HM Government

Government Functional Standard

GovS 007: Security

Version: 1.0
Status: Approved for internal government trial
Date issued: 24 July 2020

This functional standard sets expectations for undertaking work within the scope set out in clause 1.2.

It is part of a suite of functional standards designed to promote consistent and coherent working within government organisations and across organisational boundaries, and to provide a stable basis for assurance, risk management and capability improvement. Functional standards are designed to be used as a suite (they cross-refer where needed), and contain mandatory and advisory elements described in consistent language, see table below.

Term	Intention
shall	denotes a requirement: a mandatory element.
should	denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	denotes a description.

The meaning of words is as defined in the Shorter Oxford English Dictionary, except where defined in the Glossary in **Annex B**.

It is assumed that legal and regulatory requirements are always met.

Produced by Government Security Group

Alternative format versions of this report are available on request from GSFInfo@cabinetoffice.gov.uk

Contents

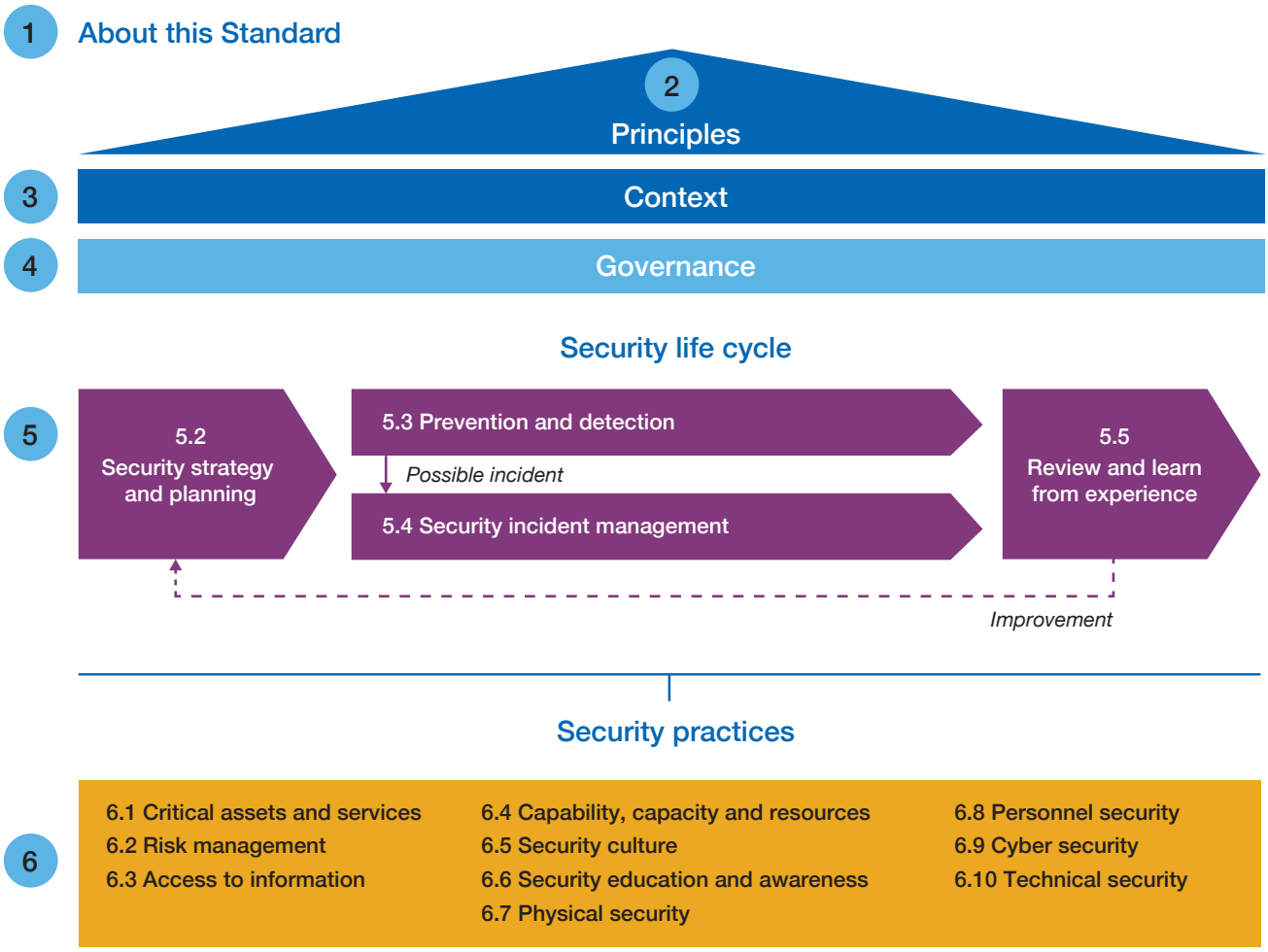

Figure 1 Scope of this functional standard

1 About this government functional standard

1.1 Purpose of this standard

The purpose of this standard is to set expectations for protecting:

- the government's people, information and assets
- visitors to government property, and third-party suppliers whilst engaged on government business
- citizen data

This standard provides direction and guidance for:

- permanent secretaries, directors general and chief executive officers of arm's length bodies, ensuring the right environment for effective delivery and performance
- leaders and members of Clustered Security Units and Centres of Excellence
- security advisers, and other named security officials
- those responsible for communicating security information to governmental staff and visitors
- staff and third parties, working within and for government, who have a responsibility to ensure security practices are followed

1.2 Scope of this standard

This standard applies to government security risk management, planning and response activities for cyber, physical, personnel, technical and incident management [1]. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm's length bodies or their contracted third parties.

Where activity requires staff or third parties to have developed vetting status, the requirements and recommendations contained in this standard are mandatory [2].

Note: Certain practices listed within this document might be contracted out to third parties. In such instances the detail within this document should be superseded by any existing commercial requirements. However, moving forward it is expected that parties should comply with and refer to this standard.

1.3 Government standards references

The following standards are necessary for the use of this standard:

- GovS 003: Human Resources
- GovS 004: Property
- GovS 005: Digital, Data and Technology
- GovS 008: Commercial
- GovS 010: Analysis

2 Principles

Those responsible for security shall ensure:

1. a security risk management approach based on an assessment of threat and vulnerability and which ensures that security enables the business of government and supports government policy and objectives
2. security risks are managed appropriately, with governance frameworks and controls being proportionate to the prevailing level of risk
3. security planning is holistic, covering all aspects including cyber, personnel, physical, and technical, aiming to prevent incidents as well as responding and learning from them
4. protective security reflects the UK's national security objectives and ensures that the government's most sensitive assets are protected
5. there is a focus on embedding the right security culture and behaviours
6. work is assigned to competent, appropriately skilled people
7. accountabilities and responsibilities are defined, and traceable across every level of management [3]
8. public service codes of conduct and ethics and those of associated professions are upheld

3 Context

3.1 Overview of security

The Prime Minister is ultimately responsible for the security of HM Government. He or she delegates accountability to the Cabinet Secretary, who in turn delegates accountability to Permanent Secretaries and Accounting Officers. Accounting Officers are accountable to Parliament for the security of their organisations.

The Government Security Group, based in the Cabinet Office, oversees government security at the direction of the Government Security Board and is responsible for the development of the Security Function and management of the Clustered Security Units. The latter being the operational centres that deliver security services to Departments and agencies, which fall within their remit. The Government Chief Security Officer (a Director General appointment) is accountable to the Civil Service Board.

The Government Security Group aims to deliver:

- an integrated and impactful function
- a dynamic response to risk
- excellent shared security services
- an exciting and rewarding security profession
- insightful and expert colleagues

The Government Security Group is distinct from the Cabinet Office's National Security Secretariat (NSS), which delivers the Government's national security, foreign policy priorities and shapes the UK's response to international issues which impact national security.

Management of security is on three levels, as shown in Figure 2: Cross-government, Cluster and Organisational (including arm's length bodies), with Departments consolidated into Clustered Security Units.

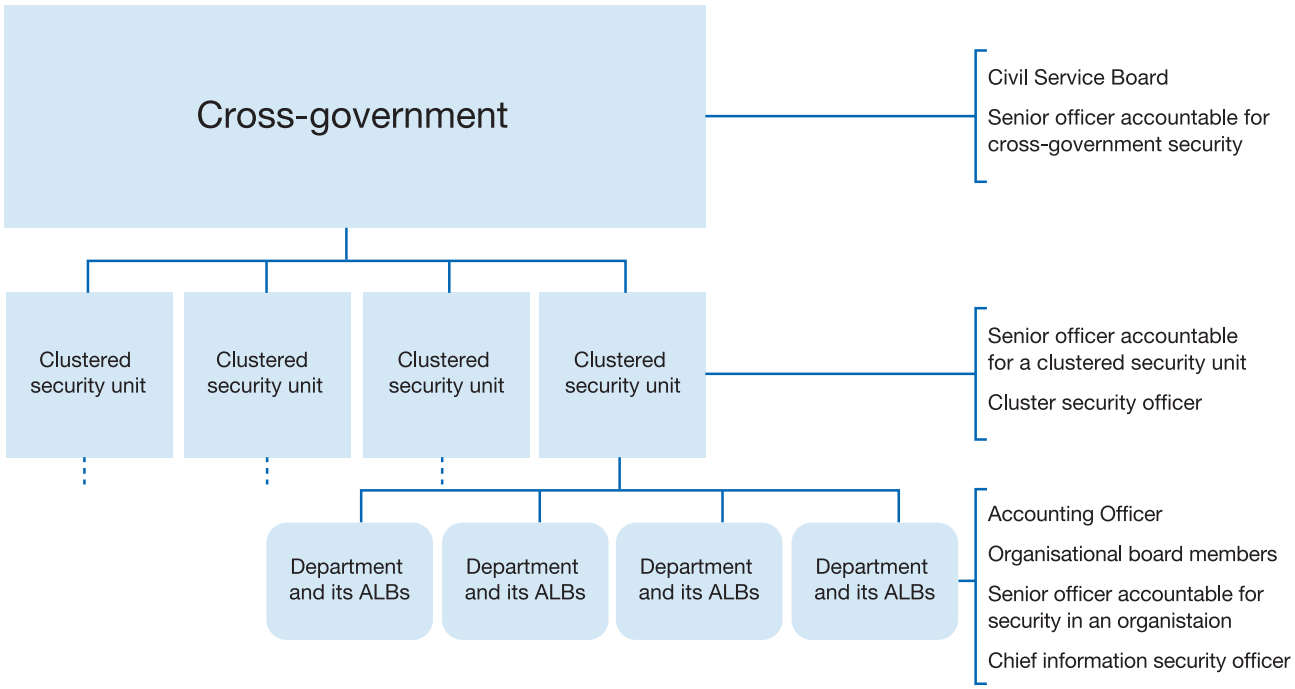

Figure 2 Three levels of security with associated roles (see 4.5)

Note: Each Clustered Security Unit is led by an accountable officer, responsible the provision of protective security services (see 4.5.2).

3.2 Integrated protective security

Security comprises four interconnected aspects: physical (relating to buildings), personnel (relating to people), cyber (relating to information systems technology) and technical (relating to counter eavesdropping). When considered together, these elements comprise protective security [1].

Physical security is the practice of protecting elements of government infrastructure, estates and personnel against attacks or compromises in the physical (i.e. tangible, real-world) environment.

Personnel security, in this context, is the practice of ensuring the security of government information and infrastructure against threats arising from government personnel. This could include deliberate attacks, criminal activity for-profit, or gross negligence, and could manifest in a variety of environments, including the physical (i.e. tangible, real-world) or virtual (i.e. in cyberspace). Such individuals could join government service intending to commit such acts, or decide to do so after employment.

Cyber security, in this context, comprises technologies, processes and controls that are designed to protect systems, networks and data from the deliberate exploitation of computer systems, technology-dependent enterprises and networks.

Technical security is the practice of detecting the compromise of protective security systems, analysis and prevention of technical attack, mitigation of technology vulnerabilities and the deployment of countermeasures.

Underpinning all four is good **incident management** - the organisation's response to a security incident. A security incident is any circumstance that has arisen that has the potential to compromise government assets including people, property or information.

4 Governance

4.1 Governance and management framework

4.1.1 Overview

Governance is a set of policies, standards, processes and organisational arrangements through which management activities are authorised, directed, empowered and overseen, to achieve organisational goals and manage risk appropriately. Security governance should be integrated into the organisation's overall governance, so as to align security objectives and requirements with the organisation's strategic aims and delivery objectives.

4.1.2 Cross-government management

A cross-government security policy framework [4] should be defined and established to provide a broad framework for managing security in order to protect UK government assets (people, information and infrastructure). The policy framework should focus on outcomes required to achieve a proportionate and risk-managed approach to security that enables government business to operate effectively, safely and securely.

The cross-government security policy framework should be supported by policies, standards, best-practice guidance and approaches which should be maintained and communicated to those with organisational security responsibilities.

4.1.3 Organisational management

Each organisation in government, shall define and establish a security governance and management framework covering physical, personnel, cyber, incident management and technical security [1]. Frameworks should include authority limits, decision-making roles, rules and definitions, degrees of autonomy, assurance needs and processes, reporting structure, accountabilities and responsibilities. This governance and management framework should cover the practices described in this functional standard.

Security management frameworks should be responsive to new and changing circumstances, reflect actual and emerging security threats and include how organisations should manage risk (see 6.2). Where systems have broken down or individuals have acted improperly, appropriate action should be taken.

The accounting officer for each organisation shall appoint:

- a board member (or equivalent) with a specific security remit (see 4.4.6)
- a senior officer accountable for security (see 4.4.7)

Organisational senior officers accountable for security should work together to ensure policies, practice guidance and processes are followed in their respective areas in order to mitigate security risk.

4.2 Assurance

Assurance is the systematic set of actions necessary to provide confidence to senior leaders and stakeholders that the security function is providing a safe and successful platform for delivery of policy, strategy and objectives. Organisations shall comply with mandated cross-government assurance activities as coordinated by the Cabinet Office [5].

4.2.1 Assurance framework

Objective, evidence-led evaluation of the effectiveness of the Government's security controls should be undertaken to monitor delivery, identify activities and support improvement, and to make informed decisions. Analysis in support of evaluation shall be undertaken in accordance with GovS 010: Analysis.

Assurance should be carried out on at least three levels:

- by, or on behalf of, operational management within organisations, applying judgement to support successful delivery and adherence to functional standards
- by, or on behalf of, senior management, independent of operational management, in accordance with the defined assurance approach
- by independent bodies (within or external to government, such as internal audit and National Audit Office) that can provide an objective evaluation of the adequacy and effectiveness of governance, risk management and controls

The work of internal and external assurance providers should be planned to minimise operational disruption and overlap with the organisation's other assurance activities, whilst remaining rigorous.

Where assurance includes formal review activity, the customer for the review should be clearly identified.

4.2.2 Human resources and security

Due to the interdependencies between personnel security and human resource management, organisations shall include the assurance of human resource management activities within their organisational approach to security. This should be aligned to the overall government assurance practice, guidance and arrangements. In accordance with government audit procedures and roles, human resource activity should be assured at three levels:

- first by human resource managers operating within established frameworks to the organisation's risk threshold
- second by risk, quality and compliance professionals within the organisation
- third by cross-government independent audit experts

See GovS 003: Human Resources.

4.3 Decision making

Decisions should be made in a timely manner by evaluating alternative choices against agreed criteria. Relevant stakeholders and subject matter experts should be consulted. Decisions might relate to:

- setting policy for security across the government, cluster or organisation
- developing new controls for a perceived threat to government security
- approving plans for adhering to this security standard and associated requirements;
- security vetting
- incident management and breach response

Analysis relating to decisions should be undertaken in accordance with GovS 010: Analysis.

4.4 Roles and accountabilities

4.4.1 Overview

Roles and accountabilities for those engaged in government security related roles shall be defined in the respective governance and management framework. This includes, but is not limited to, who in each organisation is accountable and what activities, outputs or outcomes they are accountable for [3]. The responsibilities should cover every aspect of this functional standard.

4.4.2 Senior officer accountable for cross-government security

The senior officer accountable for cross-government security is accountable to the Civil Service Board for cross-government security policy and standards and for advising accounting officers on setting the risk threshold for their organisations. In particular, they should:

- define and establish cross government security policy and standards
- monitor performance against policy and standards
- oversee day-to-day operations including responding to serious and/or cross-government security incidents or issues
- provide guidance and direction to the senior security role holders, when requested

Note: This role is currently known as the Government Chief Security Officer.

4.4.3 Senior officer accountable for a clustered security unit

The senior officer accountable for a clustered security unit is accountable to the senior officer accountable for cross-government security for the provision of protective security services for the organisations comprising the clustered security unit.

Note: The senior officer accountable for a clustered security unit is usually the accounting officer (see 4.4.5), but can be a director general level appointment for the lead department in the cluster.

4.4.4 Chief security officer

A chief security officer is accountable to the senior officer accountable for a clustered security unit for the day-to-day operation of the unit. In particular, they should, in consultation with each constituent organisation's senior officers accountable for security:

- define and establish the services to be delivered
- define and agree the Memorandum of Understanding and service levels with each organisation within the cluster
- deliver protective security services (the service catalogue) to organisations within their cluster

Protective security services should cover physical, personnel, cyber and other cross-cutting areas of security, such as technical security, cyber security consulting and national security vetting amongst others.

Note: the chief security officer is usually a director level appointment and is often the senior officer accountable for security in an organisation (see 4.5.6) for the lead Department in the cluster.

4.4.5 Accounting Officer

An Accounting Officer (or equivalent in an arm's length body) is the senior officer accountable for security in an organisation, supported by their management board. The Accounting Officer is accountable to the Civil Service Board for providing assurance that the organisation meets the requirements in this functional standard.

Note: The permanent head of a government department is usually its Principal Accounting Officer. The Principal Accounting Officer generally appoints the most senior executive in organisations under the department's ambit as an Accounting Officer.

4.4.6 Organisational board members

A board member shall be appointed by the Accounting Officer to have specific responsibility for oversight of security compliance and auditing processes, including arrangements to determine and satisfy that delivery partners, service providers and third-party suppliers, apply proper security control, including understanding and managing security issues that arise because of dependencies on external suppliers or through their supply chain.

Each management board member in an organisation is accountable to the Accounting Officer (or equivalent in an arm's length body) for oversight of, and responsibility for security risk management in their respective business area(s).

4.4.7 Senior officer accountable for security in an organisation

The senior officer accountable for security in an organisation is accountable to the Accounting Officer (or equivalent in an arm's length body) for the implementation and maintenance of security standards across the organisation and for ensuring correct procedures and delegations are in place to respond to security incidents.

They shall be responsible for:

- advising the organisation's senior officers on security issues, including the management of security risks
- appointing an incident manager, when needed
- articulating the security needs of their organisation
- overseeing and reporting on the delivery of services to agreed standards
- defining and owning local security policies
- securing funding for professional training, qualifications and continuous development
- requesting advice and guidance for the senior officer accountable for cross government security, when needed

The senior officer accountable for security in an organisation should act as an intelligent customer, taking on responsibility for defining the security services required by their organisation, requesting services from the cluster security officer (see 4.4.4) and ensuring the requirements of their organisation are being met to agreed standards and service level agreements.

Note: This role is commonly known as the Senior Security Advisor.

4.4.8 Chief information security officer

The chief information security officer is accountable to the senior officer accountable for security in an organisation (see 4.4.7) for the security of information in electronic form [6]. In particular, they shall:

- advise the organisation's board on how to exploit technology to deliver the organisation's strategic objectives, and provide strategic leadership for the organisation's IT community and its investment in technology
- be responsible for the development and maintenance of the organisation's IT strategy, IT architecture, IT policies and standards, technology assurance and IT professionalism

4.4.9 Incident manager

The incident manager is accountable to the senior officer accountable for security in an organisation (see 4.4.7) for the management and resolution of an incident and any subsequent breach, in particular assessing:

- the type of incident
- whether the incident is a security breach
- if the breach involves a loss or compromise
- the level of impact of the breach

The person appointed as an incident manager should not have any conflict of interest in investigating the incident.

Note: The senior officer accountable for security in an organisation can undertake the role of incident manager. For cross-government incidents this role can be undertaken by the senior officer accountable for cross government security.

4.4.10 Security specialists

Other specialist security roles should be defined to suit the needs of the security related activities being undertaken. This can be for a variety of aspects of security practice in accordance with this functional standard and the organisation's governance and management framework. Such roles may be advisory or executive.

Note: Examples of specialist roles include, but are not limited to, risk owners, information asset owners, data protection officers, communications security officer, crypto custodian and intelligence handling coordination.

5 Security life cycle

5.1 Overview

The security life cycle includes strategy and planning, prevention and detection, incident management and reviews lessons learned; see Figure 3.

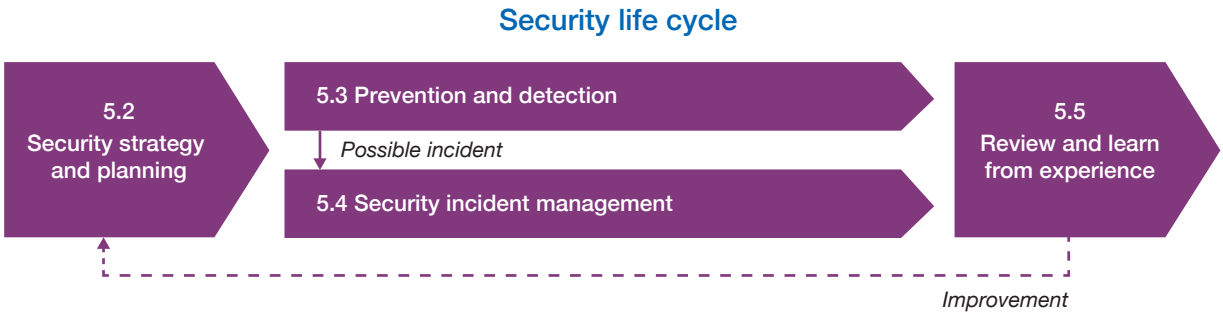

Figure 3 Security life cycle

5.2 Security strategy and planning

5.2.1 Security strategy and planning

Organisations' security strategies should align with the vision for protective security in government, as set by the senior officer accountable for cross-government security (see 4.4.2). Organisations should seek to develop plans that deliver the 'Protect to Enable' element of the Government Security Function, that is, they should seek to protect government operations to the appropriate level, while enabling the functioning of government's services and operations.

Security plans should take into account incidents that have been reviewed and incident response plans. Security planning should be holistic, encompassing all aspects of good protective security.

5.3 Prevention and detection

5.3.1 Security arrangements

Organisations should undertake a regular assessment of the security arrangements that they have in place, and assess whether these remain appropriate to the organisation's specific requirements. Day-to-day security activity in an organisation should be carried out in a way that avoids security incidents arising in the first place.

Security concerns, noted by anyone working for or with government, including third party contractors, should be reported in a timely manner.

5.3.2 Incident management plan

Each organisation shall produce, and regularly test, a security incident management plan, describing how security incidents should be managed and resolved. This framework should be communicated to appropriate stakeholders. The incident management plan should include:

- activities as described in this functional standard in the incident management technical standard [1]
- the roles and responsibilities of individual officers
- measures for communication with personnel and the emergency services, especially at the time of the incident and period immediately following an incident
- a provision for a review of best practice

The incident management plan shall be supported by policies, processes and systems to ensure reports and actions are received and can be acted on without undue delay.

Government organisations shall have management structures which ensure shared communications between human resources and security teams, and provide policies and procedures for detecting, reporting, responding to and handling incidents, including disciplinary measures which are communicated to, and understood by, staff.

5.3.3 Breach response plan

Organisations should plan proactively for the mitigation of possible breaches through the development of a breach response plan(s). The plan should include controls, mitigating measures and continuous improvement actions, for each recognised threat or group of related threats.

The breach response plan should include:

- the roles and responsibilities of individual officers
- actions to be taken in responding to a breach, taking account of any legal obligations associated with the reporting of a breach
- measures for clear communication with personnel and the emergency services, especially at the time of the breach and period immediately following a breach
- a provision for a review of best practice

5.4 Security incident management

5.4.1 Overview

The primary practices for managing an incident are shown in Figure 4 and described in the clauses 5.4.2 to 5.4.4. Security incidents should be managed in accordance with the incident management plan (5.3.2) and, where relevant, a breach response plan (5.3.3).

5.4.2 Incident reporting

A security incident (breach or attempt), when detected, should be reported as soon as possible within the organisation's defined timeframe, so it can be investigated.

Those with security related responsibilities shall understand their legal obligations for reporting incidents to their management boards and other interested parties, such as the Information Commissioner's Officer and Government Security Group.

Note: This should consider legislation including the general data protection regulation (GDPR)

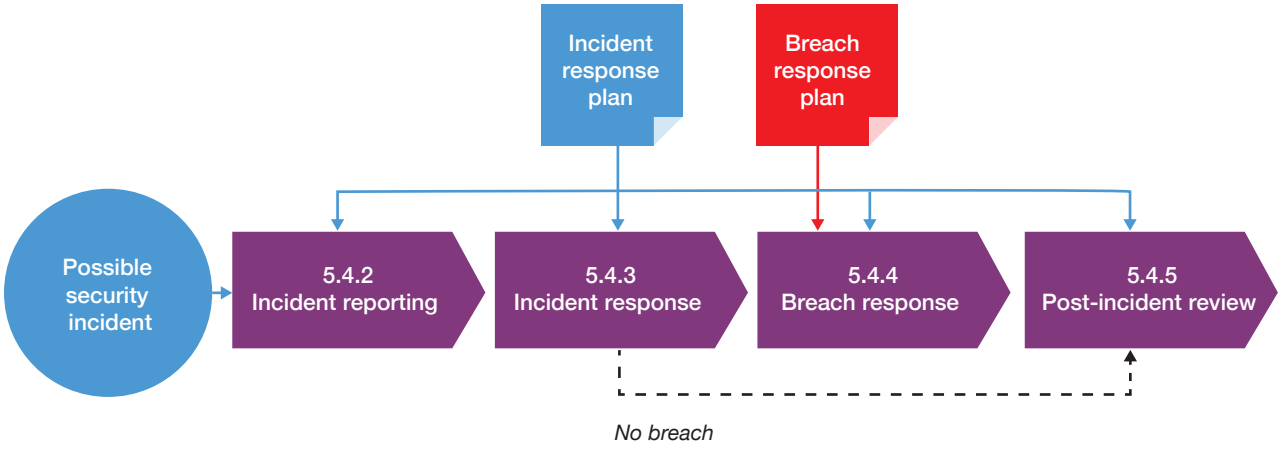

Figure 4 Steps in security incident management

Note: See Annex C for a description of technical security standards.

5.4.3 Incident response

The incident manager should handle the response to any security incident in accordance with the incident management plan (5.3.2), including taking action on failures of personnel to comply with security policies and procedures. Any lessons learned and updating of procedures shall be recorded (see 5.5).

5.4.4 Breach response

Any security breach should be assessed, categorised in terms of type and impact, and its cause determined. Incident investigations and the reporting of breaches should be recorded in detail and reviewed regularly. The incident manager should handle a security breach in accordance with the relevant breach response plan (5.3.3). Where no plan exists, one should be developed.

5.4.5 Post-incident review

Incidents should be reviewed and the incident response plan updated to include any learning to ensure that the same incident or breach cannot be repeated. Identified vulnerabilities should be remediated and degree of risk should be reassessed. Organisations should implement necessary changes to its security governance and management framework, or insure training that would prevent further occurrences.

The incident manager should handle the response to any security incident in accordance with the incident response plan, including taking action on failures of personnel to comply with security policies and procedures. Any lessons learned and updating of procedures shall be recorded.

5.5 Review and learn from experience

Learning from experience helps to avoid repeating the same mistakes and helps spread improved practices to benefit current and future security arrangements.

Lessons should be continually captured from all levels of the organisation, evaluated and action should be taken to mitigate risk and facilitate continual improvement of security practices at cross-government and organisational levels.

6 Security practices

6.1 Critical assets and services

Organisations shall identify and catalogue both the critical assets (including information) they hold and the key operational services they provide, so that they are aware of their existence and can take the necessary mitigating action. This includes understanding the technologies used and other dependent services (such as power, cooling, data) and the impact of any loss of service.

6.2 Risk management

Understanding risk helps government organisations to make informed, practical decisions, enabling business continuity and resilience.

Government organisations shall establish policies, processes and capabilities to enable understanding of the risks to the organisation, its people, assets and the services it provides. That understanding should be achieved through risk assessment, relevant to each organisation's own context, by skilled people using appropriate mechanisms, and by the establishment of risk appetites.

Responsibilities for risk management and associated decision-making shall be defined, with the Accounting Officer holding overall accountability and ensuring that practical direction is set on what aspects of the organisation and its activities and services are to be protected, and articulating risk appetites in terms of the level of acceptance of risk in respect of those aspects. The Accounting Officer may delegate responsibility to make decisions on the identification and management of risks, with identified risk owners.

6.2.1 Organisational risk management framework

Policies and processes shall be in place to acquire capabilities to regularly conduct risk and vulnerability assessments, and to review resilience planning for critical assets (see 6.1), particularly those identified as critical national infrastructure. Security processes should be designed and operated to mitigate the identified risks within agreed tolerances, and to keep pace with security risks as the threat and delivery landscape changes. Planning and testing processes and controls should be designed and operated to identify and inform risks and risk management.

Organisations shall be familiar with how the National Technical Authorities (the National Cyber Security Centre, Centre for the Protection of National Infrastructure [7], and UK National Authority on Counter-Eavesdropping) can help identify and manage risk, and should work with the Government Security Profession to identify, source and support the skilled resources needed.

6.2.2 Risk assessment

Organisations should periodically undertake a risk assessment of their information and services to identify possible threats and their range of consequences. Preventative measures should be developed to:

- mitigate the risk of a security breach occurring
- prevent further occurrences or reduce the impact of the breach

Buildings, systems and processes should be designed to incorporate features that are designed to avoid or prevent security breaches. See also GovS 004: Property.

6.2.3 Business continuity

Security objectives should be taken into account in an organisation's business continuity plans and processes, so that a security failure or compromise does not lead to unwarranted loss of operations or service.

6.3 Access to information

Organisations should implement protective security measures to mitigate insider threat across government and ensure consistency and efficiency between government organisations.

Those working on government business shall be made aware of the correct procedures and policies for handling sensitive information and appropriate security classification policies [6]. Access to classified, sensitive or critical information and key operational services should only be provided to identified, authenticated and authorised users or systems and proportionate risk mitigation controls should be applied. A list of users with access to information or key operational services should be known and continually managed as part of business continuity planning (see 6.3).

Information assets shall be classified according to HMG classification policy [5].

6.4 Capability, capacity and resources

Capability, capacity and resources management balances the supply and demand for appropriate resources (such as people, equipment, material and facilities) that can be deployed when needed. Resources might be sourced from within government, by recruiting or from the supply chain, using the GovS 003: Human Resources and GovS 008: Commercial standards.

A comprehensive view of future resource needs to address security vulnerabilities, and responses should be developed and maintained, with possible shortfalls identified and addressed. Resources should be secured or developed to meet the planned needs; if insufficient resources are available, work should be re-planned to reflect such constraints.

6.5 Security culture

A security culture with unambiguous personal accountability and an understanding of managing risk, responsibility and reputation should enable the government to function effectively.

Government organisations shall have:

- a security culture publicised and lead by example from the top of organisations, with the Accounting officer (or equivalent in an arm's length body) and executive board following the relevant processes and policies
- an open dialogue on security including encouraging the reporting of near misses to facilitate lessons learned

6.6 Security education and awareness

Security education and awareness activities are intended to ensure that members of the workforce are aware of and understand the organisation's security policies, processes, systems and controls; thereby helping to mitigate the risk of staff being responsible for data breaches and other security incidents and ensuring that business objectives are delivered safely and securely. Security education and awareness activity should include a combination of:

- induction material and programmes for employees and contractors
- periodic education and awareness events and campaigns for employees and, where appropriate, contractors on matters of importance to the secure delivery of business objectives
- continuously available Security Education and Awareness products to support locally led initiatives
- specific training and briefings for particular audiences.

Organisations shall ensure that new joiners have immediate access to induction material and core learning on security responsibilities and obligations. Induction should include, but not be limited to:

- the necessary policies and processes to be followed; the availability of facilities and tools appropriate to the role being undertaken
- a formal briefing on why and how security is important to the organisation and the particular role concerned
- early and on-going training required
- the granting and review of appropriate access to information and other systems in accordance with the role undertaken and the level of security clearance granted.

Organisations shall have in place an on-going and regularly reviewed and updated programme of Security Education and Awareness activities, tied to the attainment of business objectives and in line with security policies. The programme should include: appropriate threat briefings, other communications and learning materials for senior officials, line managers and other generic audiences; and specific briefings and learning materials for more specialist audiences with particular exposures, needs and security obligations.

Education and awareness activities should highlight personal accountability and encourage appropriate security behaviours, with incentives to deliver this tied to the organisation's HR policies and procedures. Communications and monitoring shall be in place to ensure all staff undertake mandatory training courses, briefings or e-learning; and these should be supported by management intervention, reporting and assurance.

GovS 003: Human Resources, should be followed, in support of this area of activity, guided by the security profession.

6.7 Physical security

Appropriate physical security measures [1] shall ensure a safe and secure working environment for staff and visitors, protecting them against a wide range of threats (including theft, terrorism or espionage). Organisations should implement layered security measures at government occupied buildings comprising multiple security measures that complement each other, provide a proportionate degree of protection against diverse threats, and offer a contingency in the event of one measure failing.

Physical security measures should consider, but not necessarily be limited to:

- building physical security into designs of buildings to protect assets and enable modern ways of working
- designing a layout that mitigates the risks of having vulnerable space at the base of the building
- implementing protective and preventative measures to reduce the likelihood of damage and injury being caused to assets, whilst ensuring adherence to UK building regulations

Government organisations shall have:

- processes and plans in place to determine the appropriate physical security requirements through risk assessment
- mechanisms to implement internal and external security controls in a layered fashion that deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack
- controls for controlling access and proximity to the most high-risk sites and Critical National Infrastructure assets

Consideration should be given to the physical environment in which civil servants and contractors operate. This is likely to include those areas on the front line, including the reception or receiving areas of any government building that protect publicly available spaces. It also encompasses staff working areas in OFFICIAL and above working spaces. Consideration should be given to specific security control rooms and guard force areas. To ensure the effective running of government business security of storage facilities shall be considered and appropriate controls around mail or deliveries applied. To manage risks to an organisation measures to protect people and assets from an intruder should be in place as well as vehicle management to protect against vehicles being used as a weapon.

Those managing government property shall comply with GovS 004: Property.

Note: See Annex C for a description of technical security standards.

6.8 Personnel security

Government organisations shall deliver the appropriate combination of recruitment checks, security vetting and on-going personnel security aftercare to reduce the risk from insider threat [1].

Government organisations shall have consistent HR and personnel security policies and processes, including recruitment checks in accordance with national security vetting: clearance levels [2]. Prospective employees shall be subject to pre-employment screening checks and, where necessary, vetting. New staff, or those new to a role should undergo a risk-based assessment for their suitability. Security clearances should be maintained and verified on an on-going basis, and where necessary, withdrawn. Processes in place to ensure staff are aware of their obligations under the Civil Service Code and their responsibility to the Official Secrets Act (1989), and that breaches can result in disciplinary action.

Processes should be put in place to define:

- the basis for risk-based decisions to allow employees to undergo the national security vetting in parallel to check against the baseline personnel security standard
- the basis for which clearance level different job roles require
- how vetting assessment, recommendations and decisions should be recorded and reported
- the approach to maintaining clearances, including the Annual Security Appraisal Form (ASAF) for Developed Vetting (DV) cleared employees
- the process by which clearance levels are reviewed, and particularly when staff move into new roles
- the approach to handling refusal or withdrawal of clearances, both for candidates at the recruitment stage and those already in employment
- the process by which security clearances are transferred to another government organisation, when an employee moves

Consideration should be given to the risk assessment of all individuals working on government business to limit the threats posed from insiders. This is likely to include risk assessment of roles, security considerations during recruitment, security assurance of individuals throughout their time within the organisation and alignment of organisational policies with security to outline expectations of staff in matters such as, though not limited to, travel overseas, use of information technology or use of social media. Exit procedures should also be in place to limit the risk of staff damaging the organisation upon exit.

Those managing personnel shall comply with GovS 003: Human Resources.

Note: See Annex C for a description of technical security standards.

6.9 Cyber security

The security of information and data is essential to good government and public confidence. To operate effectively, the UK government needs to maintain the confidentiality, integrity and availability of its information, systems and infrastructure, and the services it provides. Organisations that handle government data and information shall meet the standards prescribed by HM Government [1 and 6].

Government organisations shall have:

- an understanding, by all staff, of the expectations the organisation makes of them for the proper protection of information (including partner information) and understand where to seek help if they are unsure
- processes in place to identify and protect core assets and systems delivering essential functions

Organisations should take steps to detect cyber attacks and should have a defined, planned and tested response to such incidents, especially when they impact sensitive information or key operational services.

Systems that handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities. Highly privileged accounts should not be vulnerable to known cyber-attacks.

There should be a statement of assurance for all projects that shows evidence of assessing information risks and the controls put in place. Organisational boards assessing risk should have the information to be able to identify major projects that have high-information security risks. The organisation has clear information security guidance and standards available to new projects. Organisations should have managed, risk-informed security controls to mitigate applicable risks while deterring, detecting and protecting against malicious or negligent behaviour.

Due consideration should be given to the protection of enterprise technology within an organisation, and ensure that any infrastructure is not vulnerable to common cyber-attack. Cyber security also comprises the protection of end-user devices and email used throughout the organisation. Due consideration should also be applied to the protection of digital services operated by an organisation and cyber threats such as, though not limited to, identity theft, breaches of access and intellectual property theft.

Note: See Annex C for a description of technical security standards.

6.10 Technical security

Technical security relates to the protection of security systems from compromise and/or external interference that might have occurred as a result of an attack. Government organisations should have:

- policies and processes to control the use of mobile devices in sensitive areas
- staff awareness of the risks of using personal devices in government buildings
- security management processes that facilitate staff to conduct sensitive conversations and meetings in an appropriate environment
- processes to maintain the technical integrity of the government estate
- security managed estate improvement plans to mitigate the compromise of the building structure from close access or standoff attack

A. References

ID	Description
1	Government Security Group, Technical security standards – for physical, personnel, cyber security and incident management (2018)
2	Ministry of Defence and United Kingdom Security Vetting, National security vetting: clearance levels (2020)
3	Government Security Group, Roles and responsibilities **https://www.gov.uk/government/publications/government-security-roles-and-responsibilities**
4	Government Security Group, Security Policy Framework (2018)
5	Government Security Group, Departmental Security Health Check (2016)
6	Government Security Group, HMG Government Security Classifications Policy (2018)
7	National Cyber Security Centre, Advice and guidance **https://www.ncsc.gov.uk/section/advice-guidance/all-topics**

B. Glossary

Term	Definition
Compromise	In the context of security, compromise is bringing an asset (including people, property or information) into disrepute or danger.
Critical national infrastructure	Those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends.
Cyber security	Protective cyber security measures put in place to mitigate against the consequences of an external cyber attack on government information, personnel or infrastructures.
Developed Vetting	A level of security clearance which allows unsupervised access of material up to and including “SECRET” on a regular basis.
Insider threat	The threat posed by staff, contractors or contracted third parties not following or deliberately disregarding established policies.
Personnel security	Personnel security is the practice of ensuring the security of government information and infrastructure against threats arising from government personnel.
Physical security	Physical security is the practice of protecting elements of government infrastructure, estates and personnel against attacks or compromises in the physical (i.e. tangible, real-world) environment.
Prevention (security)	In the context of security, prevention is the action of stopping a security incident arising.
Property	Land, buildings, infrastructure or facilities held in any form of tenure.
Protective security	The term used to define physical, personnel, cyber and technical security working in concert to protect an organisation and its assets.
Risk appetite	The amount of risk the organisation, or subset of it, is willing to accept.
Risk tolerance	The threshold levels of risk exposure that, with appropriate approvals, can be exceeded, but which when exceeded will trigger some form of response (e.g. reporting the situation to senior management for action).
Security breach	A security breach is the confirmed compromise of government assets without permission or authority. This includes people, property or information.
Security incident	A security incident is any circumstance that has arisen contrary to policy and that has the potential to compromise government assets. This includes people, property or information.
Security threat	A possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.
Security vulnerability	A weakness that could be exploited by an adversary.
Service catalogue	A list of operational security services that Cluster Security Units provide to their clustered organisations.

C. Subject specific security standards

This functional standard is underpinned by four subject specific standards which define the requirement for physical, personnel, cyber security and incident management [3]. As far as possible the security standards define outcomes, allowing organisations flexibility in how the standards are implemented, dependent on their local context. The definition of 'important' and 'appropriate' are deliberately left open, so that organisations can apply their own values based on their particular circumstances. An organisation's leaders are accountable for the effectiveness of these decisions.

Physical technical security standard

This document provides a specification for the layered security measures expected to be delivered as standard at a government-occupied building. Consideration should be given to the physical environment in which civil servants and contractors operate. This is likely to include those areas on the front line, including the reception or receiving areas of any government building that protect publicly available spaces. It also encompasses staff working areas in OFFICIAL and above working spaces. Consideration should be given to specific security control rooms and guard force areas. To ensure the effective running of government business security of storage facilities must be considered and appropriate controls around mail or deliveries applied. To manage risks to an organisation measures to protect people and assets from an intruder should be in place as well as vehicle management to protect against vehicles being used as a weapon.

Personnel technical security standard

This document provides organisations with details of the minimum personnel security standards which, when met, will mitigate against the insider threat across government and ensure consistency and efficiency among organisations.

Consideration should be given to the risk assessment of all individuals working on government business to limit the threats posed from insiders. This is likely to include risk assessment of roles, security considerations during recruitment, security assurance of individuals throughout their time within the organisation and alignment of organisational policies with security to outline expectations of staff in matters such as, though not limited to, travel overseas, use of information technology or use of social media. Exit procedures should also be in place to limit the risk of staff damaging the organisation upon exit.

Cyber-security technical standard

This document defines the minimum security measures that organisations are required to implement with regards to protecting their technology and digital services to meet their security obligations. Compliance with this standard can be achieved in many ways, depending on the technology choices and business requirements in question. For digital services, this set of standards is complementary to the Digital Service Manual. Consideration should be given to the protection of enterprise technology within an organisation and ensuring that any infrastructure is not vulnerable to common cyber attack. Cyber-security also comprises the protection of end user devices and email used throughout the organisation. Consideration should also be applied to the protection of digital services operated by an organisation and cyber threats such as, though not limited to, identity theft, breaches of access and intellectual property theft.

Incident management standard

This document defines the minimum measures that organisations are required to implement with regards to managing security incidents. In all cases relevant guidance should be followed.