This is a draft
Your feedback will help us improve it.

Manage identity risks to your service

You need to know what risks your service might be affected by. These could be risks to:

- your organisation's reputation or finances
- any information your organisation keeps or collects about your users
- any property, equipment or resources your organisation owns (these are also known as 'critical assets')

You can control these risks and minimise the impact they'll have on your service and users if you manage your risks.

You'll be exposed to a higher level of risk if your organisation creates or works with digital identity accounts. This is because the information you'll be working with is more sensitive and valuable than usual.

There are 7 steps involved in managing your risks:

1. Be aware of what context you work in
2. Identify what risks you are or could be exposed to
3. Find out how much impact these risks could have
4. Plan how you will protect yourself against these risks
5. Record these risks in a 'risk register'
6. Communicate these risks with your stakeholders and users
7. Monitor and review the risks

1. Be aware of what context you work in

Some things might affect the work you do, such as:

- the environment you're working in
- the people or organisations you work with

Being aware of these things will help you identify any risks that you could be exposed to.

These risks could be:

- external risks
- internal risks
- security risks

External risks come from outside your organisation, for example an organised crime gang. Your organisation might be exposed to these types of risk if XXXX.

Internal risks comes from within your organisation, for example people you work with. Your organisation might be exposed to these types of risk if:

- you do not do thorough background checks on new staff
- you do not check if any software you use has been corrupted

Security risks could be things like:

- data breaches
- users creating or signing in to your service with fraudulent digital identity accounts

2. Identify what risks you are or could be exposed to

When you have an idea of what types of risk exist, you must think about what risks your service or organisation:

- could be exposed to
- is already exposed to

You can do this by considering all scenarios where any **threat** leads to a **vulnerability** that has a direct **impact** on an asset.

- Begin by evaluating all applicable assets - how critical are they to your identity service
- Evaluate the vulnerabilities to your service
    - Rank vulnerabilities accordingly in terms of the controls they affect

A table outlining vulnerability ratings is provided as guidance in the annexe.

- Evaluate how effective controls and safeguarding mechanisms are that you have in place are
    - Pay attention to such things as a control's ability to deter attacks, it's ability to respond to an attack
    - Consider how often the control is tested and when was the last time it was tested
    - Has there been any change in legislation that affects the control

    - Have any modifications to the environment in which the control operates been made that affects its ability to safeguard

- Evaluate different threat actors that pose a risk to your service. When doing so focus on what the consequences would be should these risks materialise

Different threat actors have different motivations and capabilities. You need to consider the various actors and where their actions could cause disruption and to whom.

Threats can come from politically motivated groups, organised criminal gangs, state sponsored groups, insider employees and contractors or members of the public.

The impacts could affect individuals, relying parties, attribute providers, identity providers, information exchange parties and the wider framework infrastructure.

After evaluating the above:

- Identify all potential risks keeping in mind the assets, vulnerabilities, threats and consequences.

Useful information on emerging threats can be found by consulting the NCSC website and other resources like this. You should regularly consult these resources to help you in your identification process.

3. Find out how much impact these risks could have

You must find out how much impact these risks could have.

- Rank the criticality of assets and the impact of a threat

You can do this by deciding which groups would be affected by the risk and then giving each impact a rating along with a short description.

Ratings should be ordered from the highest level of criticality down to the lowest. This helps to focus resource allocation on the most important areas of risk management.

A template to help you do this is included in the annexe of this document.

- Rank the vulnerabilities you have identified and align this to your assessment of the controls and safeguards you currently have in place

Treat each control you have assessed separately.

- Determine what the threats are and the impact and consequences to each group
    - Assets
    - People
    - Capability
    - Information
    - Identity
    - Organisation

- Consider the consequences of compromises to:
    - Information integrity and accuracy
    - Service availability
    - Individual and wide scale identity loss of theft
    - Financial loss
    - Reputation and brand damage

- Rank these accordingly.

For guidance a table of potential consequences is provided in the annexe.

- You now need to consider the likelihood of any of these risks occurring.
    - Likelihood of risk is usually considered as:
        - Extreme
        - High
        - Medium
        - Low
        - Negligible

You need to consider the various sources of risk and the effectiveness of the controls that you have evaluated.

- Rank the tolerance level of each risk identified
    -

Each risk identified takes all the evaluations you have carried out so far and then is described in terms of its risk level. This is the potential consequences of the risk event, the likelihood of it occurring, and what you determine as an acceptable level of tolerance.

Risk management incorporates sound management oversight and communication of risk to all involved stakeholders and you should keep this in mind and produce a risk management plan.

4. Plan how you will protect yourself against these risks

You must make a plan to show what you and your organisation will do to be protected against these risks.

5. Record these risks in ‘a risk register’

A risk management plan is usually best actioned with a risk register.

The risk register provides an agreed record of the significant risks that have been identified through the risk assessment process. Assigning ownership of risks and will also give you a record of the control activities that are currently undertaken. It also provides a record of the additional actions you should propose to improve control of particular risks, including responsibility and timescales for the implementation of those intended controls.

For risks to be managed efficiently the register should be well constructed and dynamic. You should use this to effectively drive changes and improvements. Risk registers provide the assurance required that risks and controls are being monitored and it is something that the auditor will investigate thoroughly.

A suggested template for a risk register is provided

6. Communicate these risks with your stakeholders and users

You must tell any people you work with about the risks you've identified and what you're planning to do to protect yourself against them. The needs of stakeholders for information will vary depending on their role.

You will have internal decision makers such as Risk Advisors, Information Security Officers, Asset Owners, Compliance Officers and other senior management that need to know how risk is being managed and treated along with external stakeholders such as auditors, other organisations who may need to be alerted to any threats that could affect them, people responsible for fraud reporting and the framework’s authoritative body if risks pose a threat to other entities in the framework. There may be instances when risks identified may have an affect on some regulations that you must meet in which case you need to follow the appropriate course of action to communicate the risk and its treatment.

7. Monitor and review the risks

You must make sure you monitor these risks over time.

Effective risk management is not a static process but one that needs continual attention and monitoring. It is important to view this as a process that aims to continually improve the efficiency of controls and safeguards to reduce risks that impact digital identity. You need to continually consider the implementation of controls, whether they remain relevant, whether changes in environment or technology has an effect on risk and who needs to be informed. You should pay as much attention to monitoring and reviewing risks that may change priority due to staffing or resource changes and emerging threats that may take a risk from low likelihood to high.

You can choose to 'close' a risk if you think:

- something is no longer likely to have an impact on your service
- you feel like you've done everything you can to protect your service against a particular risk

8. Identity Risk

[Specific stuff around managing identity risks]
Impact on identity services

9. Identity fraud risk

[Specific stuff specifically dealing with fraud risk]

10. Mitigating risk through monitoring

[Stuff around how to mitigate identity and fraud risk through transaction, behavioural and session monitoring]

Threats to online services and vulnerabilities

Threat actors

Compromise methods

Types of attacks

Controls

Behavioural monitioring

Transaction monitoring

Session monitoring

Put a SOC in it…

Response, escalation

Risk management is a process that allows individual risk events and overall risk to be understood and managed proactively. Additionally, correct risk management can optimise success by minimising threats and maximising opportunities. When implemented as a structured process it can:

- determine the nature of threats
- help identify vulnerabilities
- provide quantification of the potential consequences of future events
- help determine the resources needed to protect and safeguard, systems, information and other assets
- help provide controls and safeguards to protect and support operations

The Trust Framework's governance function is provided with assurance that risk management and risk assessment procedures are being followed when evidence can be collected demonstrating:

- That risk management and risk assessment procedures are implemented
- That risk management and risk assessment procedures are followed
- That any deviation from these is agreed by the authoritative body
- That their effectiveness is tested
- That reports are given to the authoritative body as requested

It is a requirement that Risk Management and Risk Assessment are ongoing activities which identify all risks, including risks that might be caused by countermeasures introduced to address other risks.

This document describes the requirements for risk management and risk assessment.

Part 1 of this document details the risk management method to be followed
Part 2 of this document defines the risk assessment phases to be followed

The appendix gives a number of example scenarios. These examples are commonly found risks and are provided as guidance. The list should not be viewed as exhaustive and auditors will pay attention to emerging risks and require information and evidence collection that risk identification, threat, vulnerability and risk analysis are ongoing processes.

For requirements and guidance on risk management, see the following:

- BS EN ISO/IEC 27001;
- ISO/IEC 27005;
- BS ISO 31000;
- BS EN IEC 31010:2009; and
- NCSC guidance.

Part one

Risk Management

Risk Management

The requirements for risk management

1. Based on a comprehensive business, security and fraud impact assessment and risk assessment.
2. Documented in a standardised manner.
3. Reviewed and approved by the board and senior management at least annually.
4. Information should be disseminated to relevant employees.
5. Properly managed in any instance when the maintenance and development of continuity planning is outsourced to a third-party.
6. Have a specific methodology and process outlining what conditions should prompt implementation of the plan and the process for invoking recovery and continuity of services.
7. Have a specific methodology and process outlining what immediate steps should be taken during a disruption to respond to unanticipated threat scenarios and changing internal conditions.
8. Focused on the impact of various threats that could potentially disrupt operations rather than on specific events.
9. Developed based on valid assumptions and an analysis of interdependencies
10. Effective in minimising service disruptions and loss through the implementation of mitigation strategies.

Operational Risk Management

Digital Identity and Risk Management

Requirements and Standards to be followed:

- BS EN ISO/IEC 27001;
- ISO/IEC 27005;
- BS ISO 31000;

- BS EN IEC 31010:2009; and
- NCSC guidance.

Assurance Levels

Implementation environment

Top down
Bottom up

Risk management responsibilities

- Senior Information Risk Owner
- Information Asset Owner
- Risk Manager

Potential for risk

1. Data security
2. Governance
3. Methods of authentication
4. Transaction monitoring
5. Liability

Safeguarding

1. Limiting access to …
2. Limiting access to…
3. Monitoring…
4. Monitoring …
5. Policy…(standardisation etc.)

Risk management methodology

The risk management methodology to be followed comprise the following steps:

1. Establish the context
2. Risk assessment
3. Risk identification
4. Risk analysis and evaluation
5. Risk treatment plan
6. Communication
7. Monitoring and review

8. Risk register

Part 2
Digital Identity and Risk Assessment
Risk assessments
Infrastructure
Roles and responsibilities
Risk assessment process and procedure
Identification
Identification and determination of assets
Identify threats
Analyse vulnerabilities
Identify existing controls
Determine consequences
Identify incident scenarios
Analysis
Analyse risk
Assess impact
Assess probability
Estimate level of risk

Evaluate
    Evaluate risk

Part 2
Risk Identification
    Assets
    Vulnerabilities
    Threats
Risk Evaluation
Threats to assets
Vulnerabilities
Potential breaches
Probability
Impact
Countermeasures
Consequence review
Risk avoidance

Fraud risk assessment

It is a requirement that specific Fraud Risk Assessments are conducted for each service.

All service providers are expected to show that they have fully considered potential fraud risks and identified them accordingly. Additionally, evidence needs to be in place that demonstrates how fraud risks are mitigated, controlled and managed.

At a minimum this means Fraud Risk Assessments are conducted:

Before the system becomes operational
At predetermined intervals confirmed in an audit schedule, this is usually at least once a year
Whenever a new fraud risk is identified or suspected
Whenever structural or functional changes are made
Any proprietary changes are made

Appendix
Example risk scenarios
Personal data breach
Loss of availability
Compromise of cryptographic algorithms
Compromise ...

Part two

This section defines the risk assessment process and has three stages as follows:

1) Risk identification: Identifying the different factors (assets, threats, vulnerabilities, consequences and incident scenarios) that will identify and evaluate the risks:
2) Risk analysis: Determining the risk level based on the impact of each incident scenario and their probability of occurrence.
3) Risk evaluation: Producing a scored list of all the identified risks, based on the risk analysis results; the business criteria; the affected assets and their vulnerabilities and the potential threats.

1) Risk identification:
    a) System scope delimitation: Determining the scope included in the risk assessment and its boundaries
    b) Asset identification: Identifying any type of item that has value to the organisation and that could cause damage if it is involved in an incident.
    c) Threat analysis: identifying all agents, either natural or human made, accidental or intentional, internal or external, that could pose a threat to the organisation.
    d) Vulnerability analysis: Identifying all potential weakness in the organization that could facilitate a successful attack and cause damage to the assets.
    e) Consequence determination: Identifying the possible consequences that different events could have on the organization.
    f) Incident scenario identification: Determining the possible events that could have an impact on the organization and that will serve as a base to identify the risks.
    g) Risk analysis: Determining the risk level based on the impact of each incident or scenario and their probability of occurrence.
    h) Risk evaluation: Producing a scored list of all the identified risks, based on the risk analysis results; the business criteria; the affected assets and their vulnerabilities and the potential threats.

2) Risk analysis
    a) Analyse risk
    b) Assess impact
    c) Assess probability
    d) Risk level estimation

3) Risk evaluation
    a) Assets: identification, classification and evaluation

b) Threats to assets: classification and evaluation
c) Vulnerabilities present
d) Probability or frequency of the threat
e) The impact that the risk has or could have on the entity's organisation
    i) Categories of impact
        (1) Inconvenience, distress, or damage to standing or reputation;
        (2) Financial loss or liability;
        (3) Harm to public interests;
        (4) Unauthorised release of sensitive information;
        (5) Personal safety
        (6) Civil or criminal violations.
    ii) Evaluation of impact
        (1) Low
        (2) Medium
        (3) High
    iii) Scoring
f) Countermeasures that can reduce the impact
g) Consequence review/risk profile
h) Risk avoidance
i) Risk transfer
j) Risk mitigation
k) Residual risk, risk acceptance, risk treatment plan, etc
l) Compensating controls.