ONR GUIDE			
LEADERSHIP AND MANAGEMENT FOR SECURITY			
Document Type:	Nuclear Security Technical Inspection Guide		
Unique Document ID and Revision No:	CNS-INSP-GD-1.0 Revision 1		
Date Issued:	January 2018	**Review Date:**	January 2022
Approved by:	Matt Sims	Professional Lead Security Specialism	
Record Reference:	2021/7933		
Revision commentary:	Administrative review only pending in depth analysis of Inspector survey responses		

TABLE OF CONTENTS

Published 01/18

1 INTRODUCTION

1.1 The Nuclear Industries Security Regulations (NISR) 2003 (Reference 7.1) contains requirements for responsible persons to make certain arrangements including standards and procedures to ensure the security of the nuclear premises, Nuclear Material (NM) or Other Radioactive Material (ORM) stored on the premises, Sensitive Nuclear Information (SNI) and standards and procedures for the transportation of Category I - III NM.

1.2 Regulation 4 of NISR requires there to be an approved security plan for each nuclear premises[1] which details those arrangements for the protection of NM/ORM and SNI, including contingency plans. Regulation 7 places the requirement for the dutyholder to maintain arrangements in accordance with the approved plan. Similarly, transporters of Category I - III quantities of NM are required to detail their security arrangements in an approved Transport Security Statement in accordance with Regulation 16 and Regulation 17 requires them to maintain those arrangements. For the purposes of this guide, the term security plan will be used to refer to both approved documents.

1.3 The Office for Nuclear Regulation (ONR) has established a set of outcome focused Security Assessment Principles (SyAPs) (Reference 7.7) which provide a framework for it to assess security arrangements defined in security plans and make consistent regulatory judgements on the adequacy of those arrangements. The Fundamental Security Principles (FSyPs) and their underpinning Security Delivery Principles (SyDPs) are goal-setting and do not describe what the dutyholder's arrangements should contain; this is the responsibility of the dutyholders who remain responsible for security.

1.4 To assist inspectors, ONR produces a suite of guides to assist them in making regulatory judgements and decisions in relation to the adequacy of compliance. This inspection guide is one of the suite of documents provided by ONR for this purpose.

2 PURPOSE AND SCOPE

2.1 Security plans should be structured in a format consisting of high-level claims, supported by arguments substantiated by evidence. Where the dutyholder is required to have an approved security plan, the purpose of this guide is to facilitate a consistent and effective approach to inspecting compliance with the arrangements described in the plan and detailed in the underpinning documentation concerning FSyP 1 – Leadership and Management for Security.

2.2 The judgements made by the inspector will primarily relate to the efficacy of the implementation of arrangements described in evidence that supports the security plan to ensure that associated arguments are fully substantiated. However, ONR takes a sampling approach to regulation and it is possible that elements of evidence within the plan or underpinning the plan were not subject to assessment as part of the approval process. Therefore, when reviewing or inspecting evidence as part of the intervention, the judgement may relate to the adequacy of the arrangements which support the approved plan. The inspector may also provide advice and guidance in the interests of encouraging dutyholders to seek continuous improvement.

2.3 The guidance in this TIG should not be regarded as either comprehensive or mandatory, but provides a framework for inspectors on which to base their judgements and discretion during such inspections.

[1] As defined by Regulation 2 of NISR 2003.

2.4 This guidance consists of four main sections and five annexes which will help inspectors plan and implement their security leadership and management compliance inspections.

2.4.1 Section 3 summarises the relationship of leadership and management for security to the relevant legislation.

2.4.2 Section 4 provides a brief overview of the purpose of the FSyPs and associated SyDPs.

2.4.3 Section 5 provides guidance on the expectations for leadership and management for security and practical guidance on organisational arrangements that an inspector may take into account when organising inspections of the implementation of SyDPs 1.1 – 1.5 arrangements.

2.4.4 Section 6 provides general guidance on preparation for, delivery of and reporting of findings of inspections. Details of the facets of leadership and management that an inspector should check during interventions are contained in Annexes A – E.

2.5 The International Atomic Energy Agency (IAEA) publish the Fundamentals document "Objectives and Essential Elements of a States Nuclear Security Regime", NSS 20 (Reference 7.3) which requires Member States to ensure that dutyholders establish and implement an effective integrated management system and demonstrate leadership in nuclear security matters.

2.6 The high level Leadership and Management for Safety requirements defined in General Safety Requirements Part 2 (Reference 7.4) recognise the interaction between nuclear safety and security culture and the importance of fostering both in a harmonious manner. SyAPs transposes these requirements in the UK, and this guidance considers the relevant aspects of leadership and management for security.

2.7 Nationally, the 2014 HMG Security Policy Framework (Reference 7.5) places a mandatory expectation on government organisations to have an appropriate governance structure and effective leadership for security in place.

3 RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The term 'dutyholder' mentioned throughout this guide 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.

4 OVERVIEW OF FUNDAMENTAL SECURITY PRINCIPLE 1: LEADERSHIP AND MANAGEMENT FOR SECURITY

4.1 Leadership and management for security (FSyP1) as described in the SyAPs, identifies the expectations related to the development and maintenance of the security capability within the dutyholder's organisation. Covering five key delivery principles, it states that "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". The qualifying text describes that due to their inter-connected nature, there is an overlap with some aspects of the principles and therefore when inspecting dutyholders arrangements, leadership and

management for security should be considered as an integral component of the overall leadership and management approach.

4.2 The associated security delivery principle (SyDP 1.1) considers the governance and leadership of the security arrangements. It notes robust governance incorporates clear Terms of Reference, a direct chain of accountability for security through to the main Board member responsible for security oversight. It notes that directors, managers and leaders at all levels should focus the organisation on achieving and sustaining high standards of security and on delivering the characteristics of a high reliability organisation. Additionally, reporting structures should be clearly understood, and the organisation should demonstrate well-defined control of resources and delegated personal authorities.

4.3 SyDP 1.2 notes that a capable organisation should have the capability to implement and maintain the security of its business, to have a correctly resourced governance structure and associated organisation. It expects that all persons with responsibility for security have the appropriate authority for their role with clearly defined accountabilities and objectives. Additionally, it expects that a capable organisation will have effective knowledge management arrangements including an 'intelligent customer' capability with the necessary competencies, experience and knowledge to maintain the capability of governing, leading and managing security at all times.

4.4 SyDP 1.3 notes that decisions associated with security matters should be informed, rational, objective, transparent, prudent and given adequate priority to aid decision making at the appropriate level within the organisation. The decision process should ensure that all relevant data and opinions are collected, recorded and considered, respecting and encouraging the contribution of those with divergent views. Security decisions should not be delayed unnecessarily (e.g. for commercial reasons) and personnel should be empowered to take timely decisions in the interests of security. It also encourages staff to display a questioning attitude to security inclusive of contractors.

4.5 An integral component of effective leadership and management arrangements is to ensure lessons are learned from internal and external sources. The expectation is that the organisation will be able to demonstrate how learning from experience is used to continually support and improve leadership processes and arrangements, organisational capability, the management system, security decision making and security performance. SyDP 1.4 highlights the arrangements organisations should have in place to learn and implement lessons from a wide range of sources. This includes security near-misses, which should be seen as opportunities to learn and responded to in a manner that fosters a culture of open reporting.

4.6 Dutyholders should have an independent (of security management) assurance structure to provide ongoing confirmation that the security organisation is delivering the required security outcomes. The management system, as captured in SyDP 1.5, should ensure there is Board-level assurance and oversight of the dutyholder's security performance in place, which includes the monitoring of key performance indicators and compliance while welcoming challenge from across the organisation.

5 GUIDANCE ON THE EXPECTATIONS OF ARRANGEMENTS FOR FUNDAMENTAL SECURITY PRINCIPLE 1 - GENERAL CONSIDERATIONS

5.1 The dutyholder's leadership and management arrangements contained within their security plan incorporate those structures, policies (such as a Nuclear Security Policy-NSyP) and processes necessary to enable the effective delivery of nuclear security.

When inspecting these arrangements, the roles and responsibilities of all directors, managers and leaders at all levels (process owners) with security responsibilities should be clearly stated.

5.2 The organisation should have a process that manages changes to their security plan, including a methodology to control any change to the security organisational structure. Such arrangements should be consistent with the Nuclear Industry Code of Practice on the 'Nuclear Baseline' (Reference 7.10).

5.3 The organisation should have in place robust arrangements for identifying the competence needs of all persons with nuclear security responsibilities. Although ONR would not normally inspect the competence of dutyholder's staff, inspectors will inspect records and arrangements to ensure workers are appropriately trained, and their competence adequately assured by the organisation.

5.4 The organisation should be able to demonstrate effective oversight of nuclear security through a robust internal challenge capability that is independent of the operational line management.

5.5 The organisation's integrated management system should take into account the security implications of all activity and ownership of that system should reside at a senior management level. The management system should demonstrate how organisational resilience is achieved. Senior managers must be able to demonstrate they understand the scope of their business and its relationship between their security arrangements and those of other stakeholders and contractors.

5.6 Decisions with the potential to affect security arrangements (including major change initiatives) should be taken using a prudent, rational process that incorporates diversity, transparency and challenge and should not be out-sourced to contractors or negatively influenced by group-think behaviours.

5.7 The organisation's security plan should clearly identify a structure, framework and processes which support organisational learning. Integral to demonstrating effective organisational learning is the process that identifies and collects pertinent information on security events. The organisation's arrangements should comply with NISR 2003 security event reporting requirements, and include a mechanism to undertake investigations to identify the cause and effect of events as well as ensuring lessons are learnt, formally captured and shared to appropriate parts of the organisation.

5.8 The organisation should have security assurance arrangements in place that are independent of security management, deliver evidence based assurance and promote a challenge culture across the organisation and its contractors.

6 GUIDANCE ON THE INSPECTION OF LEADERSHIP AND MANAGEMENT FOR SECURITY ARRANGEMENTS

6.1 Inspection is one of three key building blocks for all of ONR's regulatory activities, the others being assessment and investigation. ONR expects its inspectors to be able to deliver inspections in a consistent manner resulting in similar outcomes for similar findings. Inspectors should apply the principles contained within the ONR General Inspection Guide. Inspections involve the examination of documentation and arrangements of the facility, its security processes, operations and organisation underpinning the security outcomes in its security plan. A sampling approach should be used when planning inspections, which will be based on the confidence the inspector has of the organisation's approach to leadership and management for

security, the risks and vulnerabilities of activities covered by the security plans and recent events or operating experience at the facility.

Planning, Delivering and Managing Intervention Outcomes

6.2 **Planning**. The inspector should be clear as to the purpose of the proposed intervention and why is it being considered; is it regulatory intelligence, divisional strategy, routine compliance or another reason that is driving the requirement? The periodicity of Leadership and Management for Security (LMfSy) interventions will be influenced by the annual ONR assessment of the dutyholder's security performance, together with any intervention findings and regulatory intelligence obtained since the last inspection. Once these initial considerations are understood, the inspector should be in a position to define and agree the outcomes and outputs of the intervention. Where delivery of these objectives identifies the requirement for additional regulatory resources, support from other specialists, for example ONR LMfS (safety) inspectors, should be sought.

For further guidance see:

- Intervention Planning and Reporting Guide – ONR-INSP-GD-059.
- General Inspection Guide – ONR-INSP-GD-064.

6.3 **Preparation**. Preparation includes a review of the inspection history for that dutyholder. Previous Intervention Records (IR) and the Regulatory Issues Database (RID) should be reviewed to determine if there are legacy concerns or issues outstanding which are relevant to the planned inspection. Preparation for a LMfSy inspection should include a review of relevant guidance which could include the dutyholder's NSyP, management system manual, knowledge management policy and internal assurance policy. Inspectors should use the relevant guidance, in conjunction with their knowledge and experience of relevant good practice, to develop a clear understanding of the compliance standards that are expected.

6.4 **Delivery**. To effectively deliver the intervention, the inspector will need to be clear as to their expectations and the standards they will assess the dutyholder against, how they will implement the intervention, areas that require sampling, and the evidence required to be seen/obtained to support outputs and outcomes.

6.5 To assist inspectors in making regulatory judgements and decisions in relation to the adequacy of compliance, specific considerations for each of the FSyP 1 elements are covered in the Annexes as follows:

- **Annex A** - SyDP 1.1 (Security Governance and Leadership)
- **Annex B** - SyDP 1.2 (Organisational Security Capability)
- **Annex C** - SyDP 1.3 (Security Decision Making)
- **Annex D** - SyDP 1.4 (Organisational Learning for Security)
- **Annex E** - SyDP 1.5 (Security Assurance Processes)

7 FURTHER READING

7.1 Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 NO. 403

7.2 IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). January 2011.

7.3 IAEA Nuclear Security Series No. 20. Objective and Essential Elements of a State's Nuclear Security Regime.

7.4 IAEA General Safety Requirement GSR Part 2 Leadership and Management for Safety. June 2016

7.5 HMG Security Policy Framework. Cabinet Office.

7.6 NISR 2003 Classification Policy.

7.7 Security Assessment Principles

7.8 Independent Oversight – A Nuclear Industry Good Practice Guide. Produced by the Cross-Industry Internal Regulation Working Group and Published on Behalf of the Safety Directors Forum – January 2014.

7.9 The UK Corporate Governance Code. Financial Reporting Council- September 2014.

7.10 Nuclear Baseline and the Management of Organisational Change. Produced by the Cross-Industry Organisational Capability Working Group and Published on Behalf of the Safety Directors Forum – March 2017.

7.11 IAEA Nuclear Safety Standard NS-G-2.11. A System for the Feedback of Experience from Events in Nuclear Installations. May 2006

7.12 IAEA Safety Guide GS-G-3.1 Application of the Management System for Facilities and Activities (July 2006).

7.13 IAEA Safety Guide GS-G-3.5 Management System for Nuclear Installations. (September 2009)

7.14 ONR Guide NS-TAST-GD-093 (Rev0) – Guidance for Leadership and Management for Safety

7.15 ONR Guide CNS-TAST-GD-1.1 (Rev0) – Security Governance and Leadership.

7.16 ONR Guide CNS-TAST-GD-1.2 (Rev0) – Organisational Security Capability.

7.17 ONR Guide CNS-TAST-GD-1.3 (Rev0) – Security Decision Making.

7.18 ONR Guide CNS-TAST-GD-1.4 (Rev0) – Organisational Learning for Security.

7.19 ONR Guide CNS-TAST-GD-1.5 (Rev0) – Security Assurance Programme.

7.20 ONR Guide CNS-TAST-GD-3.1 (Rev0) – Analysis of Security Roles and Associated Competencies.

7.21 ONR Guide CNS-TAST-GD-3.2 (Rev0) – Identification of Learning Objectives and Training Needs.

7.22 ONR Guide CNS-TAST-GD-3.3 (Rev0) – Measurement of Competence.

7.23 ONR Guide CNS-TAST-GD-3.4 (Rev0) – Organisation of and Support to the Training Function.

ANNEXES

Annex A – SyDP 1.1 (Security Governance and Leadership)

Governance Standards and Expectations

The IAEA Safety Standard for and the Application of the Management System (Reference 7.12) and Leadership and Management for Safety (Reference 7.14) recognise the duality needed in a dutyholder's management system for safety and security. Members of the dutyholder's Board should have clear roles and responsibilities for security matters, both collectively and individually. They should hold the senior management to account for which they should be provided with good quality, current security information regarding threats and risks in addition to any operational performance information generated by the organisation, including metrics. Strategic direction and leadership of security should be appropriately prioritised for which the Board must have appropriate membership and competence (either through direct experience or readily accessed subject matter experts) to interpret the security information and use it to validate the efficacy of security programmes.

Effective oversight should be demonstrated through structured, integrated and diverse means such as self-assessments at facility/department level, internal independent oversight or regulation, robust governance structure, external assessments or peer reviews. The level and rigour applied to this oversight should be implemented using a graded approach especially where oversight is dependent on performance indicators that have inherent limitations. The Board should be compliant with the United Kingdom's corporate governance code published by the Financial Reporting Council (Reference 7.9) and should be able to demonstrate how they have integrated into their performance arrangements the principles of the independent oversight good practice guide (Ref 8) published by the Safety Directors Forum.

Inspectors should consider the following regarding the arrangements and their implementation:

- Does the Board have clearly defined roles and responsibilities?
- How does the Board ensure that security is given equal priority to safety when providing strategic direction and leadership?
- Are there mechanisms in place to ensure the Board receive current, high quality security information on threats and risks?
- Does the Board have appropriate membership and competence to assess and act effectively on security information?
- How are decisions taken on security matters by the Board based on information from a breadth of sources including performance indicators, staff feedback, event investigations, independent and self-assessment and is it of a satisfactory quality?

Leadership Standards and Expectations

The organisation should create and publish a Nuclear Security Policy (NSyP) which is widely available and promoted at all levels within the organisation. The policy should explain that security has a high priority and reflects that a credible threat exists and that individuals all have a role to mitigate elements of that threat. Roles, accountabilities, standards and

expectations of security behaviour should be clearly explained, linked to the NSyP and be applicable to all from the Board down.

Leaders and managers at all levels in the organisation should promote and display standards of behaviour which enable staff to engage with them regarding security concerns. Management should ensure that organisational security arrangements are robust, seek effective solutions to nuclear security issues and set out key objectives and targets for improving nuclear security in order to reduce risks. The dutyholder should ensure their management system meets national or international quality management system standards (i.e. ISO 9001 (Quality Management) or IAEA Safety Standard No GS-R-3 (The Management System for Facilities and Activities – Reference 7.12)).

Inspectors should consider the following regarding the arrangements and their implementation:

- Is there a clear, comprehensive and concise NSyP in place together with a commitment to adhere to it?
- Are roles, accountabilities, standards and expectations of behaviour for nuclear security clear, linked to the NSyP and apply to all from the Board down?
- Is the NSyP, standards and expectation effectively communicated across the organisation including stakeholders and contractors?
- How does the dutyholder reinforce and monitor compliance with the NSyP, standards and expectations from the Board down?
- How does the dutyholder's management demonstrate clear commitment to maintaining nuclear security?
- Does the dutyholder encourage regular face-to-face engagement between the Board, the senior management team and staff (such as visits to work areas to observe conditions first hand and to display and reinforce standards and expectations)?
- Is there a performance management system in place? Does it promote nuclear security without inadvertently encouraging perverse and/or counterproductive behaviours?
- Are staff routinely consulted and engaged on security issues such that their skills and knowledge are used to inform decision making at senior levels?
- Is there an integrated management system in place that adheres to current relevant good practice?
- Is the Board an 'intelligent customer' with sufficient security competence or experience to ensure assurance reports inform effective decision making?

Annex B – SyDP 1.2 (Organisational Security Capability)

Standards and Expectations

A consistent issue identified across a number of security events internationally has been the competence of those responsible for security to mitigate, or deal with, those events. Therefore, a key focus of any inspection should be to determine whether an organisation is considered capable from a security perspective. This would normally include an inspection of the nuclear baseline to check if the organisation is adequately resourced, a determination of whether there are sufficient numbers of Suitably Qualified and Experienced (SQEP) persons available to effectively deliver the security regime, resilience and the provision of an intelligent customer capability for security. The Safety Directors Forum's good practice guide on the nuclear baseline and management of organisational change provides a comprehensive framework against which the organisation can be assessed (Reference 7.10).

Inspectors should consider the following regarding the arrangements and their implementation:

- Check whether staffing arrangements are based on the current version of the Nuclear Baseline? Determine whether any changes to the business that might affect the appropriateness of the staffing model are being addressed (for example, change of categorisation level or introduction of a new VA)?

- Where significant human-based claims are made in the security plan, how does the dutyholder demonstrate that individual and team performance is underpinned by adequate supervision?

- Where staffing requirements vary depending on different operational modes or states and situations (e.g. night, weekends), how does the dutyholder demonstrate that there are adequate resources for the most resource-intensive conditions feasible in each operational mode/state?

- Where applicable, have the potential implications of sharing staff between multiple units or facilities been addressed, including where staff are co-opted from a shared work pool? Determine if the dutyholder has adequately addressed competence requirements (both role specific and general security awareness for the unit/facility) and assessed if the workload is achievable (in normal and emergency conditions)? Confirm the dutyholder has taken into account other factors such as the potential for procedural errors related to operational or design differences between units/facilities?

- Check if the dutyholder undertakes reviews of the staffing model on a periodic basis to ensure the model will achieve the security outcomes contained in the security plan? Confirm that any deficiencies identified during the reviews are adequately addressed or have been included in the security improvement schedule?

- Do staffing arrangements allow sufficient time for training and development or rest and recovery, particularly during busy periods such as increased security threat levels or maintenance outages?

- Is there evidence of effective management of staffing levels above the required minimum, for example rapid call-out due to unexpected absence?

- Do qualitative and quantitative indicators highlight problems with staffing levels and task organisation? Factors that could indicate potential problems include:
    - high levels of maintenance or procedure modification backlogs;
    - events relating to staff shortages, work patterns, communication or co-ordination issues within or between teams, or inadequate supervision;
    - high levels of overtime;
    - deferrals or significant delays to nuclear security related work programmes;
    - large numbers of outstanding actions; and
    - symptoms of personnel stress due to under or overload (e.g. high levels of sick leave, union grievances).

- Does the dutyholder's design authority have formal processes which understand and maintain security design knowledge? How does it assess the impact of proposed design changes on the functionality, reliability and availability of security arrangements contained in the security plan?

- Is there a strategy to ensure that the risks associated with losing personnel with mission critical knowledge are identified, and assess the adequacy of arrangements for succession planning?

- Is there a human performance improvement programme that continually identifies opportunities to improve security performance and expand the knowledge of the organisation?

- Does the organisation have a competence management system which adequately identifies all security related roles and their associated training requirements? Is a security competence gap analysis done for all relevant individuals and appropriate training plans put in place to address identified deficits?

- Are the organisation's arrangements for security training effectively resourced, and how is the training content specified and delivered, monitored and course effectiveness assessed? Consider examining a sample of course material designed by the organisation to determine whether a recognised design methodology has been used such as the systematic approach to training.

- Has the dutyholder developed and implemented strategies for knowledge capture, transfer and retention to preserve unique knowledge and skills?

- How does the culture of the organisation promote the transfer of knowledge, particularly tacit knowledge among security personnel? Does it have a knowledge champion and do managers serve as role models for others to emulate with regards to knowledge transfer?

- Does the dutyholder discourage knowledge transfer by rewarding employees based upon their being the sole source of critical knowledge and information? Does it reward employees for sharing their knowledge and information widely?

- Are managers personally involved in ensuring that the knowledge management programme is developed, implemented, continuously improved and integrated with the organisation's overall management system? Is it demonstrated through manager's involvement in the training, qualification, and performance of their personnel?

- Does the dutyholder utilise benchmarking to transfer knowledge, improve performance, and emulate relevant good industry practices and is this process integral to the organisation's culture?

Annex C – SyDP 1.3 (Security Decision Making)

Standards and Expectations

The dutyholder's arrangements should enable prudent, timely decisions to be made at the appropriate level by SQEP personnel. However, they should also permit decision-making to be transferred elsewhere within the organisation if the situation requires it. The organisation's security plans should not require all security decisions to be 'referred upwards', they should apportion authority at the appropriate level whilst recognising senior managers (including directors and the Board) should be involved in making strategic-level security decisions.

There is an expectation that security related decisions should also cater for the potential for error, uncertainty and the unexpected, and those taken in the face of uncertainty or the unexpected should be appropriately and demonstrably conservative. Arrangements should recognise that operational decisions may have to be made quickly, with imprecise and incomplete information. However, where appropriate, decision making should incorporate diversity of view, for example by involving individuals from other business units in the peer review process. Security-related decisions should not be 'out-sourced' to a third party, such as contractors, nevertheless where civilian guard forces are utilised and their shift supervisors and junior managers are authorised to make operational decisions, security plans should explain the scope of their authority, and internal arrangements to provide appropriate oversight by SQEP members of the organisation's staff.

Inspectors should consider the following regarding the arrangements and their implementation:

- How does the decision making process enable prudent and timely decisions to be made at the appropriate level by competent personnel?
- Do decision-makers have the necessary authority and the means to ensure that their decisions are implemented?
- How does the dutyholder ensure if decision-makers are demonstrably able to make rational, prudent and timely decisions?
- Is there an ongoing mentoring, training and assessment programme for inexperienced decision-makers? If appropriate, confirm whether individuals have the opportunity to realistically, but safely, practice their decision-making skills and learn from the experience?
- What processes are in place to ensure senior decision-makers are provided with adequate situational awareness and understanding to ensure that decisions are informed by the best available information in the time at hand?
- Does the dutyholder have mechanisms in place to involve internal and external stakeholders in the decision making process?
- Does the decision-making process allow for a range of potential solutions to be developed and tested?
- Is the process appropriately transparent, auditable and does it mandate the authority of individuals who are accountable for decisions taken?
- Does the process employ consistent, simple processes and methodologies which assist decision-makers?

- Is the process adequately flexible to allow for the reassessment of decisions and incorporate a review-learn-improve process?
- How is the process protected from negative influences and behaviours and does it allow appropriate challenge?

Annex D – SyDP 1.4 (Organisational Learning for Security)

Standards and Expectations

There is an expectation that dutyholders will have effective processes which seek out, analyse and act upon lessons from a wide range of sources. Security plans should identify the dutyholder's learning processes aimed at identifying and understanding the reasons for differences between actual and intended security outcomes and they should have a structured system for implementing and delivering corrective actions in a timely manner. Dutyholders' arrangements should describe their investigation processes for all types of events, recognising both safety and security significant events may be the result of malicious activity. Where an event meets NISR 2003 reporting requirements, dutyholders are legally required to make a report to ONR, therefore their security plans should include a clear description of these arrangements within mandated timelines. Near misses should be seen as opportunities to learn and the dutyholders should promote a culture of open reporting.

Inspectors should consider the following regarding the arrangements and their implementation:

- Does the dutyholder have a framework for organisational learning that incorporates the three essential components; leadership buy in, achieving learning through change management and utilising diverse information sources?
- Does the dutyholder have a policy for systematically identifying and correcting deficiencies in security?
- Are the dutyholder's security and safety OPEX policies effectively aligned?
- How does the dutyholder encourage staff to report security deficiencies and security improvement opportunities?
- How do the dutyholder's policies ensure it focuses on corrective action rather than blame towards personnel who report security deficiencies?
- How does the dutyholder encourage a learning organisation through actively seeking lessons learned from other organisations and, where appropriate, applying them to their organisation?
- Does the dutyholder regularly debrief staff on recent security issues that have occurred at the facility and utilise lessons identified to refresh staff understanding?
- Does the dutyholder have sufficient training for staff and management to recognise and report problems, and have enough experienced staff trained in root cause analysis to fully assess all reported security events?
- Check whether the dutyholder has adequate resources allocated to managing and reporting security deficiencies and confirm they are compliant with legislation and the ONR mandated reporting process?
- Does the dutyholder's process inform their Board on the findings of significant security deficiencies including analysis of the event and emerging trends?
- Are there indicators of backlogs in event investigations and corrective action closure, looking particularly for adverse trends?
- Does the dutyholder conduct data analysis to identify trends or recurring issues and implement proactive measures to mitigate these?

Annex E – SyDP 1.5 (Security Assurance Processes)

Standards and Expectations

Dutyholders should demonstrate in their security plan clear arrangements for the assurance of security, including a challenge function that is adequately resourced with SQEP personnel. The assurance arrangements should be Board-led, independent of security management and utilise an appropriate performance measurement framework. It should have the authority to undertake independent investigations and recommend improvements.

Inspectors should consider the following regarding the arrangements and their implementation:

- Is there an independent internal assurance function with clearly defined terms of reference (including responsibility, accountability and authority)? How does the Board demonstrate it uses this function and that it values its outputs?
- Does the dutyholder consider security assurance a key business delivery and is it a standing agenda item in their Board/management meetings?
- Is the internal regulation team adequately resourced with suitably competent personnel e.g. do they have knowledge of both security and assurance good practice?
- How does the dutyholder ensure the internal assurance team has sufficient authority and high-level support (including a route to escalate concerns to Board level)?
- Does the dutyholder undertake quality checks to ensure assurance reporting meets internal and external expectations and needs, in terms of understanding, timeliness, completeness and value?
- Does the internal assurance team have a process for sharing their feedback or providing copies of their inspection reports with other stakeholders including ONR?
- Is there a programme for internal inspections based on a coherent plan, with clearly identified priorities and documented within the dutyholder's management system?