Annex A).

2. RISK MANAGEMENT STATUS

(Please tick the box that applies)

Controls appropriate		**Controls not appropriate**	
I am satisfied that the controls listed in the Registers referred to above are appropriate. They provide reasonable assurance that the risk will not occur or if it does occur, it will be detected and corrected in sufficient time to reduce the impact of the risk to tolerable or negligible levels.		I am not satisfied that the measures/controls in place to manage the risks for which I am responsible are appropriate. Remedial action as detailed below is being taken in order to safeguard the Assembly from the impact of the risk materialising.	
Detail the broad basis for this assurance *i.e. how does the reporting officer know that controls are effective and operating as intended?*		***Detail the remedial action or*** *the factors that prevent adequate management of the risk.*	

3. DELEGATED RESPONSIBILITIES

As detailed in the delegation letter of functions and financial responsibilities of 16 December 2015, I confirm that all expenditure:

- has been incurred within agreed budgets and pursuant to monthly review with Heads of Business / staff with budget responsibilities;
- has been properly authorised;
- complies with the Assembly's procurement procedures regarding Directorate responsibilities; and
- represents value for money.

Outline the measures taken and detail any exceptions below

4. INFORMATION MANAGEMENT

I have confirmed that the manner in which information is generated, transmitted and stored is appropriate for the content involved and does not pose a risk to the business or reputation of the Assembly.

Outline the measures taken and detail any exceptions below

5. FRAUD / BRIBERY

I am satisfied that the controls in place to manage the risks of fraud and bribery (including those arising from responsibilities under the Bribery Act 2010) are appropriate.

Outline the measures taken and detail any exceptions below

6. INTERNAL / EXTERNAL AUDIT ACTION POINTS

I have verified that all accepted recommendations made by Internal Audit and the Northern Ireland Audit Office have been or are being implemented as agreed, including agreed implementation dates.

Outline the measures taken and detail any exceptions below

7. Significant Changes to Risk/ Risk Management or other ADDITIONAL INFORMATION

Detail any significant changes to the allocated Corporate risk(s) or Directorate risks (e.g. in respect of impact or likelihood) or to the manner in which risk is managed.

Please highlight any additional material issues which may be of interest to the Accounting Officer and the Secretariat Audit and Risk Committee.

Business Area Input
I have confirmed with the relevant Heads of Business that there are no additional factors which may impact on risk or the manner in which it is currently managed.

Signed: **Name:**

Grade: **AG2** **Date:**

ANNEX A

RISK MANAGEMENT CHECKLIST

All roles, responsibilities and levels of accountability in respect of allocated Corporate risk(s) and Directorate risks are communicated and understood.
Policies relevant to the management of allocated Corporate risk(s) and Directorate risks are in place along with corresponding guidance, instructions etc.
Sufficient resources have been identified and the efficiency and effectiveness of their use monitored.
The management of allocated Corporate risk(s) and Directorate risks has been included in the business planning process.
The controls used to manage allocated Corporate risk(s) and Directorate risks are regularly reviewed to ensure they remain appropriate to the associated likelihood and impact.
All relevant action points in relation to Internal and External Audit reports are up to date.
Effective communications are in place to ensure that incidents relating to allocated Corporate risk(s) and Directorate risks are brought to the attention of the Accounting Officer, SMG and SARC as necessary.

ANNEX C

Standard Risk Register Template

NORTHERN IRELAND ASSEMBLY SECRETARIAT

CORPORATE / DIRECTORATE RISK REGISTER

Date

INTRODUCTION

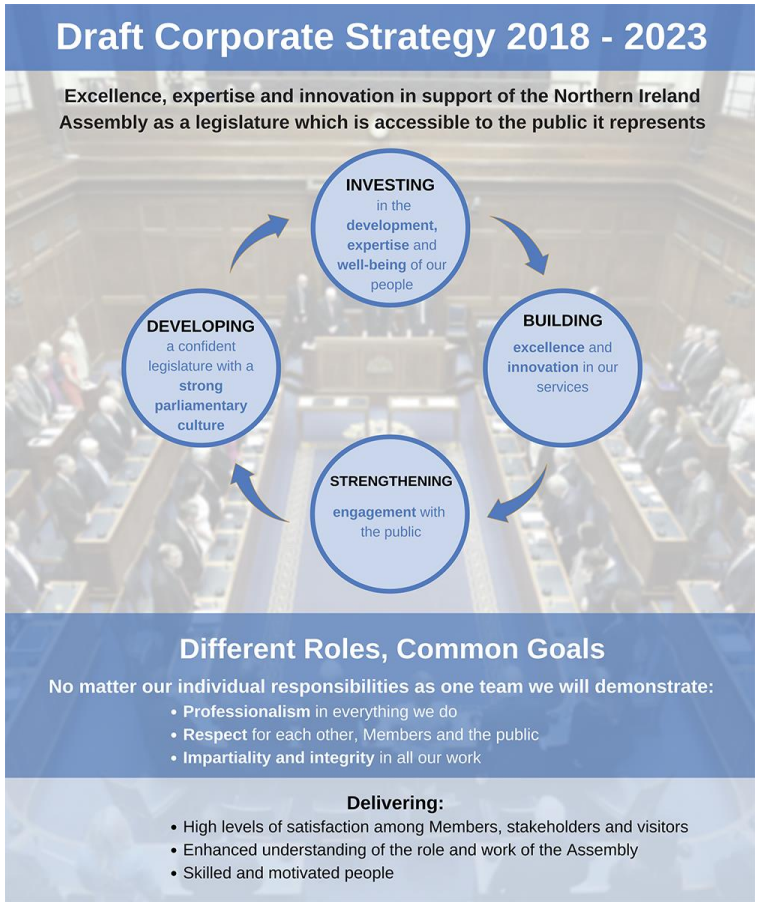
Risk is any event or uncertainty that may enhance or impede our ability to achieve current or future aims.

The Risk Management Strategy forms a central part of our internal control and corporate governance arrangements. It defines our approach to Risk Management throughout the Secretariat. It also ensures a consistent approach to dealing with risks which may have an impact on our ability to achieve the Commission's vision, strategic goals and aims.

The Risk Management Process Guidance incorporates five phases, the last of which is reviewing and reporting risk. This Risk Register reports on risk within the Directorate and allows risk to be kept under regular review.

Northern Ireland Assembly Commission Draft Corporate Strategy 2018 – 2023

This draft corporate strategy was presented to the Commission on 5th July 2018.It was agreed that formal Assembly Commission approval for the draft strategy will not be sought until the Assembly resumes normal business and a new Assembly Commission is appointed and that the five year period of operation will not commence until formal approval is obtained .It was, however, agreed that the Secretariat should produce a 2018-2019 Corporate Plan reflecting the key elements of the draft corporate strategy. A full version of the draft strategy can be accessed here.



Explanatory Notes

Section A provides the risk title and a score for the risk based on 3 criteria, each is defined below.

Inherent Risk is that risk which exists before any management controls are applied. This enables decisions to be made about resources and the level of priority given to managing a risk.

Residual Risk is determined as the level of risk that remains after existing controls (section B) have been actioned. The residual risk gives an indication of how effectively a risk is being managed by existing controls.

Target Level of Risk is the level of risk that management has set as its target level of risk.

Management Comments provides an assessment of whether management consider that the additional controls to be actioned (section C) will be sufficient to bring the level of residual risk down to the target Level of Risk.

Corporate Alignment shows which Corporate Strategy goals the risk could impact upon and conversely which risks are relevant when considering strategic goals during strategic and business planning.

Risk Scoring is based on impact and likelihood as indicated in section A of each risk and summarised in the Risk Assessment Matrix below.

Impact	**Critical**	**5**	G	Y	A	R	R
	Major	**4**	G	Y	A	A	R
	Significant	**3**	G	Y	Y	A	A
	Moderate	**2**	G	G	Y	Y	Y
	Minor	**1**	G	G	G	G	Y
			Remote (<10%)	**Unlikely (11-30%)**	**Possible (31-59%)**	**Probable (60-84%)**	**Almost Certain (>85%)**
			1	**2**	**3**	**4**	**5**
	Probability						

Section B provides a summary of controls already in place to manage the risk.

Section C provides a summary of additional controls that will be put in place to manage the risk.

Summary of Corporate Risks

Ref	Overarching Risk Description
CR1	Insufficient budget approved by the Assembly to enable delivery of the Assembly Commission's Corporate Strategy 2018-23
CR2	Major Incident / Breakdown (including security incident)
CR3	Errors or omissions in equality, governance or regulatory requirements
CR4	Loss of staff, skills and knowledge and / or staff engagement
CR5	Obligations arising from the United Kingdom leaving the EU are placed on the Assembly

Directorate Risk Summary

Ref	Overarching Risk Description	Inherent Impact	Inherent Likelihood	Inherent Risk Score	Residual Impact	Residual Likelihood	Residual Risk Score	Total Target Risk Score	Alignment with Corporate Aims	Movement
DR1	Eg	5	4	R 20	4	4	A 16	Y 6	Building	
DR2										
DR3										
DR4										
DR5										
DR6										

A DR1 - Title	**Risk appetite:**	**Risk owner:**

Corporate Alignment Corporate Aims: e.g. Building	**Score Key (Likelihood x Impact = Total Score)** **Impact:** 1. Minor 2. Moderate 3. Significant 4. Major 5. Critical **Likelihood of Occurrence**: 1. Remote (<10%) 2. Unlikely (11-30%) 3. Possible (31-59%) 4. Probable (60-84%) 5. Almost Certain (85%+)

Management Commentary: Implementation of the additional actions to be taken to manage the risk is sufficient to reduce the level of residual risk onto or below the target level of risk.	**Inherent Risk Scoring**			**Residual Risk Scoring**			**Target Risk Scoring**		
	Impact	**Likelihood**	**Total Score**	**Impact**	**Likelihood**	**Total Score**	**Impact**	**Likelihood**	**Total Score**
	Eg **5**	**4**	R **20**	**4**	**4**	A **16**			Y **6**

Root causes		**B Risk response**	**Who performs it?**	**How often?**	**How evidenced?**

C Additional actions to manage the risk	**Implementation date**	**Who will perform it?**	**How often?**	**How evidenced?**	**Position at**

Annex D

NI Assembly Secretariat Risk Management Flowchart