ONR GUIDE			
SECURITY ASSURANCE PROCESSES			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-1.5 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Superintending Inspector	
Record Reference:	TRIM Folder 4.4.2.19071. (2017/100009)		
Revision commentary:	New Document Issued		

TABLE OF CONTENTS

Published 03/17

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account 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 (Reference 1).

1.2 The term 'security plan' is used to cover all dutyholder submissions such as nuclear 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 ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's security assurance processes. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets 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.

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.

3.2 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. ONR considers leadership and management for security to be an important component of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 Fundamental Principle J of the CPPNM refers to quality assurance and states that a quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied. The importance of issues relating to Governance and Leadership are also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12:

  a) developing, implementing and maintaining appropriate and effective integrated management systems including quality management systems; and

  h) 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.

4.3 A more detailed description of the Fundamental Principles and Essential Elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 2).

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS AND RELEVANT GOOD PRACTICE

5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder's security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder's submission demonstrating they have effective processes in place to achieve SyDP 1.5 – Assurance Processes, in support of FSyP 1 – Leadership and Management for Security. The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 5) describes the Cabinet Secretary's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs. This ensures that dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, SNI and the employment of appropriate personnel security controls both on and off nuclear premises.

5.3 The Classification Policy (Reference 6) indicates those categories of SNI, which require protection and the level of security classification to be applied.

5.4 A dutyholder's internal assurance capability is not exclusive to security performance but covers other key functions including safety and emergency preparedness. Therefore inspectors should draw from guidance both within and outside of the security programme area when considering the effectiveness of a dutyholder's security assurance processes. Of relevance are:

- TAG CNS-TAST-GD-015 - Guidance on the assessment of a dutyholder's security performance (Reference 8).

- TAG NS-TAST-GD-080 - Challenge Culture, Independent Challenge Capability and provision of Nuclear Safety Advice (Reference 9).

6. ADVICE TO INSPECTORS

The Nature and Purpose of Security Assurance

6.1 The dutyholder and senior managers should understand the nature of security assurance and its important position in regulation. To deliver a mature objectives-focused and risk-based approach to nuclear security, the dutyholder should have a well-developed strategy and process for internal assurance, including a 'challenge' function that is suitably resourced. That capability may be part of a wider integrated management system that meets a variety of needs in terms of oversight and regulation. This approach to regulation emphasises the importance of the dutyholder's governance arrangements, their ownership of risk management and placing less reliance on external regulation to provide assurance.

6.2 Challenge and advice are linked although there is a distinction between those directly supporting line management in an advisory function and those providing internal, but independent challenge. Ideally separate organisational teams should deliver these functions. The dutyholder should remain an 'intelligent customer' with sufficient internal expertise to do this work without relying on contractor support.

6.3 There are a number of prerequisites of a strong internal assurance process that meets the expectations of stakeholders:

- First, is strong governance that makes clear responsibilities and expectations at all levels within an organisation.

- Second, is a 'challenge culture' that is part of a wider organisational culture to encourage self-awareness, and a willingness to give and receive advice together with a questioning attitude and accountability for risk management.

- Third, to understand risk and the effectiveness of its management, Board members and senior managers need to have objective evidence-based feedback on security performance. The Board needs to have security competence, perhaps supported by an expert non-executive director or nuclear security committee, with oversight through some form of Audit, Risk and Assurance committee. Feedback, that shapes Board direction, is usually based on indicators and metrics drawn from audits, incident reports, penetration testing, exercises, competence testing, security cultural surveys, systems data, and organisational learning as well as outputs from periodic reviews. It is linked to a robust close-out arrangement that confirms effective action has taken place, issues have been resolved and there is an audit trail for what has been done.

- Fourth, that at all levels across a dutyholder's organisation; personnel adopt a challenge and security culture that has self-awareness and internal challenge at its core.

6.4 The purpose of security assurance is for an independent expert assessor, from outside the operational management chain, to be able to confirm that security objectives have been met to an adequate standard, the organisation is compliant with the law and corporately there is an expectation that the organisation is committed to continual improvement thereby consistently managing risks effectively. Externally, confidence in internal assurance assists regulators to fulfil their role in meeting government and public expectations.

6.5 Assurance should be part of a positive organisational culture and takes many forms. Line management assurance takes place at all levels albeit it is not independent. For example, there is an expectation that first-line supervisors would observe work, reinforce good practice and coach. Senior managers would hold performance review meetings. However, independent internal assurance is usually mandated corporately to reflect relevant good practice, and provide a view on the health of an organisation. External independent assurance is undertaken by national regulatory bodies including ONR. Assurance activity may be captured in an annual review of Safety, Security and Environment hosted by dutyholders when the organisation explains the outcome of their assurance to external regulators. This often takes the form of a review of operations considering: what went wrong, where good practice was delivered, areas for improvement, and priorities for the next reporting period.

6.6 A mature and proportionate assurance regime is an essential element of a dutyholder's approach to nuclear security and safety. Should the dutyholder's assurance regime not meet expectations, then ONR inspectors would consider further interventions to assess performance based on regulatory intelligence. However, the existence of an external regulator does not decrease the need for a dutyholder to develop an appropriate and credible internal independent assurance capability. In this way a combination of internal and external assurance holds the dutyholder to account, ensures compliance, and sets the conditions for improvement in managing risks.

Regulatory Expectation

6.7 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies clear security assurance arrangements, including a challenge function that is adequately resourced.

FSyP 1 - Leadership and Management for Security	Assurance Processes	SyDP 1.5
There should be evidence-based assurance processes in place to inform strategy through the Governance process, which welcomes challenge from across the organisation.		

7. WHAT IS ASSURED – SECURITY PERFORMANCE

7.1 In the context of the SyAPs, security performance, based on the security delivery principles, should be assured in order to provide evidence to senior leadership and key stakeholders that risks are being effectively controlled and compliance with regulatory requirements is being achieved. Reflecting relevant good practice, and as part of a good security culture, independent assurance should be Board-level led to help enable them to manage security performance effectively and in so doing meet regulatory expectations.

7.2 Dutyholders may assess and assure security performance based on a doctrinal framework and methodology, essentially a Performance Indicator framework that reflects industry good practice. Performance management includes security capability and its delivery (processes, decision making and behaviours). That capability is captured in the security plan, which the dutyholder should ensure is effective, provide assurance to that effect or otherwise, and provide evidence of its effectiveness to ONR and/or other regulators. Thus the outcome of assurance is to certify compliance with the security plan and its delivery as well as demonstrating a mind-set of continuous improvement. In that way the expectations of stakeholders, including the regulator and hence public, are addressed.

8. METHODS TO ASSURE SECURITY PERFORMANCE

8.1 ONR inspectors will regulate against dutyholder's arrangements throughout the reporting year based on information from their own activities, including interventions. These interventions will be shaped by the dutyholder's own assurance activity. Feedback from the dutyholder enables external regulation to be proportionate and targeted, making best use of resources.

8.2 In carrying out assurance, the assessment of performance should be evidence-based, not simple assertions, and drawn from analysing both qualitative and quantitative data. Drawing from nuclear safety advice on 'challenge' (NS-TAST-GD-080 Revision 2), the dutyholder should show evidence of an ability to deliver a mature and proportionate assurance regime.

Inspectors should consider:

- Is there an independent internal assurance function with clearly defined terms of reference (including responsibility, accountability and authority)? It should be valued by and used at Board level. It should also be understood and accepted at all levels of management as providing an independent assessment of performance and allow continuous improvement. Should a dutyholder have an internal regulation team covering Environment, Health, Safety, Security and Quality, then all aspects, including Security should be adequately resourced with suitably competent personnel, to ensure effective internal regulation that will provide the assurance ONR seeks. A competency matrix for the role should be available to assess the quality (objectivity and integrity) of those carrying out internal assurance as this, along with other factors, will shape ONR regulatory effort.

- Are personnel undertaking assurance demonstratively independent from the operational line of management and have sufficient authority and high level support together with credibility with the regulator? (including a route to escalate concerns to Board level).

- Is there a suitable framework and lexicon, drawing on SyAPs, on which to judge and communicate performance based on an assessment of security delivery, planning and culture?

- Does a Performance Indicator framework exist and does it reflect industry good practice?

- Is the scope of internal assurance explained? The scope should cover the whole security regime, confirm it reflects the SyAPs, and has a performance indicator framework. As necessary, it should be targeted, based on inspections and audits, review of documentation together with assessment of routine 'surveillance' gathered from performance data, and incident reporting along with pertinent regulatory inputs. Internal investigations to establish the causes of events, together with corrective actions and dissemination of organisational learning, could be included as appropriate within the assurance function.

- Is there ownership and understanding at Board and Executive Management level? Security assurance is considered a key business delivery and is a standing agenda item at their meetings to ensure security is given adequate consideration in decision making? Senior leadership should ensure that the assurance capability is independent, authorised, resourced, integrated into business practices and reports regularly at Board level. If the internal assurance capability is considered to be immature, then there should be a plan in place to develop that capability. The Board itself should be an 'intelligent customer' with sufficient security competence/advice to ensure assurance reports assist it in effective decision making.

- Is there an internal, independent, suitably qualified and experienced team of assessors, organised to provide the necessary expertise across security functions, with access to all levels of management? The team should understand what is assessed and how to deliver assurance. It should be appropriately knowledgeable in security matters to be sufficiently questioning, able to approach an issue from alternative perspectives and challenge the underlying logic for an idea or action. They should demonstrate knowledge of assurance good practice based on sources of relevant good practice and guidance. Those carrying out internal assurance should have their competence measured against technical, behavioural and influencing skills.

- Are there mechanisms in place to identify under-performance, gaps in good practice and the causes? Once assessed there should be a reporting process to ensure different levels of management are made aware of findings according to relative importance. Assurance teams may also provide guidance on how issues might be addressed but they do not own the risk, nor should they directly challenge the authority of operational management.

- Whether there are quality checks to ensure assurance reporting meets internal and external expectations and needs, in terms of understanding, timeliness, completeness, and value? That reports are evidence based, consistent with good practice and proportionate. Assurance outputs will indicate both good and bad practice, and may include advice. Although the duty rests with the dutyholder's management to rectify any adverse situation, acting as an intelligent customer, they may use suitably experienced personnel, such as human performance and factors experts, industry groups and government authorities (e.g. Centre for the Protection of National Infrastructure).

- Do the internal assurance team have a process for sharing their feedback with other stakeholders? For interaction with ONR, that might be through Level 4 meetings, or providing copies of their inspection reports. High quality feedback should shape ONR's own activities and its judgements on the efficacy of dutyholders' internal regulation. A dutyholder normally holds a formal annual review for safety, security and environment. It is an opportunity for dutyholders' senior managers to review their performance over the previous year, provide self-assessment, and seek comment from both internal assurance and regulators.

- Is there a programme for internal inspections based on a coherent plan and with clearly identified priorities? That the activity is documented within the dutyholder's management system? The internal assurance regime should add value and visibly support the improvements to the dutyholder's performance.

9. REFERENCES

1. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403

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. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.

3. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

4. **Convention on the Physical Protection of Nuclear Material (CPPNM)** https://ola.iaea.org/ola/treaties/documents/FullText.pdf

5. **HMG Security Policy Framework**. Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

6. **NISR 2003 Classification Policy** – Trim Ref. 2012/243357.

7. **Security Assessment Principles** – Trim Ref. 2017/121036

8. **TAG CNS-TAST-GD-015** - Guidance on the assessment of a dutyholder's security performance.

9. **TAG NS-TAST-GD-080** - Challenge culture, Independent Challenge Capability and provision of Nuclear Safety Advice.

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

10. GLOSSARY AND ABBREVIATIONS

CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide