access
freedom to do more

Risk Assessment Process & Methodology

Tier 2

Document Control Reference: ISMS 4.4
Issue No 2.8
Issue Date: 01.03.2024

The Armstrong Building
10 Oakwood Drive
Loughborough
LE11 3QF

T 01206 322 575
T 0845 345 3300
F 01206 322 956
E info@theaccessgroup.com

Scope

This method of risk assessment is applied throughout the Access Group in respect of all Information Security risks. This includes, but is not limited to: physical assets, human resources, intellectual property, our reputation, datacentre services, suppliers, staff, technology, buildings, processes, procedures, and services.

Responsibilities

Risk accountability: The Access Board and Divisional Management Teams (DMT) are legally accountable for cyber risk management. They must ensure that the appropriate strategies, risk management policies, resources and budget are in place to effectively manage risk.

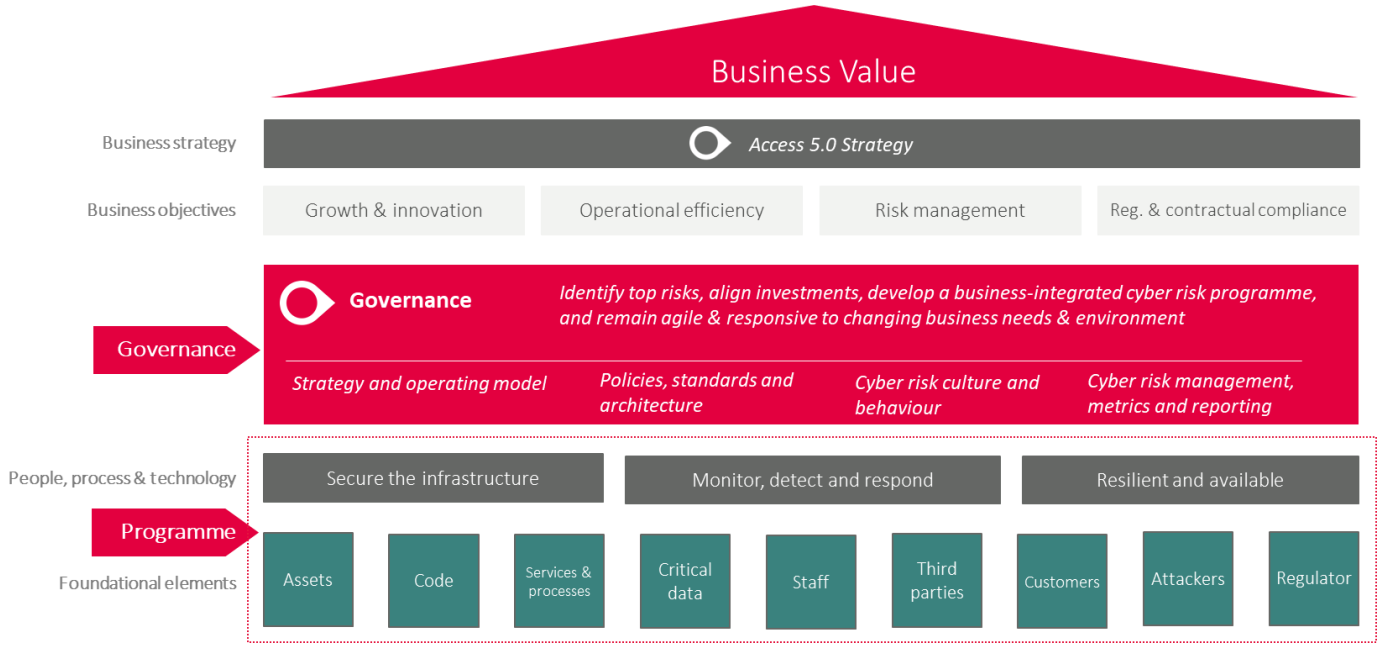
Risk Owner: This is the individual or team who has operational responsibility for ensuring an individual risk is recorded, managed and reported on appropriately. Their responsibility will have been delegated as part of their role by the Board or DMT.

Risk Decision Makers: This is some on at Board or the DMT level who will make the decision on what Access will do about a risk; tolerate, terminate, transfer or treat as ultimately these are business decisions.

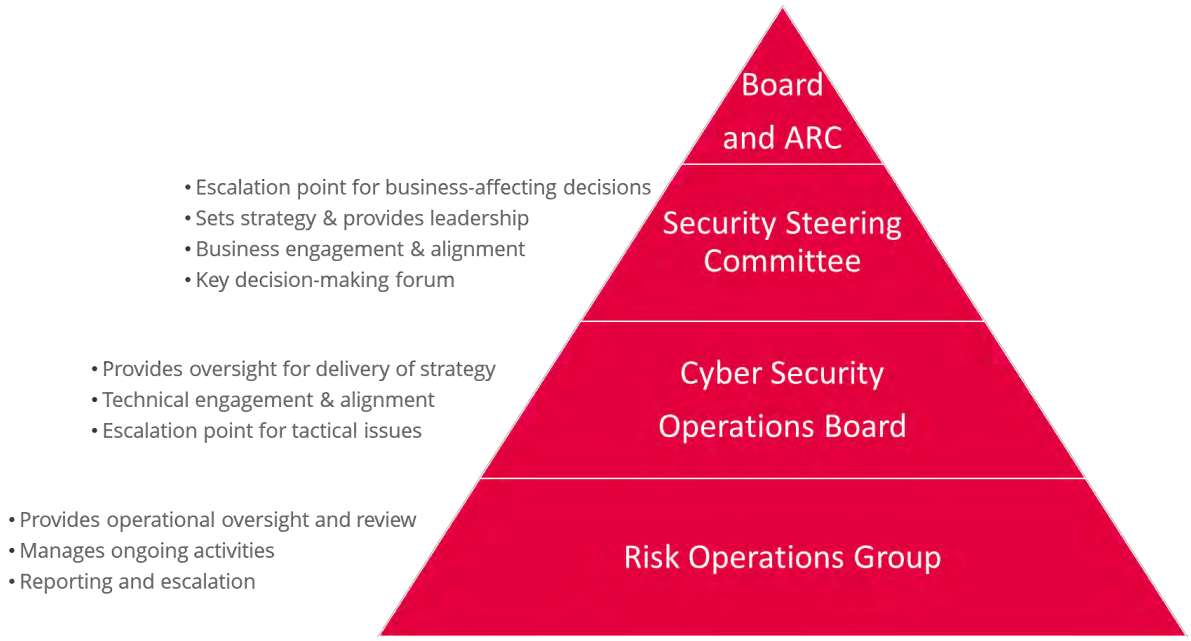
Risk Oversight: The Risk Operations Group overseen by the Information Security Manager is responsible for ensuring that effective risk assessments have been carried out wherever they are required by the ISMS.

Governance

Recognising that good risk management goes together with good corporate governance. At Access our risk management is designed to contribute towards the overall strategic aims of the business. It's important to understand that the Information Security team does not actually manage risks. The role of the Information Security team is to help facilitate a process for identifying, assessing, and analysing risks, to provide a uniform method of recording risks across the business and to ensure that Board and Divisional Management Teams have the information they need to make risk-informed decisions.



The Risk Operations Group will evaluate the cyber security risks, assist the Divisions in reviewing their registers and provide information on the performance of our risk management. This is done in the context of the cyber security governance framework.



Assessing Risk

A cyber security risk assessment is the process of identifying, analysing, and evaluating risk. It helps to ensure that the cyber security controls we choose are appropriate to the risks Access faces.

Without a risk assessment to inform our cyber security choices, we could waste time, effort, and resources. There is little point implementing measures to defend against events that are unlikely to occur or won't impact Access.

Likewise, we might underestimate or overlook risks that could cause significant damage. This is why so many best-practice frameworks, standards and laws – including the ISO27001 and Data Protection Legislation – require risk assessments to be conducted.

A risk assessment consists of three parts:

- risk identification.
- risk analysis.
- risk evaluation.

Identify your risks

Risk Identification – This is all about recognising what could go wrong and potential risks that exist within our business environment. The best way to do this is via a Business Impact Analysis (BIA)

A BIA exercise is to understand the perception of the risks from all parts of the business. Answering the basic question of what could go wrong?

The scope of the BIA should be for those areas you control. For example, if the product is hosted by CHS then you don't need to do an analysis on the hosting, CHS will do this as part of their risk assessment. Equally, you don't need to analyse the IT infrastructure or buildings as that is the role of IT and Facilities respectively. It is important to clearly define the scope and settle any 'grey areas' at the outset. Don't just assume that because you have decided that this is not a risk you manage that someone else knows it's one you are expecting them to manage for you.

Once you have the scope, determine the teams you believe are most critical to the delivery of the service and focus on those. Also, identify your subject matter experts (SMEs) for each of these teams. Ideally, they should be individuals who actually do the job daily, which is not always managers. Those doing the hands-on work are often the most knowledgeable about processes and system dependencies and will provide the most accurate and critical assessment.

Talk with your SMEs and ask them to outline the risks to the business. If it is determined that this is a legitimate risk that your part of the business owns, then recorded in your risk register.

Analyse your risks

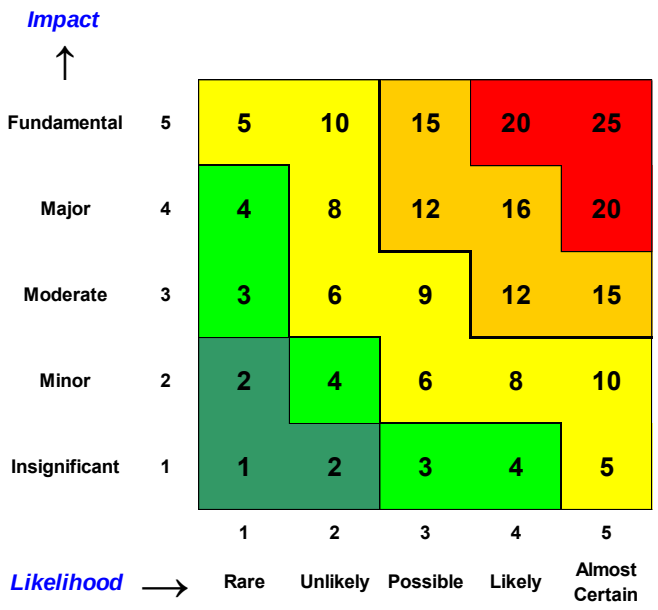
Risk Analysis – Once the risks have been identified, they need to be assessed based on a defined risk assessment methodology. There is a standardised risk assessment methodology used across Access for all our divisions, products, and functions. The assessment is on two main criteria:

- the likelihood (the probability) that the risk could materialise, and
- the consequences (potential impact). The impact (the business harm) that might result from the loss of availability, confidentiality, or integrity, for each of these risks, is assessed using reports and information in relation to that asset, the criticality to the business and known issues. The impact will usually be financial, or it could be reputational. In order to correctly analyse these, consider the impact against the overall profitability of the Division.

The analysis at this stage is based on the worst-case scenario, as if "no controls" are applied to stop it. This is your 'inherent risk'

In the risk register there is a table that outlines the levels of the probability and the impact of the risks (see next page), and this will give you a number between 1 and 5 for both probability and impact. Once entered into the risk register under the columns for inherent risk and it will a risk score between 1 and 25 (see below).

SCORE	RISK TOLERANCE	FINANCIAL IMPACT	REPUTATIONAL IMPACT	PROBABILITY	RISK REVIEW PERIOD
5	>5% of profit	Incidence would have a **fundamental** impact on the ability of the Business Unit to deliver its business plan and objectives.	**Severe long term damage** to organisation's reputation, such as: ■ *Likely to be significant national and local press and TV coverage as well as industry press interest.* ■ *Reputation of other Access divisions and the wider brand* ■ *Ability to win new bids and retain or extend existing contracts could be impacted by the situation*	**Almost Certain** or highly likely to occur **Greater than 75%** likelihood of occurrence	**Continual review** of the risk with an action plan in place, along with meeting minutes
4	3.5 - 5% of profit	Incidence would have a **significant** impact on the ability of the Business Unit to deliver its business plan and objectives.	**Long term damage** to organisation's reputation, for example: ■ *Likely to be some national and local press and/or TV coverage as well as the possibility industry press interest.* ■ *Ability to retain or extend existing contracts could be impacted.* ■ *Reputation of other Access divisions may be affected.*	**Likely** to occur **Between 50% and 75%** likelihood of occurrence	**Continual review** of the risk with an action plan in place, along with meeting minutes
3	2.5 - 3.5% of profit	**Moderate** impact on the ability to deliver over the short to medium term	**Medium term damage** to organisation's reputation, including: ■ *Some impact upon the client relationship and/or client's confidence in the business.* ■ *Possibility of some local press coverage and/or industry interest.*	Moderately likely or **possible** that it may occur **Between 30% and 50%** likelihood of occurrence	Reviewed **once per quarter** and decisions are minuted
2	1.5 - 2.5% of profit	Incidence would have a **minor** impact on delivering the business plan and objectives	**Short term damage** to organisation's reputation, such as: ■ *Embarrassment contained within organisation* ■ *Minimal press interest*	Low probability or **unlikely** to occur **Between 10% and 30%** likelihood of occurrence	Reviewed **once per quarter** and decisions are minuted
1	Up to 1.5% of profit	Incidence would have an **insignificant** impact on delivering the business plan and objectives	**Insignificant damage** to organisation's reputation nor any significant embarrassment.	Very unlikely or **rare** in practice to arise **Less than 10%** likelihood of occurrence	Reviewed as **a minimum annually** and the meeting minutes noted



Control your risks

Once you have completed the analysis process look at what controls you have in place that are designed to reduce this risk.

Types of controls may include:

Technical Controls: Encryption, network authentication, VPN, access control lists (ACLs), anti-virus & anti-malware, firewalls, patching, file integrity auditing software, mirrored datacentres, software & network architecture.

Administrative Controls: Policies, guidelines, recruitment and pre-employment checks, organisational structure, roles and responsibilities, contracts (customers, staff and suppliers) , skills, audits, compliance enforcement, threat assessments, supplier assessments.

Physical Controls: Well-constructed and maintained buildings, card access systems, locked windows and doors, remote monitoring, fire suppression systems

Preventative Controls: Training, security awareness, fire and intruder alarms, maintenance schedules, least privileged access, threat & vulnerability assessments, pen testing, change management, secure coding practices.

Detective Controls: Security information & event management (SIEM), intrusion detection systems (IDS) trend analysis, CCTV monitoring, system logs.

Corrective Controls: Intrusion prevention systems (IPS), backups & system recovery, business continuity and disaster recovery plans, uninterrupted power supply (UPS)

You may not manage all these controls, but you are able to make use of them. Assess how effective they are for the risk you are trying to manage and to what extent you make use of them. Your SMEs should be able to help you in this.

The controls in this list are based on the expected controls a business should apply as part of Annex A of ISO27001:2013. And our Statement of Applicability outlines how Access expects the controls to be applied.

Evaluate your controlled risks

Generally, the controls will reduce the probability or the impact of the risk, possibly both. So when you have added the controls, score the risk again and this will give you your 'residual risk'. That score is then compared against our Risk Appetite (This is the level at which risks may be tolerated and needs to be set as part of the governance process).

1. Low Risk within acceptable tolerances (Green): Risks may be tolerated to the left of the less bold line (risk scores 1 - 4)

2. Moderate Risk close to the Access risk appetite (Yellow): Risks may be tolerated or could need monitoring to ensure they do not rise (risk scores between 5 - 10)

3. High Risk Exceeds the Access risk appetite (Amber and Red): These risks need urgent and active management to reduce them (risk scores 12 - 25)

4. **Risk acceptance levels**

RESIDUAL RISK SCORE	ADDITIONAL RISK ACTIONS PLANNED
20 - 25	Unacceptable level of exposure which requires **immediate action** by senior management
12 - 16	Unacceptable level of exposure which requires management attention and an **action plan with timescales**
5 - 10	Manage by specific response procedures and monitor their effectiveness
3 - 4	Acceptable level of exposure subject to regular monitoring
1 -2	Acceptable level of exposure

Deciding how to manage your risks

The Access Board or the DMTs will decide how they wish to manage the identified risks. This is a business decision weighing up the risk, the business aims, the resources and funds available and the senior management team are ultimately accountable for the decision. There are four basic decisions that can be made regarding each risk.

- Treat – Apply additional or strengthen existing control/s to bring the risk down to an acceptable level
- Transfer – this usually involves insurance to absorb the impact of the risk being realised
- Terminate – stop the activity that is causing the risk
- Tolerate – this is when the risk falls within our risk appetite and the controls are deemed adequate.

Note:

- When the cost of applying a control to treat a risk is more than the cost of the impact of the risk being realised then the risk should be tolerated or terminated.
- When the cost of applying a control to treat a risk exceeds the cost of the asset being protected then the risk should be tolerated or terminated.

The risks need to be reviewed regularly to ensure that the likelihood and the impact have not changed and the decision remains the right one and it recorded on the register.

Recording risk

All identified risks must be recorded on your divisional or functional Access Information Risk Register. The fields you need to complete include:

- Date Risk Last Reviewed
- Movement
- Risk Description
- Impacts
- Proximity (Date)
- Risk Category
- Risk Category Group
- Business/ Function/Team
- Client/Service
- Risk Owner (individual or team)
- Inherent Impact & Probability and Inherent Risk
- Existing Controls
- Residual Impact & Probability and Residual Risk
- Additional Risk Actions
- Who signed off on the risk decision and when?
- Action Owner
- Action Due Date

There are guidance notes in the risk register that give further details on what these fields are.

Risk review process

The Risk Operations Group will hold meetings with the DMT risk managers to review the risk assessment process and treatment plans to ensure that the risks are being correctly assessed and reviewed. Not all the risks will be assessed at each quarterly meeting.

The annual meeting schedule would be:

1st Meeting – A review of the High and Moderate risks

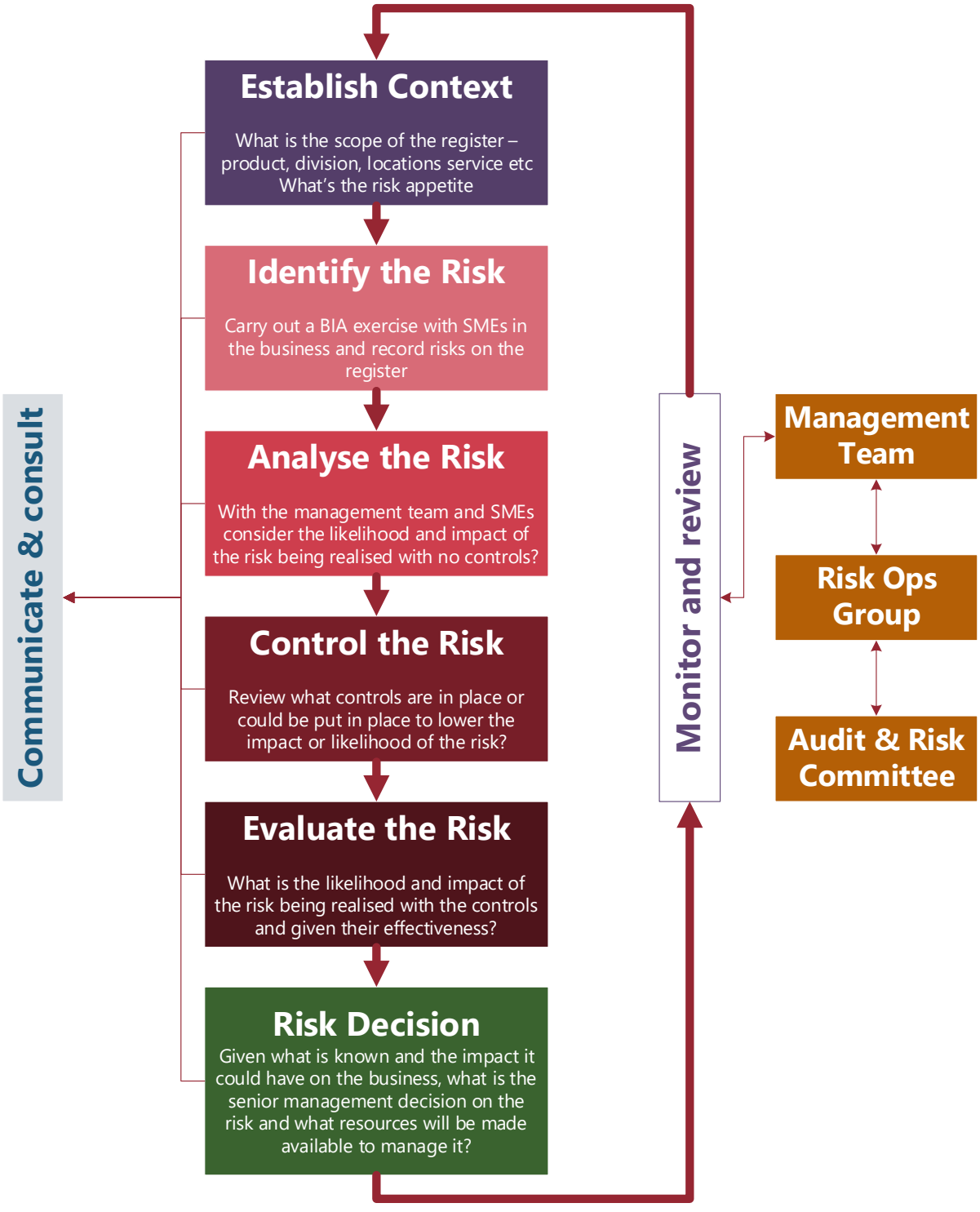
2nd Meeting – A review of the High and Low risks

3rd Meeting – A review if the High and Moderate risks

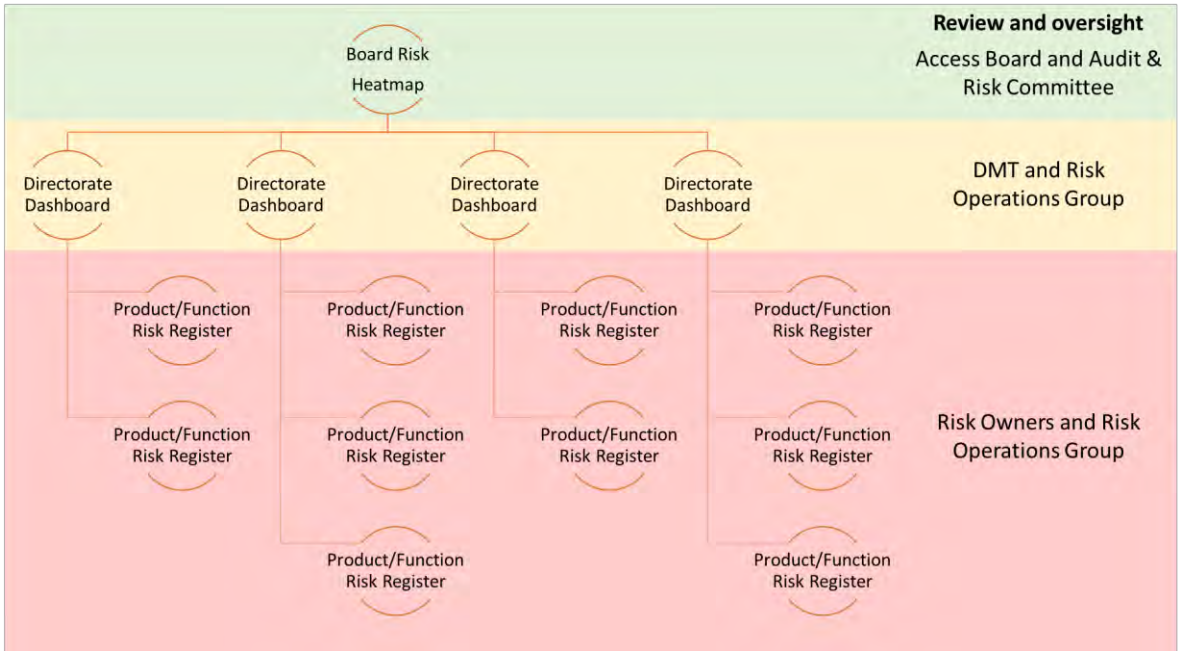
4th Meeting – A review of the High risks.

The following people will need to be included, as a minimum at each meeting, the risk document owner, individual risk owners, anyone managing actions.

Risk management cycle



Each risk register follows the same format so the risks and controls across the products can be compared and then brought into a single divisional dashboard for the DMT to review. The risk profile for each division will then be fed into a risk performance heatmap for the Board to review, giving them a high level view of risk management across the business.



Document Owner and Approval

The Director of Information Security is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

Issue	Description of Change	Approval	Date of Issue
1.0	Initial issue	ISM	15/05/2014
2.0	Methodology incorporated into process	ISM	15/7/2014
2.1	Acceptable risk section added	ISM	07/01/2016
2.2	Review of risk levels required COO	COO	24/11/2016
2.3	Amendments to fines to accommodate GDPR changes	COO	01/02/2017
2.4	Acceptable risk period extended to 1 year	COO	06/02/2017
2.5	Annual review – amendment related to GDPR	ISM	30/04/2018
2.4	Annual review – no amendments	ISM	23/01/2019
2.4	Annual review – no amendments	ISM	23/01/2020
2.5	Annual review – no amendments	MS	01/02/2021
2.6	Added in Governance details and updated process	GL	27/07/2021
2.7	Annual review – minor amendments	NB	01/03/2022
2.7.1	Brand change	MS	19/10/2023
2.8	Annual review	MS	15/01/2024

A current version of this document is available to all members of staff on SharePoint.