North Devon Council

Risk Management Model

northdevon COUNCIL

June 2023

Organisation	North Devon Council
Title	Risk Management Model
Creator	Nina Lake / Adam Tape
Approvals	Governance Committee
Distribution	Internal Document. Insite.
Filename	I:\Audit and Risk\Risk Management Framework
Owner	Corporate Risk Group (CORGI)
Review date	June 24

Document Amendment History

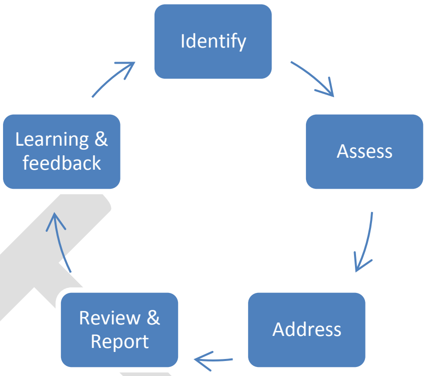
Version No.	Originator of change	Date of change	Change Description
5.0	CORGI	March 2022	General update. Escalation process for Service & Project risks.

Contents

Risk Management guidance relating to identifying risks, describing risks, risk assessment model risk ownership, addressing risks, reviewing and reporting risks, communication and learning.

Appendices: The Assurance Model, Glossary of terms.

Risk Management Guidance



Identifying risks

Definition: *Risk **identification** sets out to identify an organisation's exposure to uncertainty.*

It is the starting point in the risk management process. At this point you should **not** be trying to measure risks, but instead trying to identify the most important risks we face now or in the future that might stop us achieving objectives.

Risk **identification** can only take place once the objectives of the organisational activity under examination are SMART and clearly understood. As objectives change, so should the previously identified risks and opportunities be reviewed and updated.

A common problem at this early stage is the **identification** of too many risks. A large list of risks is unwieldy and daunting and will inevitably result in risks being poorly assessed and will lead to gradual disillusionment with the process. The key is to focus on significant risks. Many of the smaller risks will already be adequately managed through existing internal controls, processes and procedures, and may not need to be shown on the risk register.

Common types of risk facing NDC

External: not wholly within the Council's control

Political	Change of government or cross cutting policy decision
Economic	Global economic conditions
Socio-cultural	Demographic change
Technological	Systems obsolescence; procurement costs
Legal	Change to legislation / directives
Environmental	Change in environmental attitude from gov media & consumers

Operational: related to current operations – delivery, capacity and capability

Delivery

Service / product failure	Failure to deliver within agreed terms
Project delivery	Failure to deliver time / budget

Capability & Capacity

Resources	Poor £ management, insufficient HR capacity / skills, loss of assets
Relationships	Lack of clarification of partner roles, poor customer satisfaction levels
Operations	Overall capacity to deliver
Reputation	Lack of confidence or trust

Risk Management Performance & Capability

Governance	Compliance with requirements
Scanning	Failure to identify threats / opportunities
Resilience	IT system capacity to withstand attack
Security	Information or physical assets

Change: Created by decisions to pursue objectives beyond current capability

Gov.Targets Change	New and challenging targets / measures
Programmes	Programmes that threaten capacity to deliver
New Projects	Investment decisions, project prioritisation
New Policies	Expectations create uncertainty about delivery

Please see *risk identification techniques* guidance materials

Describing risks

Definition: *The purpose of* ***describing*** *a risk is to present the identified risks in a structured format to ensure that any audience will understand it.*

We want all risks to use a **description** that identifies the Cause of the risk and the Consequence(s).

Using the ‘Cause- Risk-Consequence’ principle, here is a simple example of describing a risk based on a flat tyre.

Objective: To arrive at work on time each working day

Cause: A sharp object on the road

Risk: A car tyre coming into contact with that object

Consequence: A puncture. Arriving late to work

By **describing** a risk in this way it is simpler to see if prevention can be achieved by eliminating the cause or often breaking the cause to risk connection, while control relies on breaking, or reducing, the event to consequence link.

Assessing risks

This Risk Assessment Model gives you criteria by which you should assess your risks.

Risk assessment model	
Impact	**Likelihood**
Score of 4 – Catastrophic	**Score of 4 – Almost certain**
Service disruption ○ continuity of element of service compromised ○ significant impact on corporate objectives Financial loss ○ more than £500,000. ○ dire financial impact such that a rethink of how and whether to provide service is needed Reputation ○ likely to be significant local or some national media interest ○ resignation of leading member or chief officer ○ remembered for years Legal obligation ○ failure to provide statutory services or meet legal obligations ○ central Government intervention ○ multiple civil or criminal suits or litigation People ○ fatality of one or more people ○ mass staff leaving; unable to attract staff	○ Expected to occur in most circumstances, or ○ More than 90% likely to occur in the next 12 months

Risk assessment model	
Impact	**Likelihood**
Score of 3 - Major/Grave Service disruption ○ serious impact on quality or quantity of service provision Financial loss ○ significant financial consequence, which cannot be absorbed within budget o between £50,000 and £500,000 Reputation ○ national publicity or press interest Legal obligation ○ failure to meet regulatory standards with strong regulatory sanctions ○ significant litigation People ○ serious injury to, or permanent disablement of one or more people	**Score of 3 – Probable** ○ Will probably occur in some circumstances at some time, or ○ 50% chance of occurring in the next 12 months
Score of 2 – Moderate Service disruption o noticeable effect on service provision ○ failure to meet locally determined standards of service Financial loss ○ material financial consequence, but scope to absorb within budget ○ less than £50,000 (i.e. can be contained within the corporate budget including the contingency reserve).	**Score of 2 – Possible but unlikely** o Unlikely to occur but could at some time

Reputation ○ adverse local publicity Legal obligation ○ litigation, claims suits possible People ○ major injury to an individual	
Risk assessment model	
Impact	**Likelihood**
Score of 1 – Minor/insignificant Service disruption ○ Some minor impact on a service ○ negligible effect on service provision Financial loss ○ within the delegated power to vire funds within existing budget. Reputation ○ Little local publicity or media interest Legal obligation ○ only very minor litigation possible People ○ minor injuries to people, or illness, or damage to equipment	**Score of 1 – Highly unlikely** o Will only occur in exceptional or rare circumstances

Risk ownership

All risks, once identified and assessed, should be assigned to an ‘owner’ who has responsibility for ensuring that the risk is monitored and managed over time.

A risk owner should have sufficient authority to ensure that appropriate action can be taken, although the risk owner might not be the person who actually takes the action to address the risk.

The actual monitoring of risks can be carried out by anyone but the results of this monitoring must be fed back to the risk owner, who will take any action as appropriate, or if necessary take it to someone that can.

Addressing risks

Definition: *The purpose of* ***addressing*** *risks is to turn uncertainty to the organisation’s benefit by reducing threats and taking advantage of opportunities.*

The appropriate response to each risk will depend on its nature and the outcome of the risk assessment. The degree of attention required should be proportionate to the level of risk and cost and benefits involved in any action taken to reduce the risk. Also in deciding how to address a risk, attention should be paid to whether it is the likelihood or impact of a risk that needs most attention.

For risks above the tolerance level, then a response must be planned to reduce the risk exposure to an acceptable level or to identify suitable contingency plans in case the risk occurs. Another option is to cease the risky activity.

Aspects to consider when deciding whether to address a risk could be:

- value of assets lost or wasted in the event of adverse impact
- stakeholder perception of an impact
- the balance of the cost of control and the extent of exposure
- the balance of potential benefit to be gained or losses to be withstood.

Identifying the possible mitigation responses to a risk is best considered jointly by management and the individual risk owners and possibly those involved in processes which create the risk.

Mitigation actions needs to be drawn to reduce the risk identifying

- what can be done,
- by whom, and
- by when, or
- a contingency plan.

Actions need to be assigned to an individual to ensure they are carried out on time. The actions need to be built into Service Plans or Project Plans as appropriate.

There are four approaches we can consider when determining how to **address** a risk:

Tolerate

- The exposure to risk may be tolerable without any further action being taken.
- The cost of taking action may be disproportionate to the potential benefit gained.
- This tolerance may also be supplemented by contingency planning.

Treat

- The majority of risks will be addressed in this way, with mitigating action taken to control the risk to an acceptable level.

Transfer

- For some risks the best response may be to transfer them.
- This may be done by conventional insurance or paying a third party to take the risk in another way.
- This option is particularly good for mitigating financial risks or risks to assets.
- Transference will be used to reduce the exposure to risk for NDC or there may be another organisation more capable of effectively managing the risk.

NB: Some risks are not fully transferable e.g. a risk to our reputation.

Terminate

- Some risks will only be treatable, or controlled within acceptable levels by terminating the activity.

This option can be particularly important in project management if it becomes clear that the projected cost / benefit is in jeopardy.

Reviewing and reporting

Definition*: The management of risks has to be reviewed and reported for two reasons.*

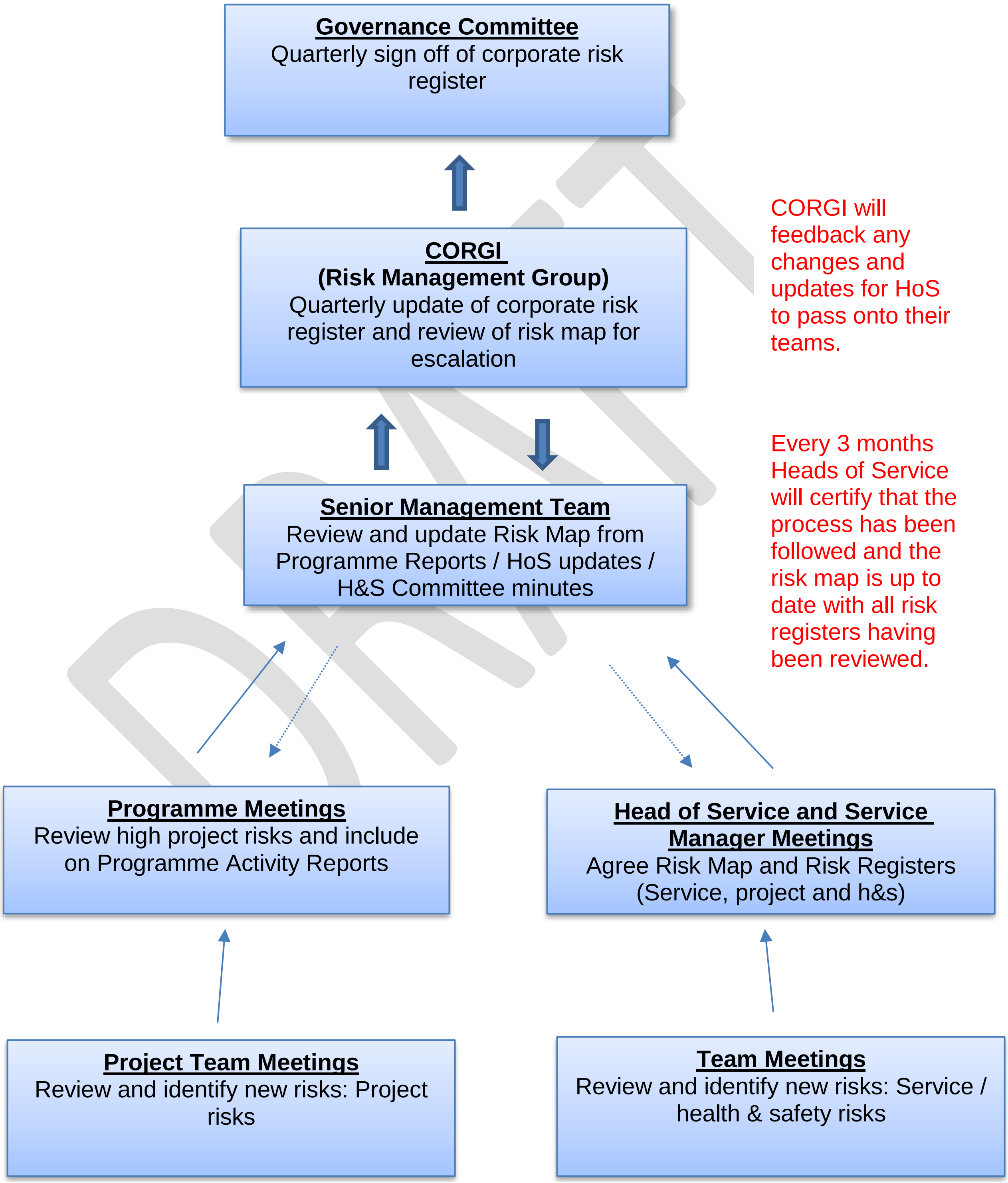
- *to monitor whether or not the risk profile is changing; and*
- *to gain assurance that risk management is effective and to identify when further action is necessary.*

Regular discussion about risks should take place between Heads of Service and managers, and between managers and staff to ensure that risk management becomes a routine activity in the same way as performance management.

Who reports to who?

The Corporate Risk Register will be reviewed quarterly by the CORGI (Corporate Risk) Group reporting onwards to the Governance Committee.

The NDC Risk Map, showing service and programme risks, will be reviewed quarterly by the Senior Management Team, where Heads of Service will be asked to certify that the risks are up-to-date having been reviewed and discussed at team/project meetings, as per the escalation process below. Urgent risks will be escalated to the Chief Executive.



Governance Committee
Quarterly sign off of corporate risk register

CORGI
(Risk Management Group)
Quarterly update of corporate risk register and review of risk map for escalation

Senior Management Team
Review and update Risk Map from Programme Reports / HoS updates / H&S Committee minutes

Programme Meetings
Review high project risks and include on Programme Activity Reports

Head of Service and Service Manager Meetings
Agree Risk Map and Risk Registers (Service, project and h&s)

Project Team Meetings
Review and identify new risks: Project risks

Team Meetings
Review and identify new risks: Service / health & safety risks

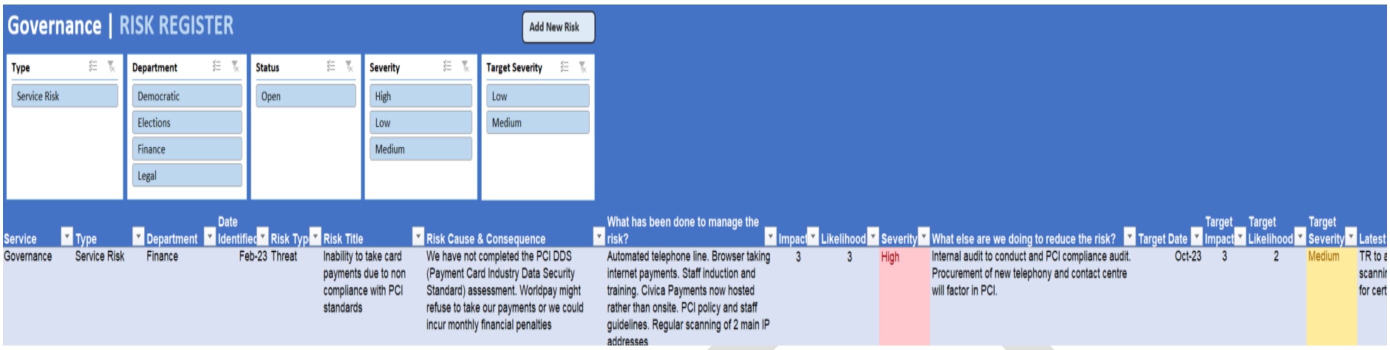
CORGI will feedback any changes and updates for HoS to pass onto their teams.

Every 3 months Heads of Service will certify that the process has been followed and the risk map is up to date with all risk registers having been reviewed.

The principle of the risk escalation process is that a member of staff at a team meeting or project team meeting can identify a risk that, if appropriate, can be quickly escalated to the corporate risk register and reported to the Governance Committee.

Project/Programme Risk Logs will remain open for the lifecycle of the project and be maintained by the Project Manager, with high-risks being identified in a Highlight Report and reviewed by the Programme Meetings and Senior Management Team.

When **reporting** risks, service or programmes, we use the following standard excel spreadsheet to create the risk logs which then feeds into the risk map summary:



Governance | RISK REGISTER

Type: Service Risk

Department: Democratic, Elections, Finance, Legal

Status: Open

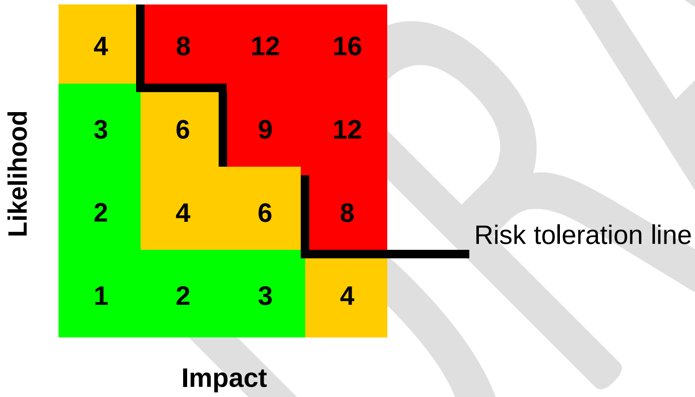
Severity: High, Low, Medium

Target Severity: Low, Medium

Service	Type	Department	Date Identified	Risk Type	Risk Title	Risk Cause & Consequence	What has been done to manage the risk?	Impact	Likelihood	Severity	What else are we doing to reduce the risk?	Target Date	Target Impact	Target Likelihood	Target Severity	Latest
Governance	Service Risk	Finance	Feb-23	Threat	Inability to take card payments due to non compliance with PCI standards	We have not completed the PCI DDS (Payment Card Industry Data Security Standard) assessment. Worldpay might refuse to take our payments or we could incur monthly financial penalties	Automated telephone line. Browser taking internet payments. Staff induction and training. Civica Payments now hosted rather than onsite. PCI policy and staff guidelines. Regular scanning of 2 main IP addresses	3	3	High	Internal audit to conduct and PCI compliance audit. Procurement of new telephony and contact centre will factor in PCI.	Oct-23	3	2	Medium	TR to a scannir for cert

The risk matrix below is a simpler mechanism to increase visibility of risks and assist management in decision-making. It is a graphical representation of information of a risks status.

Risk Matrix



Likelihood				
4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	3	4
	1	2	3	4

The regularity of the review of a risk will depend upon the level of current risk exposure (Impact x Likelihood). The higher the risk exposure the more regularly it needs to be reviewed.

Where other risk registers exist i.e. registers required for funding bid applications, then these should be shared with the Head of Governance / CORGI group so that a corporate overview is maintained of all risks.

Communicating and learning

Definition: *Communication and learning is not a distinct stage in the management of risk; rather it is something, which runs through the whole process.*

The identification of new risks or changes in risk is itself dependent on **communication** between staff at all levels in the Council, it's contractors and partners.

It is intended that all staff be included in the process for identifying, reviewing and escalating risks to their managers. This will be through team meetings and the appraisal process.

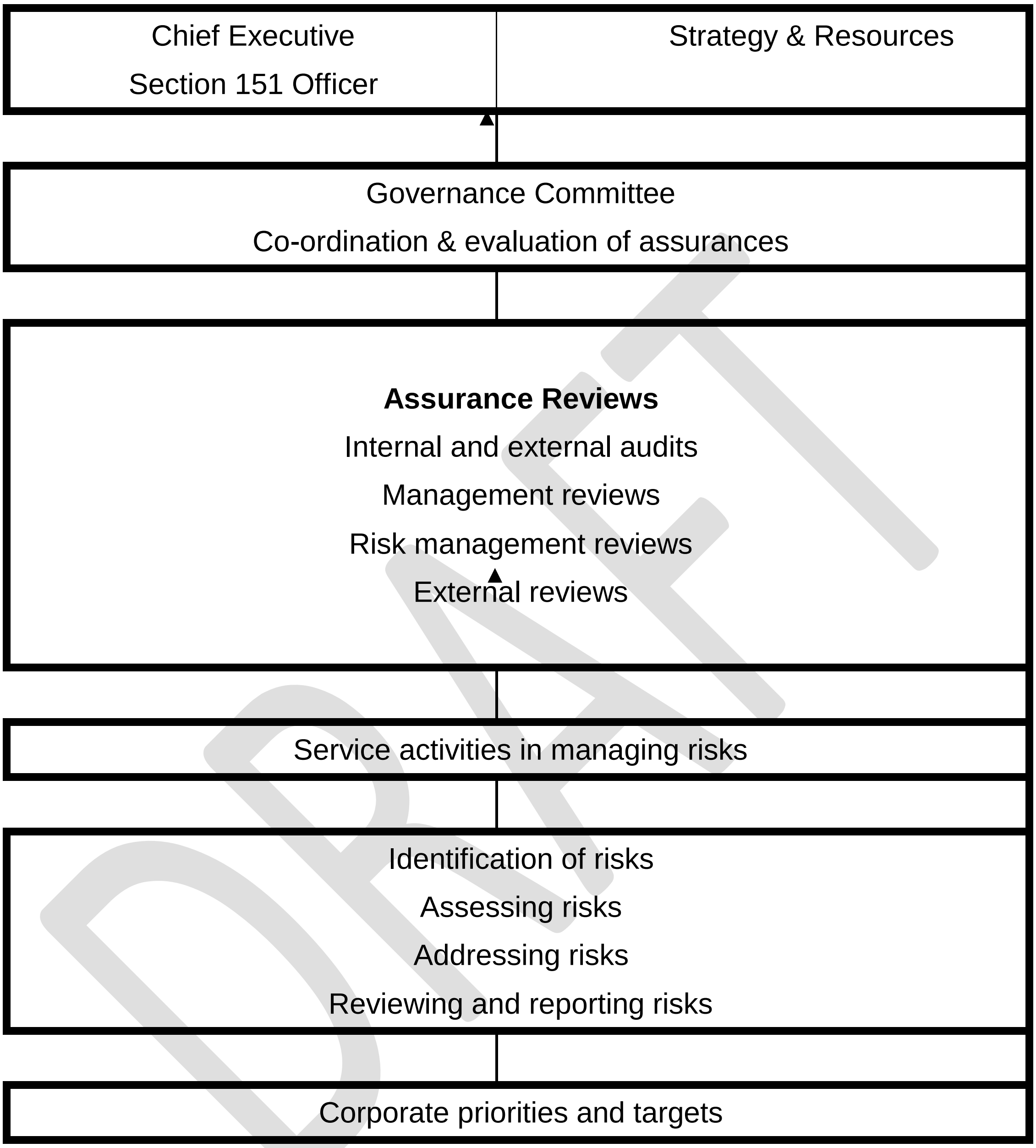
Internally, it is important that all staff understand, in a way that is appropriate and relevant to their role, what the risk framework is and their role in managing risks and keeping their service risk register up to date.

Communication will be achieved through:

- The Governance Committee, CORGI and Senior Management Team reviewing the risk management framework and signing up to its principles and processes.
- The Senior Management Team will ensure that Heads of Service are managing and monitoring risks effectively.
- The Chief Executive will gain regular assurance from Heads of Service that risks within their area of responsibility are being managed effectively, also new risks will be discussed.
- Heads of Service will be briefed on the process for identifying, reviewing and escalating risks. Risks will be discussed on an ongoing basis.
- Staff will assess risks in their operation activities and will identify and escalate risks to their managers.
- This framework will be published on Insite and communicated to all middle managers and staff when this document has been refreshed.
- Regular horizon scanning at Senior and Middle Management level

Learning will be assisted through the re-launch of this framework, manager and member training.

Appendix 1 - The assurance model



Appendix 2 - Glossary of terms

- **Assurance**: an evaluated opinion, based on evidence gained from review, on the organisation's governance, risk management and internal control framework.

- **Consequence**: the outcome of an event

- **Current Risk**: the exposure arising from a specific risk after action has been taken to manage it

- **Event**: the occurrence of a particular set of circumstances

- **Exposure**: the consequences, as a combination of impact and likelihood which may be experienced by the organisation is a specific risk is realised.

- **Impact**: the probably effect on the Council if the risk occurs.

- **Inherent Risk**: the exposure arising from a specific risk before any action has been taken to manage it.

- **Internal Control**: actions implemented to manage the risk to its current status

- **Likelihood**: the probability or chance of the risk occurring.

- **Mitigation**: the process of selection and implementation of future actions to reduce the risk

- **Risk**: uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of impact and likelihood.

- **Risk Appetite**: the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.

- **Risk Assessment**: The overall process of Risk Estimation and Risk Evaluation

- **Risk Description**: To display the identified risks in a structured format by using a table.

- **Risk Estimation**: the process used to assign values to the impact and likelihood of a risk.

- **Risk Evaluation**: the process of comparing the estimated risk against the Risk Response Matrix

- **Risk Identification**: the process to find, list and characterise elements of risk

- **Risk Management**: all the processes involved identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing the process.

- **Risk Profile**: the result of the risk assessment process can be used to produce a risk profile that gives a significance rating to each risk and provides a tool for prioritising risk treatment efforts. This ranks each identified risk so as to give a view of the relative importance.

- **Risk Register**: the documented and prioritised overall assessment of the range of specific risks faces by the Council.

- **Target Risk**: the desired level of risk following additional mitigating actions.