ONR GUIDE			
ORGANISATIONAL LEARNING FOR SECURITY			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-1.4 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19071. (2017/100007)		
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 organisational learning arrangements. 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 The importance of issues relating to organisational learning are also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 11: Planning for, Preparedness for, and Response to, a Nuclear Security Event - 3.11 biii) Feedback into the preparedness process,

including into the response plans, the results of exercises and tests of the plans, and of experience; and,

- Essential Element 12: Sustaining a Nuclear Security Regime - 3.12 f) Having in place processes for using best practices and lessons learned from experience.

4.3 A more detailed description of the 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).

4.4 Furthermore, the IAEA defines a *near miss* as "a potentially significant event that could have occurred as the consequence of a sequence of actual occurrences but did not occur owing to the plant conditions prevailing at the time." Similarly, it defines a *low-level event* as a "discovery of a weakness or a deficiency that would have caused an undesirable effect but did not, due to the existence of one (or more) defence in depth barriers." Although originating within safety standards, the definition has equal applicability within security.

4.5 Comprehensive guidance on the development of a system for feedback of experience from events in nuclear installations is set out in the IAEA Safety guide on that topic in NS-G-2.11 (Reference 8). It focuses on the main components of systems for the feedback of operational experience for gathering relevant information on events and abnormal conditions that have occurred at nuclear sites and investigation and analysis of those events including corrective actions and learning from experience.

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

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 1.4 – Organisational Learning, 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.

6. ADVICE TO INSPECTORS

6.1 An organisational learning programme is an important process which enables a dutyholder to maintain and improve efficiency and enhance nuclear security. Furthermore, it is recognised by ONR as a key element of a nuclear industry that has a culture of continuous improvement and sustained excellence in operations.

6.2 Organisational Learning is more than just learning from individual events or learning for learning's sake – it is the engine that drives improvement and is relevant in all business

areas and sectors including nuclear safety. There are two important aspects; an ability to identify learning opportunities, crucially combined with a commitment to take action. Both of these aspects are significantly influenced by the working environment and culture in any organisation or team. The culture is set by the leadership within the organisation: setting expectations, leading by example (by applying learning to their own behaviours and activities), driving learning activities, realising learning opportunities through managed change, and recognising and rewarding improvements.

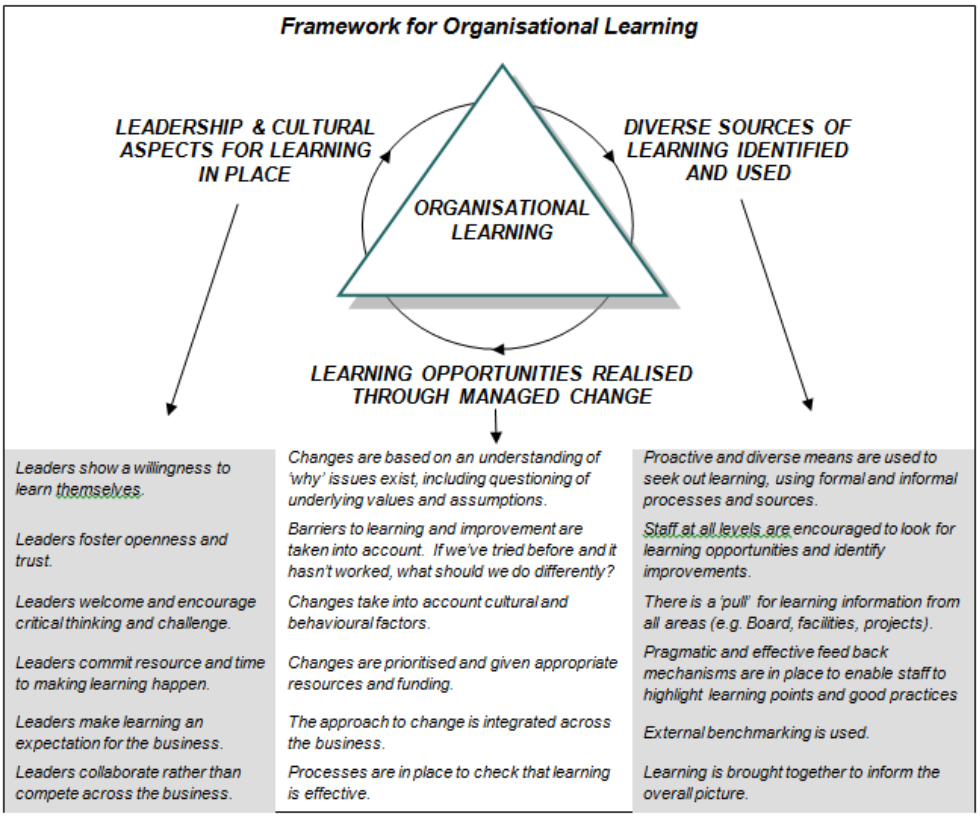
Regulatory Expectations

6.3 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies a clear structure, framework and processes that support organisational learning.

FSyP 1 - Leadership and Management for Security	Organisational Learning	SyDP 1.4
Lessons should be learned from internal and external sources to continually improve leadership, organisational capability, the management system, security decision making and security performance.		

7. FRAMEWORK FOR OPERATIONAL LEARNING

7.1 The diagram below shows a framework and essential components that support operational learning.



Component One – Leadership and Cultural aspects for Learning in place

7.2 Effective learning involves reviewing and changing processes and behaviours at all levels, starting with the Board and senior management. A fundamental requirement for an organisation to learn from its experience is senior management commitment. In the first instance this takes the form of a policy statement that clearly explains the dutyholder's commitment to the prevention of security events by applying lessons learned from previous operating experience whether internal or external. This commitment should be underpinned by adequate resourcing of the function, management prioritisation of lessons identified and ongoing monitoring of action plans to ensure issues identified are addressed.

Component Two – Diverse sources of Learning identified and used

7.3 Formal processes such as Operational Experience (OpEx) programmes play an important role in supporting Organisational Learning, however global experience shows that they form only part of the overall picture. A Learning Organisation also seeks out broader, diverse opportunities for learning from a wide range of sources (internal and external) and brings these together to draw out the learning and make improvements. This includes: tapping into the ideas, energy and concerns of those at all levels in the business, continually scanning across sectors for learning and good practices, and actively seeking advice or benchmarks (e.g. through peer reviews).

Component Three – Learning opportunities realised through Managed Change

7.4 To complete the cycle, organisations have to invest the necessary resources to implement changes in order to apply the lessons. Having information that can drive learning and then having the willingness and ability to use it effectively are distinctly different attributes. Many organisations, particularly in the nuclear sector, have well established processes for obtaining and disseminating information (e.g. OpEx). However, effort is needed to integrate diverse sources of information and define effective and prioritised actions that improve security.

8. OPERATIONAL EXPERIENCE

8.1 OpEx is an important part of organisational learning. The objective of OpEx is to proactively collect, document, organise, analyse and apply previous learning whether it relates to equipment, personnel or procedures. Such learning extends from a number of sources, the dutyholder's organisation, other operators, industry groups, governments and scientific and educational institutions.

8.2 Dutyholders should have a system that identifies and collects pertinent information on security events and adverse conditions in a timely manner. These include any deviation from the site's security arrangements in the security plan or events that could have led to a security vulnerability developing. Adverse conditions include any deviation (e.g. a noticeable or marked departure from the expected norm), abnormality, equipment/human failure or non-conformity to procedure, and information, that relates to breakdowns or conditions that resulted in no serious consequences, but reduced the layers of defence. All personnel at the dutyholder's site (staff, contractors, agency workers) should be expected to report all security events and adverse conditions.

8.3 To ensure all events and incidents which could affect security are captured, the dutyholder should establish clear reporting criteria with low tolerability thresholds. The issues should be analysed in sufficient depth to facilitate the identification of root causes and action plans implemented to address the issue. An effective learning organisation will share its experiences, both internally and externally. It is recognised that the sharing of learning from security events will need to be controlled especially where security vulnerabilities are identified. Nevertheless, there are a number of CPNI industry forums where this is possible.

9. EVENT AND ADVERSE CONDITION REPORTING AND TRACKING

9.1 The dutyholder should establish a process for all employees at the dutyholder site to identify security deficiencies as well as improvement suggestions. A confidential means should be established for security staff to identify and track events and adverse conditions that are considered to potentially identify an exploitable vulnerability in the security systems or processes. Managers should constantly reinforce the requirement to report all events and adverse conditions that occur within the organisation. All events and adverse conditions that affect security should be reported and tracked, including low-level events and “near misses".

9.2 In addition to having in place processes and procedures to learn from security events, dutyholders have a legal obligation to report security events as required by the NISR 2003 Regulations 10, 18 and 22. ONR therefore expects security events meeting reporting criteria specified in NISR and the ONR Guide on this matter [ONR-OPEX-GD-001 Revision 5] (Reference 9), to be reported as specified. This includes the findings from dutyholders investigations and Learning from Experience reports.

10. SCREENING FOR SIGNIFICANCE

10.1 The dutyholder should screen event information to ensure that all security significant matters are considered and that all applicable lessons learned are taken into account. The screening process should be used to select events for detailed investigation and analysis. A categorisation system should be developed that grades events and conditions that cover a range of risks resulting in prioritisation according to security significance and the identification of adverse trends.

11. INVESTIGATION AND ANALYSIS

11.1 Dutyholders should have a policy and procedures specifying the type of investigation that is appropriate for an event of a particular category. The policy should typically outline the means of initiating an investigation, its duration, the composition of the investigating team, terms of reference for the investigation team and how it is to report. Investigations are to be performed promptly so that information and physical evidence is not lost or corrupted. Event participants are to be interviewed while memories are fresh. A typical outline of the investigation process is at Appendix 1.

11.2 Highly significant events should be evaluated by a formally qualified multi-disciplinary evaluator team using structured root cause investigation methods. The objective is to identify the root causes so that when they are corrected, the event or condition should not be repeated. Lower significance events or adverse conditions can be assessed with less formality and rigour. For example individual expert evaluators can be used rather than a multi-disciplinary team. The objective is to identify likely or apparent causes that when corrected should prevent recurrence; however, there is an acceptance that repeat events are still possible.

11.3 The analysis of any event should be performed by an appropriate method. It is common practice that organisations who regularly conduct evaluations use standard methods to achieve a consistent approach for the assessment of events. These standard methods usually involve different techniques - each may have its particular advantages for cause analysis, depending on the issue under investigation.

12. CORRECTIVE ACTION MANAGEMENT

12.1 Actions taken in response to events constitute the main basis of the process of feedback of operational experience to enhance security at dutyholders' sites. Such actions are aimed at primarily correcting a situation, preventing a recurrence or improving the security arrangements. Corrective actions may also be identified to improve security management systems and culture, particularly where there is evidence of complacency.

12.2 Corrective actions should as appropriate:

- be specific and practical;
- address fundamental causes and not symptoms;
- include immediate actions that decrease the risk of a subsequent event or adverse condition;
- include long term actions that should be taken to achieve a permanent solution; and,
- focus on strengthening existing security arrangements in preference to developing new ones.

12.3 Recurring events warrant special attention when compared to single events, such as increasing the significance level of the event. The assessment of root causes should identify why previously completed corrective actions failed to prevent a reoccurrence of the event. The reason for the original corrective action not being effective should be addressed as part of the follow up.

12.4 The dutyholder should ensure the dates that are assigned to complete each corrective action are commensurate with the importance of the action, organisational priorities, and consideration of avoiding recurrence. Actions should be tracked and the responsible persons held accountable for completing them according to agreed timescales.

13. USE AND DISSEMINATION OF INFORMATION

13.1 Information on operational experience should be made readily accessible to all security staff and where appropriate, all employees, for example, procedures to correctly secure SNI to reduce the likelihood of repeat events. This can be done in a number of ways such as team briefings. Effective use of the feedback from operational experience should be actively encouraged and reinforced by the management chain. Lessons identified should also be included in the dutyholder's refresher training material.

13.2 Where the event has resulted in a reportable event under NISR 2003 (as amended), a follow up report should be sent to ONR.

Inspectors should consider:

- Does the dutyholder have a framework for organisational learning that incorporates the three essential components?
- Whether the dutyholder has a policy for systematically identifying and correcting deficiencies in security?
- If the dutyholder's security and safety OPEX policies are effectively aligned?
- Whether the dutyholder encourages staff to report security deficiencies and security improvement opportunities?

- If the dutyholder's policies focus on corrective action rather than blame, towards personnel who report security deficiencies?
- Whether the dutyholder encourages a learning organisation through actively seeking lessons learned from other organisations and, where appropriate, apply them to their organisation?
- Whether the dutyholder regularly debriefs staff on recent security issues that have occurred at the facility and draw on lessons identified to refresh staff understanding?
- Whether the dutyholder has sufficient training for staff and management to recognise and report problems and enough experienced staff trained in root cause analysis to fully assess all security deficiencies that are reported?
- If the dutyholder has adequate resources allocated to managing and reporting security deficiencies and whether they are compliant with legislation and the ONR mandated reporting process?
- If the dutyholder's process informs their Board on the findings of identified security deficiencies including analysis of the event and emerging trends?
- Are there indicators regarding backlogs in event investigations and corrective action closure, looking particularly for adverse trends?

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

9. **ONR Document ONR-OPEX-GD-001 Revision 5.** Notifying and Reporting Incidents and Events to ONR

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

15. 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
L&MFSy	Leadership and Management for Security
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
OpEx	Operational Experience
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide

APPENDIX 1: INVESTIGATION OF EVENTS

A1.1. The level of management to which investigators report should depend on the severity (or the potential severity) and the frequency of occurrence of the event concerned. A minor event that reoccurs should be investigated as if they were a more serious event to determine the root cause.

A1.2. The number of investigators and their areas of expertise should be based on the nature of the security incident (e.g. a Human Factors specialist might be involved in access control breaches or a C&I specialist on a security breach on an Operating Technology (OT) system).

A1.3. Training (both initial and refresher) should be provided for the staff who might take part in an investigation. This should include training in investigation techniques, documentation needs, witness interviews, conflict resolution and dealing with confidentiality issues. Whereas all investigators should receive some basic training in event investigation, including root cause analysis, for more difficult and complex investigations there may need to be at least one expert facilitator who is familiar with such methods of investigation.

A1.4. A mandate should be established for the investigation activities. This should set out the format and terms of reference and should typically cover the following areas:

- conditions preceding the event;
- the sequence of events;
- security equipment performance and system response;
- considerations of human performance;
- equipment failures;
- precursors to the event;
- response and follow-up at the plant;
- threat considerations;
- considerations relating to the regulatory process; and
- security significance.

A1.5. The mandate should include a review of the security plan as part of the assessment of causes of the event under investigation or to identify a security response that is beyond that approved in the security plan.

A1.6. The event investigator (or the lead investigator if there is more than one) should be competent in investigation skills as well as having technical, administrative and managerial competence.

A1.7. The on-site investigation should be commenced as soon as practicable to ensure that information is not lost or diminished and evidence is not degraded. It is vital that the on-site investigation does not inhibit operational staff from bringing the plant to a stable state.

A1.8. Interviews should be conducted with all the staff who were involved in the event or who were witnesses to the event. Interviews should be transcribed. A “sequence of events listing” (e.g. an event and causal factors chart) should be started immediately and should be continuously updated as new data are obtained.

A1.9. Investigators should prepare a written report and should present it to the management group that commissioned the investigation. In some cases there may be a request for corrective actions to be taken to remedy the identified root causes.

A1.10. The investigation should include:

- preparing progress reports and other interim reports documenting significant activities, findings and concerns;
- ensuring safety and security, as appropriate, at the scene of the incident;
- ensuring that the investigative activities do not result in adverse impacts on safety or security;
- ensuring an appropriate chain of custody of any evidence gathered;
- ensuring that the dutyholder management is advised of the status of the investigation and of progress and future plans in relation to it; and,
- initiating requests for information, interviews with witnesses, laboratory tests and technical or administrative support.

A1.11. It is not the objective of an event investigation to apportion blame, to determine fault, or to recommend or dispense disciplinary actions. Conducting investigations in such a way is not conducive to establishing the facts that will assist in the identification of root causes, and hence lead to the corrective actions necessary to enhance security and to improve the performance of equipment and human performance.

APPENDIX 2: ANALYSIS OF EVENTS

A2.1 In most instances the first step in the analysis of an event and the basis for further evaluation is the establishment of the event sequence. This means the listing in chronological order of all relevant occurrences or activities leading to the event and subsequent to it.

A2.2 On the basis of the event sequence, all deviations of conditions from the standard operating procedure or design specification should be determined as far as possible. The occurrences and activities that should be analysed in depth can thus be identified. Different areas should be considered in the analysis, such as design, organization, procedures, human actions, component faults and behaviour of materials. In some cases the involvement of additional expertise in the cause analysis should be considered. Very often the notions of immediate (direct, observed) causes, root causes and contributing factors are used in the cause analysis. Cause identification should be carried out for the formulation of corrective actions. The depth of the causal analysis should be adequate for ensuring the determination of appropriate corrective actions.

A2.3 Numerous methods of root cause analysis, many having a similar basis, have been developed or are under development for addressing the connection between root causes and corrective actions. Since there is no single best technique for use for all events, the evaluator should select the most appropriate tool for use in the event in question.

A2.4 The analysis of events relating to human characteristics should include the causes and circumstances of any problems with human performance that contributed to the event. Human errors that affected the course of the event may include either errors of commission or errors of omission. There may also have been procedural deficiencies, and there may have been a combination of human errors and procedural deficiencies. There may have been errors and human performance related issues in the areas of procedures, training, communication, engineering for human factors and the human–machine interface, management, and supervision. The analysis should be sufficient to categorise the human performance issues.

A2.5 The analysis should consider and resolve the following issues:

- Whether human errors were cognitive (such as failure to recognise the actual security event/situation, failure to realise which systems should be functioning or failure to recognise the true nature of the event), or whether there was an error in following procedures;
- whether human deficiencies in the use of procedures were characterised by difficulty either in terms of failure to follow an approved procedure, or in the use of a procedure that contained erroneous instructions, or were associated with an activity or task that was not adequately covered by a procedure;
- whether any unusual characteristic of the working location, such as heat, humidity, noise, radioactivity levels, accessibility or signage contributed to the problem with human performance;
- whether there were any ergonomic issues, or issues relating to engineering for human factors; and,
- the type of personnel involved (such as a security guard, a contractor's escort, security management – especially to what level were they SQEP).