HM Government

Government Functional Standard

GovS 007: Security

Version: 2.0
Date issued: 13 September 2021

Approved

This functional standard is part of a suite of management standards that promotes consistent and coherent ways of working across government, and provides a stable basis for assurance, risk management and capability improvement.

The suite of standards, and associated guidance, can be found at **GOV.UK government functional standards**.

Functional standards cross-refer to each other where needed, so can be confidently used together.

They contain both mandatory and advisory elements, described in consistent language (see the 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.

Version 2.0 of this standard replaces the previous edition V1.0 dated July 2020. The main changes, which reflect input from users of the previous version, are as follows:

- a substantial improvement of the incident management section
- a greater inclusion of aspects of risk and threat throughout
- a stronger technical security section

Produced by Government Security Group

Contents

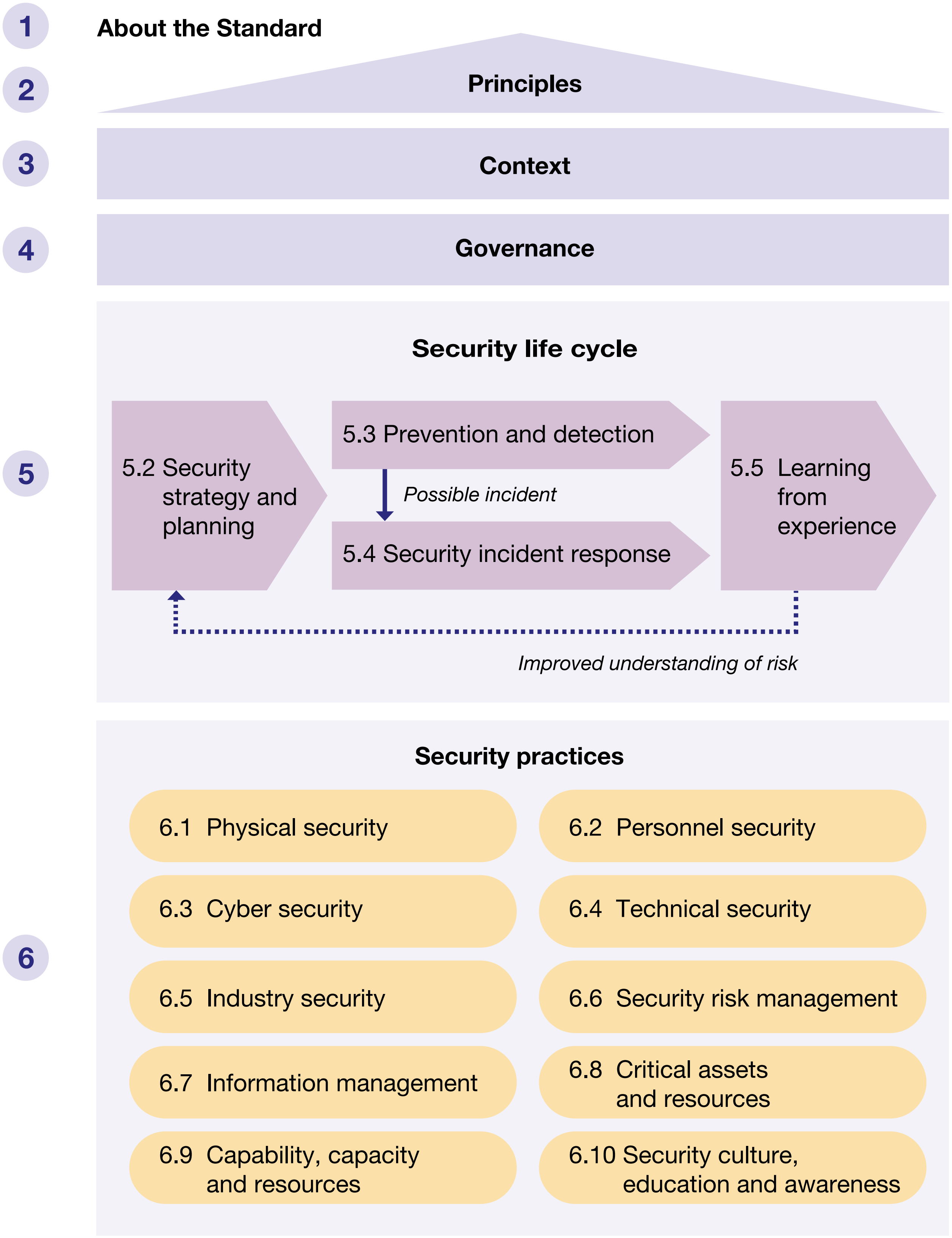
1
About the Standard
2
Principles
3
Context
4
Governance
5
Security life cycle
5.2 Security strategy and planning
5.3 Prevention and detection
Possible incident
5.4 Security incident response
5.5 Learning from experience
Improved understanding of risk
6
Security practices
6.1 Physical security
6.2 Personnel security
6.3 Cyber security
6.4 Technical security
6.5 Industry security
6.6 Security risk management
6.7 Information management
6.8 Critical assets and resources
6.9 Capability, capacity and resources
6.10 Security culture, education and awareness

Figure 1 Scope of this functional standard

1 About this government functional standard

1.1 Purpose of this government standard

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

- the government's assets (people, property and information)
- 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, to ensure the right environment for effective delivery and performance
- security advisers and other named security officials
- those responsible for communicating security information to government staff and visitors
- those working within and for the government, who have a responsibility to ensure security practices are followed (including staff, third party suppliers and members of the armed forces)

Note: this standard replaces the Security Policy Framework. The policies which sit within that framework remain in effect but are now in support of this standard.

1.2 Scope of this government standard

This standard applies to the planning, delivery and management of government security activities. It includes risk management, planning and response for physical, personnel, cyber and technical security in departments and their arm's length bodies, as well as industry [1 and 2]. Other public sector organisations, devolved or local, may find this standard useful.

Note: an organisation, in the context of government functional standards, is the generic term used to describe a government department, arm's length body, or any other entity that is identified as being within scope of a functional standard.

The structure of the standard is shown in Figure 1.

1.3 Government standards references

The following standards are directly 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

A functional standard supports achievement of the outcomes sought by an organisation. It sets expectations for what needs to be done and why, relating to the functional work within its scope, in order to achieve those organisational outcomes.

Note: for expectations relating to management of a function across government and management of functional standards, please see GovS 001, Government functions.

2 Principles

Those engaged in the management of government security shall ensure:

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

3 Context

3.1 Introduction

This section provides essential background information for the use of this functional standard.

3.2 Overview of security

The Prime Minister is ultimately responsible for the security of HM Government. The Prime Minister 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 oversees government security at the direction of the Government Security Board and is responsible for the development of good practice in relation to security.

The Government Security Group is distinct from the Cabinet Office's National Security Secretariat, 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, Cross-government, Government Security Centre and Organisational (departments and arm's length bodies).

3.3 Integrated protective security

Protective security comprises four interconnected domains, through which attacks are perpetrated: physical, personnel, cyber and technical. Although they are considered as separate domains, they rarely occur in isolation and are treated holistically.

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

Personnel security is the practice of ensuring the security of government information and infrastructure against threats arising from government personnel, others working to government and those who formerly worked in HM Government circles. This could include deliberate attacks, criminal activity for profit, unmalicious and unwitting insider threat, 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) environments. Such individuals could join government service intending to commit such acts, or decide to do so after employment [1].

Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from the deliberate and inadvertent exploitation of computer systems, technology-dependent enterprises and networks [2].

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.

Government security also includes the protective security arrangements of industry partners that provide goods and services to government or which hold government or international partners' classified information. This is described in government security as 'industry security' (see 6.5 for more detail).

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

4 Governance

4.1 Governance and management framework

4.1.1 Overview

Governance comprises prioritising, authorising, directing, empowering and overseeing management, as well as assuring and reviewing performance.

A governance and management framework shall be defined and established for the management of security across government as a whole, and in government organisations.

The governance and management framework should include the authority limits, roles and rules for making business decisions, degrees of autonomy, assurance needs, reporting structure, accountabilities and responsibilities, together with the appropriate management practices, processes and associated documentation needed to meet this standard.

4.1.2 Cross-government management

The cross-government governance and management framework should include cross-government security policies, to set expectations for managing security in order to protect UK government assets (people, information and property). 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 governance and management 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

The governance of security-related activities within an organisation should be an integrated part of that organisation's overall governance, to align security objectives and requirements with the organisation's strategic aims and delivery objectives.

Each organisation's governance and management framework shall cover physical, personnel, cyber, incident management, technical and industry security [1 and 2].

The governance and management framework should cover the practices described in this functional standard.

Security management frameworks should be responsive to new and changing circumstances and reflect actual and emerging security threats as well as including how organisations should manage risk (see 6.6). 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 4.4.5)
- a senior officer accountable for security (see 4.4.6)

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

The purpose of assurance is to provide, through a systematic set of actions, confidence to senior leaders and stakeholders that work is controlled and supports secure and successful delivery of policy, strategy and objectives. Organisations shall comply with mandated cross-government assurance activities as coordinated by the Cabinet Office.

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.

Organisations should have a defined and established approach to security assurance, which should be applied proportionately to the risk and value of the activity, and integrated with the organisation's overall assurance framework. Typically, assurance should be on at least three separate and defined levels including:

- 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) to 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 disruption to other work, avoiding overlaps with other assurance activities and duplication of effort, whilst remaining rigorous and meeting the needs of stakeholders.

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

The requirements of the Orange Book: management of risk - principles and concepts, shall be met [3].

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. 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

GovS 003, Human Resources shall be followed.

4.3 Decision making

Decisions should be made and approvals given in a timely manner in accordance with the organisation's security governance and management framework (see 4.1.3). Government standards and policy should be complied with. Decisions should be made by assessing options against defined criteria and in consultation with stakeholders and subject matter experts. Decisions should relate to:

- setting policy for security across the government, security centre 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
- responding to events, incidents or crises

Analysis shall be undertaken in accordance with GovS 010, Analysis.

4.4 Roles and accountabilities

4.4.1 Overview

Roles and accountabilities shall be defined in the relevant governance and management framework and assigned to people with appropriate seniority, skills and experience. This should include, but is not limited to, the activities, outputs or outcomes they are responsible for, and the person they are accountable to.

Note: for more detail on roles, see also [4].

4.4.2 Senior officer accountable for security across government

This role 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 the senior accountable officer should:

- define and establish the cross-government security strategy and cross-government policy and standards
- monitor performance against policy and standards
- provide guidance and direction to the senior security role holders, when requested
- respond to serious and/or cross-government security incidents or issues
- define the groups of organisations for which coordinated management of security is necessary (see 4.4.3)

Note: this role also leads the Security function across government and is currently known as the Government Chief Security Officer.

4.4.3 UK National Technical Authorities

Organisations draw on expert advice and support in the four domains of security from the UK National Technical Authorities: the Centre for the Protection of National Infrastructure on physical and personnel security; the National Cyber Security Centre on cyber security; and UK National Counter-Eavesdropping on technical security.

Note: defined groups of organisations clustered together for security management are known as Government Security Centres.

4.4.4 Accounting officer

The permanent head of a government department is usually its Principal Accounting Officer.

An organisation's Accounting Officer is accountable (via a Principal Accounting Officer where appropriate) to Parliament and the public for the stewardship of public resources, ensuring they are used effectively in the arm's length bodies within the department's ambit as an 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.

4.4.5 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 (see 6.5).

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).

4.4.6 Senior officer accountable for security in an organisation

This role 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
- ensuring an effective relationship between the organisation and those coordinating wider security provision (see 4.4.3)
- 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
- 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 Government Security Centres (see 4.4.3) and ensuring the requirements of their organisation are being met to agreed standards and service level agreements.

4.4.7 Senior officer responsible for security information in an organisation

This role is accountable to the senior officer accountable for security in an organisation for:

- advising the organisation's board on how to balance the needs of security and exploitation of technology to deliver the organisation's strategic objectives, and provide strategic leadership for the organisation's cyber and information security community and its investment in security technology
- developing and maintaining the organisation's security strategy, security architecture, policies and standards, technology assurance and professionalism
- supporting the senior officer accountable for security in requesting seniors from the cyber security centre

Note: Some departments may adopt the model of the senior officer responsible for security information in an organisation being accountable to the senior officer for security or to the Accounting Officer.

4.4.8 Incident manager

The incident manager is accountable to the senior officer accountable for security in an organisation (see 4.4.6) for the management and resolution of an incident and any subsequent breach, in particular assessing:

- the type of incident
- the risk and impact to the organisational assets
- any commercial or supply chain considerations
- implementation of plans to respond to the incident
- investigating how the incident occurred and providing lessons learned

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.

4.4.9 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 officers, crypto custodians, intelligence handling coordinators, physical security controllers, Facility Security Clearance (List X), personnel security controllers and board level contacts.

5 Security life cycle

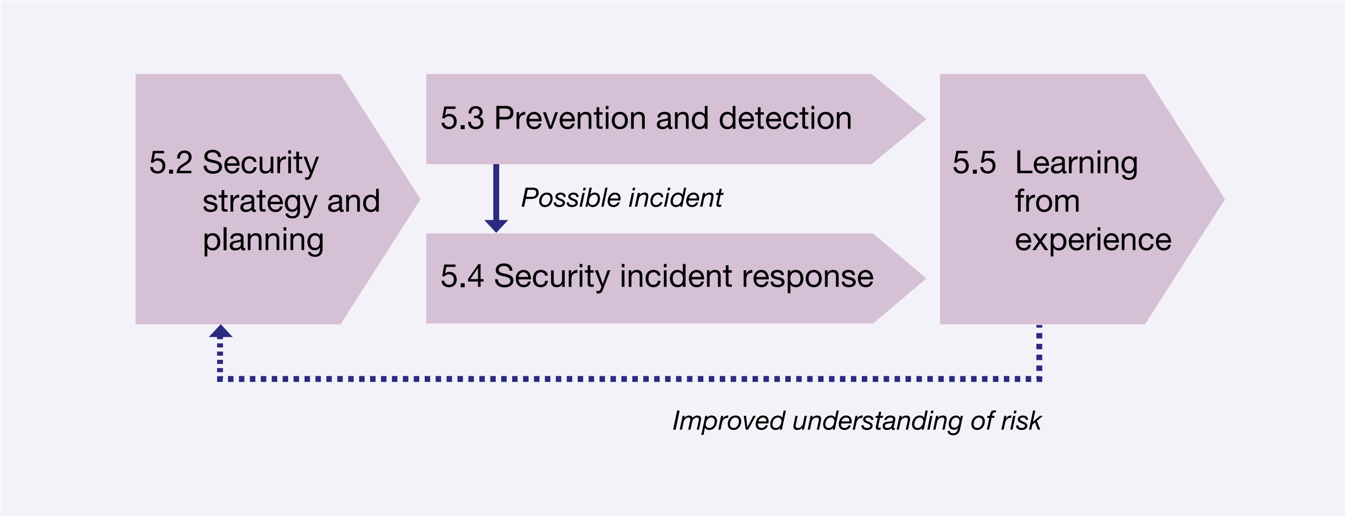
5.2 Security strategy and planning
5.3 Prevention and detection
Possible incident
5.4 Security incident response
5.5 Learning from experience
Improved understanding of risk

Figure 2 Security life cycle

5.1 Overview

The security life cycle includes strategy and planning, prevention and detection, incident management and reviews from lessons learned. See Figure 2.

Holistic management of security helps prevent security incidents and makes it easier to respond and learn lessons about how to improve. The management of security should bring together consideration of physical security (see 6.1), personnel security (see 6.2), cyber security (see 6.3), technical security (see 6.4) and industry security (see 6.5).

5.2 Security strategy and planning

5.2.1 Overview

Organisations should align their security strategies with the Cross-Government Security Function Strategy. 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.

5.2.2 Security response plans

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 and in the incident management technical standard
- 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

Security response plans 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 that ensure shared communications between human resources and security teams. The structures shall 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 Prevention and detection

5.3.1 Security arrangements

Organisations should undertake a regular holistic assessment of the security arrangements that they have in place and assess whether these remain appropriate to the organisation's specific requirement. 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 through clearly defined routes.

5.4 Security Incident Response

5.4.1 Incident reporting

A security incident, 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: consider legislation including the General Data Protection Regulation (GDPR).

5.4.2 Incident response

The incident manager should handle the response to security incidents in accordance with the organisation's security response plans (see 5.2.2), including taking action on failures of personnel to comply with security policies and procedures. Lessons learned and updating of procedures shall be recorded (see 5.5).

5.4.3 Post response review

Following events, incidents or crisis situations, the organisation's response should be reviewed and the security response plan updated to include learning that can streamline the response process and to ensure that the same situation cannot be repeated. Identified vulnerabilities should be remediated and degree of risk should be reassessed. Organisations should implement necessary changes to their security governance and management framework or training that would prevent further occurrences.

5.5 Learning from experience

Learning from experience avoids 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, holistically evaluated, and action taken to mitigate risk and facilitate continual improvement of security practices at cross-government and organisational levels.

6 Security practices

6.1 Physical security

The purpose of physical security measures is to ensure a safe and secure working environment for staff and visitors, protecting them against a wide range of threats (including theft, terrorism and espionage). Organisations should implement layered security measures in any government property or government supplier property that has government classified information, assets or people. These measures should 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:

- integrating 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
- measures 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, crown servants, military personnel and contractors operate. 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.

Government contractors processing or storing classified material on their own premises at SECRET or above shall be considered for Facility Security Clearance (List X) accreditation.

Buildings, systems and processes should be designed to incorporate features that are designed to avoid or prevent security incidents. GovS 004, Property shall be followed.

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

6.2 Personnel security

The purpose of personnel security is to assure the government that the people it employs are suitable for work in sensitive roles. It also safeguards employees from exploitation as a result of their personal circumstances.

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 [7]. 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 shall be 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 rationale for the relevant level of security clearance for different roles
- how vetting assessment, recommendations and decisions should be recorded and reported
- the approach to maintaining clearances, including the Annual Security Appraisal Form for Developed Vetting cleared personnel
- 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 for both 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.

Government contractors with employees that hold security clearances to SECRET or above should be considered for Industry Personnel Security Assurance accreditation [8]. GovS 003, Human Resources shall be followed.

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

6.3 Cyber security

The purpose of cyber security is to ensure the security of data and information. 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 [2].

All organisations using this standard 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 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 deliver key operational services shall be protected from exploitation of vulnerabilities. Highly privileged accounts should not be vulnerable to cyber-attacks.

There should be a statement of assurance for all projects that shows evidence of assessing information and cyber 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 and cyber security risks. The organisation should have clear information and cyber 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 ensuring that 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 cyber security standards.

6.4 Technical security

The purpose of technical security measures is to holistically protect sensitive information and technology from close access acquisition or exploitation by hostile actors, as well as any other form of technical manipulation. Technical security also relates to the protection of security systems from compromise and/or external interference. Government organisations shall have:

- policies and processes to control the use of mobile devices in sensitive areas
- staff awareness about 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, including the potential compromise of electromagnetic and other emanations
- security managed estate improvement plans to mitigate the compromise of the building structure from close access or standoff attack

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

6.5 Industry security

The purpose of managing industry security is to protect the government from threats relating to contractors and suppliers having access to classified information, assets and estates, all of which are vulnerable to compromise by adversaries.

The aims and intent of this standard are applicable to government contractors that access (or protect) classified information and assets, or employ staff with National Security Vetting clearances. The applicability and specific mandatory requirements for government contractors are identified in supplementary documents including: Security Requirements for Facility Security Clearance (List X) Contractors, Industrial Security Departmental Responsibilities, Contractual Process and the Industry Personnel Security Assurance policy.

Security threats to the government that seek to exploit vulnerabilities in industry security should be identified and risks assessed throughout the life-cycle of a contract, beginning before contracts are let. Appropriate security clauses should be added to contracts. To facilitate this, organisations shall:

- develop a culture whereby individuals understand that mitigating threats in industry is a collective responsibility whilst contract managers are responsible for the security of their assigned suppliers
- take a holistic approach to supplier assurance that considers and mitigates the risks posed to physical, personnel and cyber security
- set and communicate minimum contractual security requirements to suppliers.
- conduct frequent assurance to verify that security measures are being met and remain adequate
- build security considerations into departmental contracting processes, including the requirement for suppliers to notify contract managers of security incidents or changes to the security profile of their organisation
- ensure procurement is at the most suitable classification and suppliers abide by Facility Security Clearance Assurance (List X) and Industry Personnel Security Assurance policies if applicable

Organisations should meet the relevant commercial and industrial security policies prescribed by HM Government [5]. See also GovS 008, Commercial.

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

6.6 Security risk management

6.6.1 Defining and establishing risk management procedures

The purpose of security risk management is to understand security risks, which helps government organisations reduce the opportunities for threat actors to cause harm to government assets.

Government organisations shall establish policies, processes and capabilities to enable understanding of the risks to the organisation and its assets - including its people, information, the services it provides and the customers of those services. 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.

6.6.2 Organisational risk management

Organisations shall have policies and processes in place to conduct regular risk and vulnerability assessments for their organisations and their assets. Preventative measures should also be developed to:

- mitigate the risk of a security incident occurring
- prevent further occurrences
- reduce the impact of incidents

This includes reviewing resilience planning for critical assets, in particular, those identified as critical national infrastructure (see 6.8).

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 vulnerability 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 [6], and UK National Authority on Counter-Eavesdropping) can help identify and manage risk. Similarly, they should be familiar with the assistance the Government Security Centres can provide. They should work with the Government Security Profession to identify, source and support the skilled resources needed.

Organisations should establish a system for identifying security risks in a register, and for exposing these risks to the appropriate governance boards for review at appropriate intervals.

6.6.3 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.

6.7 Information management

The purpose of information management is to implement protective security measures that mitigate insider threat across government and ensure consistency and efficiency between government organisations.

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.

Information assets shall be classified according to HM Government classification policy.

All organisations using this standard shall have:

- an understanding of their policies and processes to protect sensitive data holdings
- policies, systems and processes for information handling that are compliant with HM Government information security policies and standards and relevant legislation and regulations, such as the Data Protection Act 2018 and the Public Records Act 1967
- regular training and education for all staff, and contractors who handle government information, on appropriate information security measures, including refresher training. Through proper education and awareness provisions, organisations should ensure that users are able to understand and comply with both their department's local policies and wider government policies

These information security policies should be kept up to date and should cover:

- the classification of information
- processes for the appropriate handling, storage, sharing, and destruction of information based on its marking
- systems and processes for protecting information when working remotely
- roles and responsibilities in the information handling chain
- if an organisation shares information with international partners, it shall have policies and processes in place to securely manage international classified exchanges that are compliant with government policies and standards

6.8 Critical assets and services

The purpose of critical assets and services is for organisations to identify and catalogue the critical assets (including information) they hold and 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, other dependent services (such as power, cooling, data), the supply chain implications and the impact of loss of services.

6.9 Capability, capacity and resources

The purpose of capability, capacity and resource management is to balance 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 the government, through recruitment or from the supply chain. GovS 003, Human Resources and GovS 008, Commercial shall be followed.

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.

Organisations should call upon the advice available to them across each area of government security through the Government Security Centres.

6.10 Security culture, education and awareness

The purpose of security culture, education and awareness is to enable the government to function effectively. This will be done through a security culture of unambiguous personal accountability and an understanding of managing risk, responsibility and reputation.

Organisations using this standard shall have:

- a security culture publicised and led 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

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. This will help to mitigate the risk of staff being responsible for data breaches and other security incidents and ensure 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 ongoing 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, as well as 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. These should be supported by management intervention, reporting and assurance.

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

A. References

All references are correct at the time of publication, users should check for updated versions.

ID	Description
	Government references
1	Government Security Group, *Government baseline personnel security standard* (2018)
2	Government Security Group, *Minimum Cyber Security Standard* (2018)
3	HM Treasury, *Orange Book: Management of risk – Principles and Concepts* (2020)
4	Government Security Group, *Government security roles and responsibilities* (2018)
5	Government Security Group, *Industrial Security Policies* (collection)
6	National Cyber Security Centre, *Advice and guidance*
7	Ministry of Defence and United Kingdom Security Vetting, *National security vetting: clearance levels* (2020)
8	Government Security Group, *HM Government Security Classifications Policy* (2018)

B. Glossary

See also the **common glossary of definitions** which includes a list of defined terms and phrases used across the suite of government functional standards. The glossary includes the term, definition, and which function owns the term and definition.

Term	Definition
assurance	A general term for the confidence that can be derived from objective information over the successful conduct of activities, the efficient and effective design and operation of internal control, compliance with internal and external requirements, and the production of insightful and credible information to support decision making. Confidence diminishes when there are uncertainties around the integrity of information or of underlying processes.
compromise	In the context of security, compromise is bringing an asset (including people, property or information) into disrepute or danger.
crisis (security)	In the context of security, a crisis is a direct threat or act against staff or assets that can or has caused a loss of life or critical business function.
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.
defined (way of working)	In the context of standards, defined denotes a documented way of working, which people are expected to use. This can apply to any aspect of a governance or management framework, for example processes, codes of practice, methods, templates, tools and guides.
developed vetting	A level of security clearance which allows unsupervised access of material up to and including “TOP SECRET” on a regular basis.
established (way of working)	In the context of standards, ‘established’ denotes a way of working that is implemented and used throughout the organisation. This can apply to any aspect of a governance or management framework, for example processes, codes of practice, methods, templates, tools and guides.
event (security)	In the context of security, an event is a disruptive but non-threatening organised event in your department or building, or an event in the public space, which requires security planning and mitigations to be put in place.
governance	Governance defines relationships and the distribution of rights and responsibilities among those who work with and in the organisation. It determines the rules and procedures through which the organisational objectives are set, and provides the means of attaining those objectives and monitoring performance. Importantly, it defines where accountability lies throughout the organisation.

Term	Definition
governance and management framework	A governance and management framework sets out the authority limits, decision making roles and rules, degrees of autonomy, assurance needs, reporting structure, accountabilities and roles, and the appropriate management practices and associated documentation needed to meet this standard.
incident (security)	In the content of security, an incident is any circumstance that arises where assets may be damaged, compromised, lost or leaked as a result of failure of policy or codes of conduct, existing security measures or controls, or something that requires an action/response following a direct threat or individual action, or to prevent one of the above. These could be accidental or deliberate acts by those internal or external to the department.
insider threat	The threat posed by staff, contractors or contracted third parties not following or deliberately disregarding established policies.
organisation	An organisation, in the context of government functional standards, is the generic term used to describe a government department, arm's length body, or any other entity that is identified as being within scope of a functional standard.
personnel security	The practice of ensuring the security of government information and infrastructure against threats arising from government personnel.
physical security	The practice of protecting elements of government infrastructure, estates and personnel against attacks or compromises in the physical (i.e. tangible, real-world) environment.
plan	A plan sets out how objectives, outcomes and outputs are to be delivered within defined constraints, in accordance with the strategy.
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, technical and industry 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 (for example, reporting the situation to senior management for action).
security breach	The confirmed compromise of government assets without permission or authority. This includes people, property or information.
security threat	A possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.

Term	Definition
security vulnerability	A weakness that could be exploited by an adversary.
service catalogue	A list of operational security services that Government Security Centres provide to their organisations.
strategy	An outline of longer term objectives, outcomes and outputs, and the means to achieve them, to inform future decisions and planning.

C Subject specific security standards

At the time of going to print, this functional standard is underpinned by six subject specific standards, which define the requirement for physical, personnel, cyber, technical, industry and incident management. 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.

Subject specific standard: Physical

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, government departments, all crown servants, and HM Government 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.

Subject specific standard: Personnel

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.

Subject specific standard: Cyber security

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 given 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.

Subject specific standard: Technical security

This document specifies the baseline requirements organisations must meet to mitigate against the threat of technical attack or accidental exposure of information. Compliance may be achieved in a variety of ways and consideration should be given to the organisational specific business context, location and techno-physical environment.

Consideration should be given to the range of targets susceptible to technical attack including, but not limited to, tangible physical and digital assets, as well as intangible assets such as sensitive conversations and phone calls, and electromagnetic emanations.

To manage the risks associated with technical security the range of approaches, including distanced standoff as well as both quick and deep plant close access, should be considered.

Technical security involves the lifecycle of an asset and should be considered through construction or purchase, use, and demolition or disposal. Use of both ongoing and targeted inspections by approved technical security professionals, security by design and active countermeasures is to be considered as a part of meeting technical security requirements.

Subject specific standard: Industry security

There are a number of supplemental documents relating to the security arrangements between contracting authorities and HM Government suppliers. Facility Security Clearance (List X) and Industry Personnel Security Assurance policies cater for the physical and personnel aspects of contracting at SECRET or above. These are joined by more general guidance on departmental responsibilities as well as policy on security in the contractual process. Separately, there is a Government Supplier Assurance Framework to provide departments with the tools and principles to manage supplier risk.

Subject specific standard: Incident management

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