|  |
| --- |
|  |
| ONR Technical Assessment Guide  Organisational Security Capability |



ONR Technical Assessment Guide (TAG)

Organisational Security Capability

Authored by: Nuclear Safety Inspector

Approved by: Superintending Security Inspector

Professional Lead: Superintending Security Inspector

Issue No.: 2.1

Publication Date: Sept-23

Next Major Review Date: Apr-27

Doc. Ref.: CNS-TAST-GD-1.2

Record Ref. No.: 2023/49110

Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 2.1 | Up-date to reflect relevant good practice in organisational capability assessment. |

Contents

[1. Introduction 4](#_Toc132375207)

[2. Purpose and Scope 4](#_Toc132375208)

[3. Relationship to Licence and other Relevant Legislation 5](#_Toc132375209)

[4. Relationship to IAEA Security Standards and Guides 6](#_Toc132375210)

[5. Advice to Inspectors 9](#_Toc132375211)

[References 21](#_Toc132375212)

[Glossary and Abbreviations 22](#_Toc132375213)

# Introduction

1. ONR has established its Security Assessment Principles (SyAPs) [1], which apply to the assessment by ONR specialist inspectors of security plans for nuclear facilities that may be operated by potential licensees, existing licensees, or other dutyholders. The SyAPs contain Fundamental Security Principles (FSyPs) and are supported by a suite of guides to further assist ONR’s inspectors in their security assessment work in support of making regulatory judgements and decisions. This Technical Assessment Guide (TAG) is one of these guides.
2. Duty holders must demonstrate that they have fully considered the FSyPs in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 [2].
3. A security plan is a term that covers all duty holder submissions, such as site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate on-going legal compliance for the protection of Sensitive Nuclear Information (SNI).

# Purpose and Scope

1. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgement during assessment activities relating to a dutyholder’s arrangements to develop and maintain its organisational security capability. It aims to provide general advice and guidance to ONR inspectors on how organisational security capability should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the detail or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder’s responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

# Relationship to Relevant Legislation

1. The term dutyholder is used to define responsible persons on civil nuclear licensed sites and other nuclear premises subject to security regulation, a developer carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.
2. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved transport security statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI.
3. ONR considers that an adequate organisational security capability is a key component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.

# Relationship to IAEA, Security Standards and Guides

1. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [3] and the International Atomic Energy Agency (IAEA) Nuclear Security Fundamentals [4]. Further guidance is available within the International IAEA Technical Guidance and Implementing Guides. Additional guidance is available from the World Institute for Nuclear Security (WINS) - Corporate Governance Arrangements for Nuclear Security [5].
2. Fundamental Principle F of the CPPNM refers to security culture and states that all organisations involved in implementing physical protection should give due priority to security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organisation. CNS-TAST-GD-2.1 Maintenance of a Robust Security Culture has more guidance on assessment of security culture [6].
3. Fundamental Principle I of the CPPNM refers to Defence in Depth, which includes layers of protection: structural, other technical, personnel and organisational.
4. The importance of issues relating to Governance and Leadership are also recognised in the Nuclear Security Fundamentals Essential Element 12: sustaining a nuclear security regime: A nuclear security regime ensures that each competent authority and authorized person and other organizations with nuclear security responsibilities contribute to the sustainability of the regime by:

* Developing, implementing, and maintaining appropriate and effective integrated management systems including quality management systems.
* Demonstrating leadership in nuclear security matters at the highest levels.
* Developing, fostering, and maintaining a robust nuclear security culture.
* Allocating sufficient human, financial and technical resources to carry out the organization’s nuclear security responsibilities on a continuing basis using a risk informed approach.
* Routinely conducting maintenance, training, and evaluation to ensure the effectiveness of the nuclear security systems.
* Having in place processes for using best practices and lessons learned from experience.
* Establishing and applying measures to minimize the possibility of insiders becoming nuclear security threats.
* Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times.

1. These Nuclear Security Essential Elements align with the ONR’s SyAPs Fundamental Security Principles (FSyP1) and Security Delivery Principles (SyDPs):

* FSyP1: **Leadership and Management for Security:** Dutyholders must implement and maintain organisational security capability underpinned by strong leadership, robust governance, an adequate management and accountability of security arrangements incorporating internal and independent evidence-based assurance processes.
* SyDP1.2: **Capable Organisation:** The organisation should have the capability to implement and maintain the security of its undertakings.

1. The Safety Assessment Principles (SAPs) and the following leadership and management for safety principles could equally apply to organisational security capability:

* MS1: **Leadership**: states that “Directors, managers and leaders at all levels should focus the organisation on achieving and sustaining high standards of safety and on delivering the characteristics of a high reliability organisation.”
* MS2: **Capable Organisation**: states that “The organisation should have adequate human resources. This includes having the necessary competences and knowledge in sufficient numbers to provide resilience and maintain the capability to govern, lead and manage for safety at all times.”

## Technical Assessment Guides (TAGs)

1. The following TAGs [6] are applicable to security and include relevant good practice in support of this TAG:

* **CNS-TAST-GD-11.4.6 – Managing Changes to Security Procedures and Arrangements**

This TAG addresses the management of changes to security procedures and arrangements. This includes any change to the organisational structure, staffing level and competencies, including any change to security posts covered in the Nuclear Baseline (NB), or equivalent. The NB, or equivalent, provides the basis against which any proposed organisational change can be assessed. It includes categorisation of changes to organisational nuclear security baseline posts.

* **CNS-TAST-GD1.1 - Security Governance and Leadership** –

This TAG addresses a dutyholder’s governance and leadership arrangements.

* **CNS-TAST-GD2.1 - Maintenance of a Robust Security Culture** This TAG addresses a dutyholder’s arrangements to develop and maintain a strong security culture.
* **CNS-TAST-GD3.2 - Sufficiency and Competence of Personnel Delivering Security** - This TAG addresses the dutyholder’s analysis of competence, number and organisation of personnel required to deliver nuclear security.

1. The following TAGs [6] are applicable to safety but contain relevant good practice that may read across into security to support duty holders in simplifying their management arrangements. They may be able to align safety and security processes and documentation:

* **NS-TAST-GD-027 – Training and Assuring Personnel Competence**   
  This TAG addresses how the licensee demonstrates that it has a systematic approach to identification and delivery of personnel competence and its training processes and arrangements for assuring personnel competence.
* **NS-TAST-GD-048 – Organisational Change –** This TAG addresses the adequacy of the licensee’s arrangements and their implementation, to ensure that changes to organisational structure or resources which may affect safety are adequately controlled.
* **NS-TAST-GD-049 – Licensee Core and Intelligent Customer Capabilities** - This TAG addresses how the licensee demonstrates that it has sufficient in-house expertise to maintain control and oversight of nuclear safety at all times, and the use and oversight of contractors whose work has the potential to impact on nuclear safety.
* **NS-TAST-GD-065 – Function and Content of the Nuclear Baseline -**This TAG addresses how the licensee demonstrates that its organisational structure, staffing, and competencies are, and remain, suitable and sufficient to manage nuclear safety throughout the full range of the Licensee’s business. It provides the foundation from which organisational changes can be assessed.
* **NS-TAST-GD-072 – Function and Content of a Safety Management Prospectus –** This TAG requires a licensee to have adequate structures and resources to meet the nuclear safety needs of the business.
* **NS-TAST-GD-104 – Corporate Governance for Safety –**

This TAG draws together sources of relevant good practice on corporate governance and its impact on safety into a single document aligned to The Wates Corporate Governance Principles for Large Private Companies.

## Advice to Inspectors

Delivery of a capable security organisation involves many aspects of a dutyholder’s business, including leadership and governance, management arrangements, adequate numbers of Suitably Qualified and Experienced Personnel (SQEP) and the financial resources required for secure operations. A robust security culture across the organisation is a key indicator of the organisations ability to maintain routine security and respond to security challenges.

**Security Plans**

1. The term security plans cover all dutyholder submissions, such as site security plans, temporary security plans and transport security statements and plans. SyAPs security plans generally describe a dutyholder’s security arrangements at a high level and reference out to the standards, procedures and arrangements in place to explain how the relevant security outcome is achieved. Those standards, procedures and arrangements are an integral part of the security plan. The most effective organisations integrate security with their routine business delivery strategy and plans seeking to ensure that arrangements are clear and actionable.
2. Dutyholders may seek to align safety and security processes where appropriate and include security as an integral part of key documentation: for example, in producing a combined safety and security management prospectus. The effectiveness of this approach should be assessed on its merits and in a proportionate manner.
3. The regulatory expectations placed upon the duty holder to demonstrate a capable organisation is that they will ensure that the security plans include:

* The governance structure and arrangements for security.
* A clear security organisational structure with corresponding roles and responsibilities including how organisational resilience will be achieved.
* The arrangements to maintain a design authority [[1]](#footnote-2) (DA) and a core security and intelligent customer [[2]](#footnote-3) (CS&IC) capability to maintain knowledge of security facilities, equipment, and arrangements.
* Arrangements to retain and manage the use of knowledge to ensure security arrangements are understood and risks controlled through all activities and
* The arrangements to demonstrate the adequacy of financial resources.

**Governance**

1. Corporate governance is described in the UK Corporate Governance Code, as: “…the system by which companies are directed and controlled”. It goes on to state that: “…Boards of directors are responsible for the governance of their companies”. Statutory Directors have specific fiduciary duties in law. The ONR guidance on Corporate Governance for Safety focusses on the Wates Corporate Governance Principles because they are an example of corporate governance good practice; however, dutyholders may adopt other relevant good practice.
2. It is key that to support a robust security culture duty holder boards treat security as an appropriate priority when providing strategic direction and leadership. Corporate governance for security is the combination of a company’s corporate governance arrangements and the activities undertaken by its board in ensuring adequate direction and control over security. Clearly documented corporate governance arrangements which include security will ensure it is considered during decision making.
3. The Security Governance and Leadership TAG1.1 provides guidance, and the Corporate Governance for Safety TAG104 identifies relevant good practice.
4. The regulatory expectations placed on the dutyholder is to demonstrate that:

* Corporate Governance arrangements are clearly documented.
* The Board gives appropriate priority to security matters.
* Board decision-making considers to the following factors:
* The quality of board reporting and information.
* The questioning of assumptions.
* Exploration of all relevant scenarios that may threaten security.
* Consideration of health, safety, environmental, security, quality, and economic requirements.
* Relative priorities of the range of options to minimise overall risk both in the long and short term.

**Management Arrangements**

1. Security management arrangements should be clearly articulated in the management system and reflect those described in the approved security plan. It is good practice for dutyholders to have a single management system covering all aspects of the business. For example, where there is a safety management prospectus this may include security and become a Safety and Security Managements Prospectus. Some dutyholders will also include Environment in the document.
2. Further guidance on TAG072 Function and Content of a Safety Management Prospectus (SMP) – This TAG requires a licensee to have adequate structures and resources to meet the nuclear safety needs of the business.

**Organisational Structure**

1. The dutyholder will determine its organisational structure based on the needs of its business. Inspectors should assess whether the proposed structure is fit for purpose and meets the regulatory expectations for maintaining security throughout the full range of business activities.
2. The dutyholder should maintain a core security capability of staff to ensure effective control and management for nuclear security. It should retain overall responsibility for, and control and oversight of, the nuclear and radiological safety and security of all its business, including work carried out on its behalf by contractors.
3. The Function and Content of a NB TAG065 says that “The principal purpose of the NB is to provide a demonstration that the licensee has suitable and sufficient organisational structures, staffing and competences in place to effectively and reliably carry out those activities which could impact on nuclear safety.” These key principles of a nuclear baseline are relevant good practice when applied to the organisational nuclear security baseline.
4. It is good practice for an organisation to have an up-to-date organisational baseline. The NB may be a sub-set of the organisational baseline. However, it should not be restricted to those roles set out in the site’s minimum staffing arrangements nor those which the licensee has identified as being necessary to maintain the facility in a quiescent shutdown state. It should reflect the roles needed to carry out the full range of activities.
5. It is good practice to include in the NB core security (and safeguards) posts and any associated roles, such as those required in the event of emergency security response. However, dutyholders could decide to capture the security posts in the organisational baseline. Nonetheless, the duty holder should be able to demonstrate that it has considered all activities with the potential to impact on nuclear security: activities which if inadequately conceived or executed could lead to an immediate or latent security threat.
6. The dutyholder should be able to show that it understands the security roles that need to be delivered, and that these roles will be carried out by suitable and sufficient competent resource. It is not sufficient just to show that all roles are covered, but that those individuals in post can realistically carry these roles out to the required standard and capacity. This is linked to the training and competence of people. Further guidance can be found in the TAG3.2 Sufficiency and Competence of Personnel Delivering Security.
7. ONR acknowledges that in some cases, staffing models may be based on approaches from predecessor or similar facilities, rather than being justified using detailed, auditable analysis. In such cases, the inspector should be proportionate, but request a description of the staffing model chosen and justification for its selection. In some instances, for example roles with a high potential impact on nuclear security, formal analysis may be required to demonstrate adequacy of proposed or existing staffing arrangements.
8. Details of the principles that should be assessed, and factors to be taken into consideration when determining whether the NB meets required standards and fulfils the claims and assertions made in the security plan, can be found in the Function and Content of the Nuclear Baseline TAG065.
9. Advice and support should be sought from human and organisational capability (HOC) inspectors where an assessment of the NB is being planned. The NB should follow these principles:

* The NB should consider the delivery and oversight of all activities which have the potential to impact upon nuclear security. This includes activities with a positive impact and those which, if inadequately conceived or executed, could lead to an immediate or latent detriment to nuclear safety and security.
* The NB should address the requirements of steady state conditions, periods of change and potential emergency situations at the current phase of the licensed facility’s life cycle.
* The NB should demonstrate that the dutyholder’s organisation has sufficient staff and competencies to discharge its responsibilities for delivery and oversight of nuclear security in accordance with the approved security plan.
* The licensee must demonstrate that it remains in control of nuclear security.
* The governance of nuclear security and CS&IC capability are an intrinsic part of this demonstration.
* Contract staff should appear as part of the NB resource when they are embedded within the dutyholder’s organisation or meet the criteria for holding CS&IC roles on behalf of the licensee.
* The dutyholder should have arrangements in place to manage contract staff who do not meet the criteria for inclusion in the NB, and in these cases the NB should include those employees who discharge the associated IC functions.
* Dutyholders should develop a set of indicators that provide evidence that the NB has the right organisation, staffing levels and competences and that it is being managed effectively.
* The dutyholder should have in place a process through which the NB is derived and managed.
* The NB should be maintained as a living document and provide an accurate, current reference point against which nuclear safety and security implications of proposed modifications to staffing levels/structures, workloads, and changed competence requirements can be assessed, in accordance with the licensee’s arrangements made under LC36.

**Organisational Change**

1. The dutyholder’s management of change arrangements should ensure that the nuclear security implications of a proposed change to the organisational nuclear security baseline posts are fully considered and that risks arising from inadequate impact assessment and implementation of the change are recognised and suitably controlled. These arrangements should be part of a dutyholder’s management system. Relevant good practice on categorising and managing security changes can be found in CNS-TAST-GD-11.4.6 Managing Changes to Security Procedures and further relevant good practice and be found in TAG-048 Organisational Change.
2. Dutyholders may choose to use the LC36 management arrangements for changes to organisational nuclear security baseline posts in a proportionate manner and with reference to the categorisation of change in CNS-TAST-GD-11.4.6. This integrated approach is considered good practice. However, all changes to the organisation that are specified in the approved security plan must be submitted to ONR for approval unless ONR has issued notifications under Regulation 7(2). When reviewing organisational change arrangements, consider whether the duty holder has assessed security as part of its change management risk assessment process and whether Regulation 7(2) is applicable.
3. There are many drivers for organisational change, and, without formal change management, a duty holder may not immediately recognise the implications of a proposed course of action. When organisational structures change inspectors should consider whether there is a risk that security resources may be diluted or diverted elsewhere.
4. It is important that the full implications of a proposed change or a series of changes are assessed prior to implementation. This is to guard against a failure to consider all relevant factors and potential dependencies between related changes, and the potential for salami slicing in which a major change is decomposed into a series of lesser changes which are treated independently.
5. This applies to changes at all levels in the organisation including the very top of the organisation, for example, the Board or Executive team, where changes in the composition and knowledge of either of these teams can have a potentially significant influence over security.
6. Board, Executive and Lead Team members should understand:

* The importance of management of change arrangements as an integral part of business strategy implementation, nuclear safety and resource management;
* The need for the Board/Executive to visibly commit to management of organisational change as a key business process;
* The need for the implications of all proposed organisational changes to be formally assessed using a consistent methodology which is an integral part of the licensee’s management system;
* The Board/Executive’s role in ensuring that the implications of significant and complex changes are fully assessed prior to implementation;
* The Board/Executive’s role in providing oversight of significant and complex changes and ensuring that the objectives of the changes are met;
* The importance of regularly monitoring the state of the organisation to ensure that nuclear safety is not progressively degraded over time as a result of a succession of changes;
* The need to regularly review that the licensee’s management of change arrangements are up to date and are being consistently applied across the entirety of the licensee organisation;
* The importance of having SQEPs in key management of change roles.

1. Check that the baseline contains a substantiation of the ‘right size and structure’ for the dutyholder organisation. Check that there is not a presumption that the existing structure is adequate.
2. Check that the arrangements are linked to human resource processes and that Human Resources is involved in assessing implications of changes for workforce planning and training and acting as appropriate.
3. Managers proposing changes and key role holders such as reviewers should have knowledge of:

* Roles and responsibilities;
* Staging of changes where appropriate;
* The value of enabling actions which have been properly identified and managed i.e. verifiably closed out;
* Use of performance indicators and contingency measures or remedial actions, and that they have been properly identified and managed;
* The importance of reviews at appropriate times during implementation.
* Records requirements.

1. Confirm that the arrangements are being adhered to by discussion with staff at various levels throughout the dutyholder’s organisation.
2. Check the change register and observe if:

* There are similar, linked changes which should have been managed in a coordinated manner i.e. under an umbrella or overarching management of change, and given a higher change category;
* There is evidence of ‘salami slicing’ of a larger change into a series of smaller changes.

1. Check the dutyholder's implementation of its review and audit processes and examine:

* Periodic review and update of the nuclear baseline;
* Reviews of performance indicators during and after implementation;
* Categorisation reviews;
* Independent safety reviews;
* Reviews of implementation of the arrangements and plans for improvement.
* Reviews of cumulative effects of change on the organisation.

1. Check the dutyholder’s communication arrangements to confirm whether the workforce understands the implications of significant changes and is kept informed of implementation progress.

* Check that arrangements exist to periodically update the nuclear baseline and that the baseline is up to date and reflective of the dutyholder organisation.

**Implementation of change proposals**

1. Select a sample of change proposals for checking. The sample should include top category changes if there have been any, and lower category changes throughout the range of significance. The sample should ideally include any corporate changes which may affect security on site. Consider ‘calling in’ changes (at any or all category levels) for specialist assessment.
2. For each change proposal in the sample:

* Check the register of change proposals to confirm that change proposals for significant changes were reviewed and authorised through the appropriate route and available in time to provide 20 working days’ notice for ONR assessment prior to implementation if required.
* Make a judgement about the accuracy of the classification of the change.
* Check that the substantiation document for significant changes includes where appropriate:

A clear description of the objectives of the change;

A reference to the nuclear baseline;

A risk assessment which has been used to inform the classification of the change;

A detailed implementation plan with timescales, including staging of the change where appropriate;

Enabling actions as precursors to implementation of the change;

Performance indicators to monitor the effectiveness of implementation;

Contingency plans and remedial actions;

Shadow working to confirm planned arrangements where appropriate.

* Check that authorisation to proceed with the proposed change was granted by a SQEP.
* Check that all enabling actions for significant changes were satisfactorily closed out before the appropriate parts of the change were implemented. Verify a sample of the actions if appropriate.
* Check that the performance indicators were used to monitor implementation progress and that contingency plans or remedial actions were invoked at an appropriate time.
* Check that the change proposal was signed off as complete by a SQEP.
* Check that the objectives of the change were met.
* Check that any staff implications have been satisfactorily addressed, for example:

Vacancy filling and recruitment;

Training and development.

* Check that the baseline has been updated to reflect the impact on baseline roles where appropriate.

**Security Design Authority and Core Security and Intelligent Customer**

1. The security arrangements at a nuclear premises are the product of the activities of many organisations, and changes to those arrangements may occur periodically over the site’s lifetime. Maintaining the level of security expected of a nuclear facility requires that changes to it must be made with full knowledge of the design and the security functions that need to be provided. This knowledge should be retained in a form that is practically and easily available to the dutyholder over the full lifetime of the site.
2. A dutyholder should have a formal process to understand and maintain design knowledge and design integrity. That part of the dutyholder’s organisation with the responsibility for, and the requisite knowledge to maintain, the design integrity and the overall basis for security of its nuclear facilities throughout the full lifecycle of those facilities is termed the DA. This includes sufficient knowledge to understand the need to protect against the cyber threat.
3. Existing dutyholders should have a suitable and sufficient DA capability and organisations seeking approval of a security plan should have credible programmes to develop this capability in a timely manner.
4. The DA should have sufficient knowledge to understand the security arrangements for the site and to assess the impact of proposed design changes on the functionality, reliability and availability claims made in the security plan. The DA should also have sufficient knowledge of any specific constraints that impact on the practical use of equipment and thereby need to be reflected in an effective design, such as restrictions in space, availability of site services, capability and limitations of security equipment sensors and the threat. These factors should be considered at the same time as the generic design inputs, such as legislative requirements and security standards.
5. Ownership of the security plan and responsibility for understanding the function and performance of existing security arrangements should ordinarily reside with the operations function, rather than with the DA. For new facilities within a nuclear site, the DA may be the owner of the facility security plan during the design/construction phase prior to the operations function being established however this should comply with the extant wider security plan, otherwise prior to any modification being implemented, approval of a temporary security plan or arrangement should be sought from ONR as appropriate. The DA should be expected to maintain a security plan through-life, which should include:

* recording modifications to security arrangements effected to improve performance or made in the light of operating experience;
* approving design substantiations for any modification proposed;
* recording of operating experience which might impact the design across all security arrangements, and analysis thereof to identify trends and the need for essential equipment upgrades, tighter operating constraints etc;
* communication of the need for essential security equipment upgrades, tighter operating constraints etc; and,
* effecting essential research, through-life degradation testing etc. The purpose of this research is to support security arrangements to the end of the site’s designed life or any potential life extension which may be requested by the operators.

1. ONR recognises that, for new plant, the vendor rather than the dutyholder may own the design. Where this is the case, ONR will expect the dutyholder to demonstrate how it proposes to acquire a suitable and sufficient DA capability.
2. ONR also acknowledges that the dutyholder may not have all the detailed, specialised knowledge required of all the systems and components important to security within its DA organisation. In such instances it may assign its responsibilities for some parts of the security equipment to other organisations such as those that originally designed that equipment. Bodies with these responsibilities are termed Responsible Designers (RD). However, the dutyholder should retain sufficient knowledge to act as the Intelligent Customer (IC) for equipment and services provided to it. The dutyholder should be able to demonstrate how it intends to maintain a satisfactory contractual relationship to deliver the RD service from the vendor for the foreseeable future, if this cannot cover whole plant life.
3. The dutyholder should retain sufficient knowledge of all aspects of the design to act as a DA and IC to enable it to understand the results of the Responsible Designers’ work, and to understand the security implications of that work for the life of the plant. The dutyholder should also understand any implications from the design for other security systems on its site.
4. The roles of DA and IC should be part of the dutyholder’s core capability and included in their Nuclear Baseline.
5. Details on what the inspector should consider when assessing a dutyholder’s DA including a detailed explanation of the principles can be found in the Licensee Design Authority Capability TAG-079. The key principles of a security DA capability can be found in CNS-TAST-GD11.4.6 Appendix 5.

**Knowledge Management**

1. A key component of a capable organisation is one which has in place effective Knowledge management (KM) processes. KM is defined by the IAEA in TECDOC-1510 (Knowledge Management for Nuclear Industry Operating Organisations) [7] as” An integrated, systematic approach to identifying, acquiring, transforming, developing, disseminating, using, sharing, and preserving knowledge relevant to achieving specific objectives. Knowledge management helps an organisation to gain insight and understanding from its own experience. Specific activities in knowledge management help the organisation to better acquire, store and utilise knowledge".
2. As with all such concepts, the role of the leaders within an organisation cannot be overstated. The tone and level of expectations set by the most senior manager of an organisation will drive both the implementation and the results. KM is a vital component of change management and therefore a fundamental element of a capable organisation.
3. As KM initiatives are undertaken, it is imperative that expectations and the reasoning behind those expectations are clearly communicated throughout the organisation. A spirit of knowledge sharing must pervade the organisation if the full potential of KM is to be realised. Sensitivity to the need for continual, consistent KM must become ingrained in the culture of an organisation. Therefore, a capable organisation will be able to demonstrate KM in its strategic planning; analysis and decision-making; implementation of plans; and evaluation of results processes.

**Adequacy of Financial resources**

1. The financial resources of a dutyholder are not routinely the focus of inspection activities, nevertheless dutyholders should be able to demonstrate prudent fiscal planning and articulate how they will be able to achieve and maintain the security arrangements specified in the security plan. The security plan should set out the split in the security budget between operations, maintenance, asset management and investment which is to be reviewed during the dutyholder’s annual review of security.
2. During routine regulatory engagement with dutyholders, inspectors should be alert to indirect evidence that may indicate a reduction in the ability or willingness of the dutyholder to provide or maintain adequate financial resources to ensure security. Evidence may include failure to implement security improvements; security staff shortages that are not being filled; delays in delivering activities such as maintenance of security equipment etc. Should indications be found that investment in security-related plant or people may not be adequate to provide and maintain security, the inspector should seek to establish whether it is attributable to other factors (for example difficulties in identifying SQEP resource; technical difficulties or disagreements etc.) and, if so, to progress the matter in the normal manner.
3. If the security issue cannot be resolved to the satisfaction of the inspector, and financial resource issues are identified as a possible factor, this matter should be elevated to the relevant superintending inspector for consideration. It is anticipated that discussions will take place with the dutyholder to determine the cause of the issue and attempt to resolve it. This may entail a wider ONR review of the security plan; annual financial accounts, plans for construction and key financial decision points; investment plans; lifetime plans, the nuclear baseline, and other documents. If the issue cannot be resolved, and failure to comply with the security plan is determined, consideration may be given to engaging external expert financial advice to inform the process of establishing ONR’s enforcement options. The need to take this course of action is expected to be rare.
4. Where the dutyholder's budget is controlled by another body (for example, the Nuclear Decommissioning Authority (NDA) or a parent organisation), financial (and other resourcing) arrangements are likely to be set out in contractual arrangements between the dutyholder and the controlling body. ONR may seek to examine these documents. ONR anticipates that the controlling body will co-operate with the dutyholder in ensuring the adequacy of the resources needed for security and meet its obligations under NISR 2003 (as amended). The dutyholder, however, retains an absolute responsibility for site security.

51. Should a forensic accountancy service be needed, ONR has arrangements to access Government Forensic Accounting Services.

# References

|  |  |
| --- | --- |
| [1] | ONR, “Secruity Assessment Principles,” [Online]. Available: https://www.onr.org.uk/saps/. |
| [2] | U. Gov, “Nuclear Industries Security Regulations 2003,” [Online]. Available: https://www.legislation.gov.uk/uksi/2003/403/contents/made. |
| [3] | IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM),” [Online]. Available: https://ola.iaea.org/ola/treaties/documents/FullText.pdf.. |
| [4] | IAEA, “Nuclear Security Series No. 20. Objective and Essential Elements of a State’s Nuclear Security Regime.,” [Online]. Available: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590\_web.pdf. |
| [5] | WINS, “Corporate Governance Arrangements for Nuclear Security,” [Online]. Available: https://www.wins.org/document/corporate-governance-arrangements-for-nuclear-security/. |
| [6] | ONR, “Permissioning Inspection - Technical Assessment Guides,” [Online]. Available: https://www.onr.org.uk/operational/tech\_asst\_guides/index.htm. |
| [7] | IAEA, “Knowledge Management for Nuclear Industry Operating Organisations,” [Online]. Available: https://www.iaea.org/publications/7515/knowledge-management-for-nuclear-industry-operating-organizations. |
| [8] | Financial Reporting Council (FRC), “The UK Corporate Governance Code,” 2018. |

# Glossary and Abbreviations

CPPNM Convention on the Physical Protection of Nuclear Material

CS&IA Cyber Security and Information Assurance

CS&IC Core Security and Intelligent Customer

DA Design Authority

FSyP Fundamental Security Principle

IAEA International Atomic Energy Agency

IC Intelligent Customer

KM Knowledge Management

LC Licence Condition

NB Nuclear Baseline

NDA Nuclear Decommissioning Authority

NISR Nuclear Industries Security Regulations

ONR Office for Nuclear Regulation

RD Responsible Designers

SAP Safety Assessment Principle(s)

SMP Safety Management Prospectus

SNI Sensitive Nuclear Information

SyAP Security Assessment Principle

SyDP Security Delivery Principle

SQEP Suitably Qualified and Experienced

TAG Technical Assessment Guide(s)

WINS World Institute for Nuclear Security

1. The Key Principles for the Design Authority functions are defined in CNS-TAST-GD-11.4.6 Appendix 5. [↑](#footnote-ref-2)
2. The Key Principles for Core Security and Intelligent Customer are defined in CNS-TAST-11.4.6 Appendix 4. [↑](#footnote-ref-3)