| ONR GUIDE | | | |
|---|---|---|---|
| **MEASUREMENT OF COMPETENCE** | | | |
| **Document Type:** | Nuclear Security Technical Assessment Guide | | |
| **Unique Document ID and Revision No:** | CNS-TAST-GD-3.3 Revision 2 | | |
| **Date Issued:** | March 2020 | **Review Date:** | March 2022 |
| **Approved by:** | Matt Sims | Professional Lead | |
| **Record Reference:** | CM9 Folder 4.4.2.23373. (2019/135614) | | |
| **Revision commentary:** | Administrative review in line with ongoing review of Security Assessment Principles | | |

## TABLE OF CONTENTS




Published 03/20

## 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 arrangements to measure the competence of its workforce undertaking security roles. 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 competence management 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 workforce competence are also recognised in the Nuclear Security Fundamentals, specifically:

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

  d) Allocating sufficient human, financial and technical resources to carry out the organisation's nuclear security responsibilities on a continuing basis using a risk-informed approach; and

  e) Routinely conducting maintenance, training, and evaluation to ensure the effectiveness of the nuclear security systems.

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). This publication highlights the importance of sustainability programmes to ensure that physical protection regimes are resilient and effective in the long term through adequate resourcing. With respect to competence management it advises that operators, shippers and carriers should establish sustainability programmes for their physical protection system, which should encompass human resource management and training.

4.4 The IAEA also publishes NSS 12 'Educational Programme in Nuclear Security' (Reference 14). It is intended for a range of practitioners with responsibility for nuclear security including university curriculum developers, nuclear security instructors and human resource development managers. The scope of this publication is broad and covers education in all areas of nuclear security, ranging from MSc programmes to develop highly educated staff with in-depth knowledge to a programme for developing certified nuclear security specialists.

4.5 This TAG is consistent with the Systematic Approach to Training, advocated by the IAEA in Technical Document 1254 (Reference 9), and implicit in other publications.

## 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 3.3 – Measurement of Competence, in support of FSyP 3 – Competence Management. 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 Competencies are groups of related knowledge, skills and attitudes (KSAs) needed by a person to perform a particular job. Knowledge represents the depth and breadth of absorbed and retained information by the mental faculty of a person that enables that person to deal with different situations, changes, and unexpected events. Skills are the demonstrated abilities and expertness of a person to perform a task to prescribed standards as judged by an evaluator. Attitude is the appreciation and the practiced behaviour of a person to perform a job or task with due diligence. Competencies are often wrongly expressed in a format that relates more to a description of an activity or a task. Competencies are the mental, physical and behavioural tools with which an activity or a task is executed.

6.2 A simple way to differentiate between a task and a competency is to consider whether the statement describing a competency can be used to perform a task or is it a description of the task itself? For example, for a security manager to perform the task of reviewing a particular part of a security report, a required competency would involve knowledge of the threat, being cognisant of the associated adversary path analysis and the capability and limitations of the guard force (reaction force) to interdict an adversary, together with the detection and delay capability of the site's security equipment in its various modes of operation. Another competency would be effective written communication in order to report their findings and make recommendations.

6.3 It is essential that personnel whose activities have the potential to impact on nuclear security are Suitably Qualified and Experienced (SQEP) to carry out their jobs. This includes those who directly carry out security operations and others such as directors, managers, designers, security plan authors, etc, whose roles, if inadequately conceived or executed, may affect security in less obvious ways. For example, introducing latent technical or organisational vulnerabilities. Dutyholders should, therefore, put in place robust arrangements for identifying their competence needs and ensuring these are met and maintained. The arrangements should clearly define the dutyholder's interpretation of SQEP, and identify those personnel required to be SQEP.

6.4 To assist the nuclear sector in identifying security competencies, the National Skills Academy Nuclear (NSAN) has developed 21 high level competencies covering core security areas, which are available on the Nuclear Training Network (NTN) (www.nucleartrainingnetwork.com) and via the NS4P Skills Competence Management System (www.ns4p.co.uk), reproduced in Appendix 1 (Reference 13). They do not all apply to every individual with security responsibilities, but form a useful framework for developing core competencies for specific roles. These competencies are available to NSAN members on the NS4P network. Staff discharging nuclear security roles should be included within the dutyholder's organisational baseline, see NS-TAST-GD-065 (Reference 12) and TAG 1.2.

6.5 Training is a fundamental mechanism through which personnel acquire and maintain the skills and knowledge needed to perform a job to defined standards. Training is instrumental in developing and sustaining competence. IAEA has defined

competence as “the ability to put skills and knowledge into practice in order to perform a job in an effective and efficient manner to an established standard” (Reference 8). ONR supports this definition, which is widely accepted within the international nuclear community. Other factors contributing to a person’s competence include their prior experience, aptitude, attitude, behaviours, skills and qualifications. Competence can therefore broadly be equated to SQEP. Dutyholders should have arrangements in place to define and deliver the training needed to sustain competence, and these arrangements should be defined in their security plan.

6.6 Dutyholders should establish processes that provide them with confidence that personnel whose actions have the potential to impact upon nuclear security, meet its competence expectations. An individual’s competence should be subject to periodic review and supported by a well-defined system for monitoring effectiveness, and identifying training and development requirements.

6.7 ONR does not assess the competence of dutyholder staff (e.g. security guards or control room operators) directly, or authorise them. Rather, ONR seeks confidence that dutyholders have in place, and are implementing, effective and proportionate arrangements for training and confirming the competence of all personnel whose activities may impact upon security. This should cover both dutyholder employees and others such as contracted elements of the workforce, whose actions could impact upon nuclear security A well-designed training and competence management system should adequately address the following elements:

- Analysis of roles and their associated competencies
- Assessment of competence (gap analysis)
- Identification of learning objectives and training needs
- Training programme design
- Selection of appropriate training staff, methods and media
- Evaluation of training effectiveness
- Organisation and support of the training function
- Knowledge management and capture
- A process to measure, assess and improve the competence management arrangements

6.8 This guidance should be applied in a proportionate and targeted manner. This assessment guide focuses on the assessment of competence and evaluation of training effectiveness. It presents a summary of the reasons why these are important components of a dutyholder’s training arrangements and sets out the principal factors which should be considered by the ONR inspector when assessing an organisation’s security competence measurement.

6.9 The emphasis that the inspector gives to assessing different elements of a dutyholder’s training and competence arrangements will depend upon the plan being assessed. For example, where the tasks involved in carrying out a role are already well-defined, it may not be necessary to closely scrutinise the processes used to analyse the role and define its competence and training needs. Conversely, where new activities are being developed, closer examination of the approach which the

dutyholder takes to analysing these factors may be appropriate. As an overriding principle, the inspector should consider the security significance (as effected by aspects including security function category or the categorisation for theft or sabotage) of the activities concerned and adopt a proportionate and targeted approach to applying the guidance in this document.

**Regulatory Expectation**

6.10 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies how they adopt a systematic approach to training that incorporates measurement of competence as part of an ongoing commitment that personnel whose activities have the potential to impact on nuclear security are SQEP to carry out their jobs.

| **FSyP 3 - Competence Management** | Measurement of Competence | SyDP 3.3 |
|---|---|---|
| Dutyholders should implement and maintain a process of assessment which provides confidence that all personnel whose actions have the potential to impact upon nuclear security meet defined competence expectations. | | |

## 7. ASSESSMENT OF COMPETENCE

7.1 Each person who carries out activities which may affect the security of a nuclear facility or site should be suitably qualified and experienced (SQEP). For some posts it may also be necessary to designate persons who control and supervise operations that may affect security as Duly Authorised Persons for Security Purposes (DAPSyPs). Although training plays an important role in developing the necessary competencies to become a SQEP or DAPSyP, it does not itself guarantee competence: if training is poorly specified or targeted, or the trainee is not suited to the job, then a person may fail to achieve an acceptable level of performance.

7.2 For these reasons, ONR regards the assessment of a trainee's competence and, subsequently, the periodic re-assessment of personnel, as a key element in the process of developing and maintaining the competencies needed to function as a SQEP or a DAPSyP. When properly defined and carried out, assessment serves the following important functions:

- Demonstrating that learning objectives have been achieved and a level of competence attained
- Identifying the need for refresher or additional training through identifying shortfalls in performance
- Indicating whether training has been effective in developing the required competencies. In particular, assessment can point to deficiencies in identifying training needs (gap analysis), the choice of training methods or the training programme

7.3 Dutyholders should, therefore, satisfy themselves that all staff and contractors whose actions have the potential to impact upon nuclear security meet their competence

criteria. When an individual is first appointed to a role they may not be fully competent to carry out all the duties expected of them. Thus the competence assessment process should be used to inform a management decision to restrict the individual's range of tasks to those for which they are competent (e.g. a C&I engineer may be competent to assess security vulnerabilities on most instrumentation but may not be confirmed as SQEP to monitor these systems in a site security control room and control the security response). A dutyholder's management team should positively encourage staff and contractors to raise any concerns about their own competence or readiness to carry out a task and to seek further training or advice as necessary.

**Assessment methods**

7.4 Dutyholders may use a range of different assessment methods. Their suitability will depend upon the training method and the nature of the competency being assessed. Traditional assessment methods that use paper-based question and answers may be appropriate for some activities, but will be quite inappropriate for many others. For example, they might be a sound means of assessing an understanding of prohibited items, but would not necessarily give an accurate indication of an individual's practical competence to undertake effective searching to prevent the introduction of prohibited items onto site or into sensitive areas. Assessment may take place on-the-job, within a controlled training/assessment environment, or in a workshop or a classroom. It may take place as a specific, defined activity or through continual assessment during training or performance in role. An overview of issues relating to competence assessment is provided in the IAEA Safety Report on Regulatory Body Competence (Reference10).

7.5 In some circumstances, the dutyholder may wish formally to waive some parts of training. Such waivers should be kept to a minimum, but where training is waived, the dutyholder should still assess the affected person(s) to the same, or an equivalent, standard. This provides a basis for confirming that the person is competent, despite their not receiving the waived part of training. Where a contractor takes credit for prior training and the associated competences, the dutyholder should be able to show how it has satisfied itself that the contractor's training and competence assurance arrangements are adequate, and confirm that they meet the dutyholder's expectations.

7.6 Assessment may involve carrying out real or simulated tasks, which have been shown, or are judged by the dutyholder, to be representative of the real job demands. As such, assessment methods can include written, oral or practical demonstrations of learning or competence. It is preferable that assessment is carried out by persons independent of the training itself. Some of the merits and disadvantages of different approaches to assessment are discussed in the IAEA guidance on managing a regulatory body's competence (Reference 9).

7.7 Regardless of the assessment method used, the dutyholder should be able to demonstrate that it is:

- **Valid -** i.e. it provides a reasonable indication of a person's likely performance on the real job. The criteria used to judge performance should therefore remain under constant review by the dutyholder

- **Objective -** i.e. the less judgmental the assessment method and the criteria used to judge performance are, the less uncertainty there will be about the validity of the assessment. This is of particular relevance to on-job assessment

- **Reliable -** i.e. if repeated, the assessment would be likely to produce consistent results

**Frequency of assessment**

7.8 Assessment should not be regarded as a one-off activity that takes place after initial training, and then 'qualifies' a person for the period that they subsequently remain in post. A person's competence may change over time as a result of influences such as the frequency with which a task is performed, the varying circumstances under which the task may be performed, or changes to plant or equipment. Loss of memory for the task and the procedures or arrangements which affect how it is performed may also be compounded by factors such as the development of bad habits, short-cuts etc. Changes to security system parameters or procedures may also take place when a person is away for an extended period and so affect their performance when they return to duty in a particular role. All these factors support the case for periodic re-assessment to ensure that personnel know about relevant changes to their working environment, and that they remain competent to carry out their jobs.

7.9 The frequency of re-assessment should be influenced by consideration of the following issues:

- The security significance of the roles and associated tasks which the person performs, as identified through the job and task analysis

- The frequency with which the tasks are performed

- The nature of the task (including whether it changes) and the inherent likelihood of loss of competence over time

- Upgrades to the security technology necessitating new competencies

- Operational experience feedback originating both within the dutyholder and from other organisations

- Compliance with national standards or by those of accredited or authoritative bodies

**Inspectors should consider:**

- Does the dutyholder have formally-defined provisions for assessing the competencies of all personnel whose activities impact upon security?

- Has the dutyholder put in place robust processes to confirm its contractors are competent where they are not subject to the dutyholder's own competence assessments?

- Is assessment carried out during and/or after training?
- Where possible, is the assessment carried out by a person who is independent of the training which the trainee has received?
- Does the choice of assessment method reflect the nature of the competencies which are being assessed, and the training methods and media which are available?
- Can the dutyholder demonstrate that their assessment methods provide a valid, objective and reliable basis for determining competence?
- Does the dutyholder act, in a timely manner, upon deficiencies in performance identified through the assessment or during training?
- Has the dutyholder defined the periodicity of re-assessment which is appropriate for each job or task?
- Does the frequency of re-assessment take account of factors such as the security significance of the task, the nature of the task and the frequency with which it is performed, plant/procedural changes and operational experience?
- Is re-assessment carried out in accordance with the dutyholder's defined processes?
- Does the dutyholder maintain some form of training and assessment log that can demonstrate its procedures are being followed?
- Does the dutyholder have a defined strategy for addressing failures to meet the required standards following training?

## 8. EVALUATION OF TRAINING EFFECTIVENESS

8.1 Training is effective only in as much as the learning acquired through training transfers into the real situation. For example, security control centre training is of limited benefit if it provides trainees with the skills needed to operate the alternate but not the main security control centre. Similarly, classroom training which enables students to understand the effects of blast is, in itself, insufficient to develop operational competence in responding to suspicious packages. Dutyholders should therefore have a well-defined system for monitoring the effectiveness of training, and for identifying areas where training may need to be augmented or revised.

8.2 Evaluation of training effectiveness involves an intelligence gathering exercise, the purpose of which is to provide confidence that training has been specified properly, and that it is comprehensive, effective and up to date. As such, it should draw on a range of sources such as:

- Operational experience feedback from the workplace and from other plants
- Performance measures from the site

- Security reviews and inspections
- Security operating procedures and administrative arrangements
- Revised information on training needs
- Summaries of assessments of trainees, including trainee feedback
- Changes in regulatory aspects, plant or procedures
- Independent reviews, such as those by peers under the auspices of organisations such as IAEA (IPPAS missions)

8.3 Evaluation of training effectiveness should include review of both individual elements of training as well as the scope of overarching training programmes.

8.4 The inspector should be satisfied that the dutyholder is 'closing the loop' by monitoring the systems which have been put in place to evaluate the effectiveness of each element of training. Where shortfalls in training are identified (for example, via event investigations), consideration should be given to which system elements have contributed to the shortfall, and how the system or process itself can be strengthened.

**Inspectors should consider:**

- Does the dutyholder have in place a formal process to evaluate the effectiveness of training?
- Does the evaluation process take account of information gained through factors such as operational experience feedback, trainees, instructors, plant procedures, security reviews and inspections?
- Is the way in which training is specified, delivered and assessed monitored regularly?
- Does the evaluation aim to gain information on the effectiveness of all the elements of training?
- Do the findings of the evaluation process demonstrably influence the specification or implementation of the training arrangements?

## 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. **Classification Policy for the Civil Nuclear Industry.** ONR. http://www.onr.org.uk/documents/classification-policy.pdf

7. **Security Assessment Principles for the Civil Nuclear Industry.** ONR. http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

8. **IAEA Safety Standard Series NS-G-2.8**. Recruitment, Qualification and Training or Personnel for Nuclear Power Plants. November 2002.

9. **IAEA –TECDOC-1254**. Training the Staff of the Regulatory body for Nuclear Facilities. November 2001.

10. **IAEA Safety Report No.79**. Managing the Regulatory Bodies Competence. December 2013.

11. **ONR Document NS-TAST-GD-027 Revision 4**. Training and Assuring Personnel Competence 15

12. **ONR Document NS-TAST-GD-065**. Function and Content of a Nuclear Baseline

13. **NSAN Master Security Competencies** as available on the Nuclear Training Network (NTN) (www.nucleartrainingnetwork.com) and via the NS4P Skills Competence Management System (www.ns4p.co.uk)

14. **IAEA Nuclear Security Series No. 12.** Educational Programme in Nuclear Security. March 2010.

*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 |
| DAPSyP | Duly Authorised Person for Security Purposes |
| FSyP | Fundamental Security Principle |
| IAEA | International Atomic Energy Agency |
| IPPAS | International Physical Protection Advisory Service |
| NISR | Nuclear Industries Security Regulations |
| NS4P | NS4P Skills and Competence Management System |
| NSAN | National Skills Academy Nuclear |
| NSS | Nuclear Security Series |
| NTN | Nuclear Training Network |
| ONR | Office for Nuclear Regulation |
| SNI | Sensitive Nuclear Information |
| SPF | Security Policy Framework |
| SQEP | Suitably Qualified and Experienced |
| SyAP | Security Assessment Principle |
| SyDP | Security Delivery Principle |
| TAG | Technical Assessment Guide |

## APPENDIX 1: SECURITY COMPETENCIES DEVELOPED BY THE NATIONAL SKILLS ACADEMY NUCLEAR

A1.1. The following list of high level competencies were developed by a cross-industry working group coordinated by the National Skills Academy Nuclear (NSAN) in 2015 and are available on the Nuclear Training Network (NTN) (www.nucleartrainingnetwork.com) and via the NS4P Skills Competence Management System (www.ns4p.co.uk).

A1.2. ONR does not expect every person on a dutyholder's site to be fully competent in all areas, however, there is an expectation that an individual's level of competence will be appropriate to enable them to meet the requirements of their role to the required standard.

A1.3. Competence should be measured against a scale which correlates to the expected level of knowledge or skill. This could be a three, four or five level scale with the bottom level correlating to a person new to the organisation and undergoing training to fulfil the role. The top of the scale would correlate to someone who has a deep knowledge and understanding of the skill and comprehensive practical experience to consistently perform the required task(s) in a range of contexts.

A1.4. Competence Categories :

### SECURITY CULTURE

- **Personal Responsibility**

  Proactively identifies the security requirements and measures associated with their role and ensures they rigorously implement the security measures required. Challenges the behaviour of others when they fail to implement the security measures required. Understands their part in implementing the organisation's security improvement plan.

- **Security Governance**

  Ensures the organisation has a proportionate security governance regime (processes, metrics etc). Communicates the lessons emerging from the governance regime to every level in the organisation and relevant stakeholders.

- **Leading by Example**

  Creates a vision of where an organisation needs to be with regard to security performance and encourages continuous improvement. Communicates this vision and ensures the organisation has all resources to achieve it. Acts as a role model.

- **Organisational Learning & Capture**

  Develops and embeds effective security learning processes in the organisation which support the achievement of security business objectives.

### SECURITY PLANNING

- **Scope of Operations**

  Effectively plans for proportionate security operations based on the knowledge

of security legislation, guidance, detailed knowledge of the organisation's security threats/mitigations and interpretation of security performance data.

- **Security, Strategy, Policy and Standards**

  Provides relevant knowledge and experience to the development of the organisation's security strategy, policy and standards. Understands the importance of proportionality. Bases their advice on a broad knowledge of security legislation, guidance, good practice and a detailed knowledge of the organisation's security threats, mitigations and lessons identified by the organisation's learning processes.

- **Incident Response**

  Provides relevant knowledge and experience to the development of the organisation's response to all potential security incidents. Understands the importance of proportionality. Bases their advice on broad knowledge of security legislation, guidance and detailed knowledge of the organisation's security threats, mitigations and lessons learned.

**SECURITY RISK MANAGEMENT**

- **Understanding of the Threat**

  Identifies the security threats to their organisation. Knows the relevant internal and external information to analyse and applies a risk based, proportionate approach to such analysis.

- **Asset Care**

  Identifies the action required to protect assets from security threats. Understands the principles of asset care and the importance of risk based, proportionate security approaches (methodologies, tools and techniques).

- **Supplier Assurance**

  Specifies the process for ensuring that each supplier is competent to meet their organisation's security requirements. Understands and applies the principles of supplier assurance and the security approaches to achieving it. Ensures the organisation's purchasing process has the necessary checks and balances.

- **Risk Assessment**

  Understands and applies a risk based, proportionate approach to all security matters, including the principles of risk assessment and the methodologies, tools and techniques to assess and balance risk. Builds security risk into the organisation's risk management process.

- **Counter Terrorism**

  Identifies the terrorist threats to their organisation, including their potential impact, and the necessary countermeasures required. Understands the threat and the risk this presents to the organisation facilities, assets, information and employees. Takes appropriate mitigating action.

**PERSONNEL SECURITY**

- **Pre-Employment Screening**

  Identifies when an individual (e.g. employee, supplier) requires pre-

employment screening and when appropriate, national security vetting. Understands and (where relevant) applies the process for achieving this. Understands the UK security classification system and the appropriate level of vetting to apply to any individual commensurate to their degree of access to classified information/areas. Is knowledgeable on the transfer of national and international security clearances.

- **Insider Threat**

  Identifies the insider threats to their organisation and the necessary countermeasures required. Understands the potential risks posed to an organisation by those it employs or those who supply services to it. Understands and applies the approaches to mitigating such risks.

- **After Care**

  Identifies increased security risks to the organisation from individuals who develop vulnerabilities through changing circumstances. Understands and can recognise vulnerabilities, knows the appropriate action to take and acts promptly. Ensures individuals have checks of their security clearance at appropriate intervals.

**INFORMATION SECURITY**

- **Cyber Security**

  Takes proactive action to protect the organisation's electronic information, data and control systems. Understands the relevant threats, risks and countermeasures to such information, data and control systems and takes appropriate steps to protect the company and its employees.

- **Security Classifications**

  Classifies sensitive information to the relevant legislation/guidance. Understands the UK security classification system and how it corresponds to the classification system of other nations. Can apply the UK system in the UK environment and knows the security measures to apply in every classification instance. Knows the security measures to take if foreign nationals are to be given access to UK classified documentation and if foreign classified material is to be brought into the UK.

- **Information Assurance**

  Specifies the processes for ensuring the Confidentiality, Integrity and Availability of information. Understands the principles of information assurance and the security approaches to achieving it. Ensures the organisation's information processes (electronic/written) have the necessary checks and balances.

**PHYSICAL SECURITY**

- **Physical Security and Response**

  Specifies the physical security requirements for their organisation. Is knowledgeable of the functions of physical protection systems and how to determine those essential criteria which deliver a proportionate physical protection system (i.e. the Operational Requirements process). Interprets the security threats to their organisation identifying the potential vulnerabilities to physical security and designing solutions that work in harmony with business

processes. Understands the importance of deploying proportionate and risk based physical security requirements.

- **Knowledge of Guard Force**

  Specifies the guard force requirements for their organisation. Is knowledgeable on the various types of guard force that can be deployed as part of an organisation's security measures. Can interpret the security threat to their organization, identify the potential vulnerabilities and specify, on a risk basis, the size, mix and deployment of the guard force needed.

- **Providing Guidance and Advice**

  Provides risk based, proactive advice to management and other staff based on a broad knowledge of security legislation, guidance, a detailed knowledge of the organisation's security threats and mitigations, and interpretation of security performance data.