Guide for Smaller Dutyholders to the Application of the Security Assessment Principles
Guide for Smaller Dutyholders to the Application of the Security Assessment Principles
## Contents

1. FOREWORD .......................................................................................................................... 6

2. THE PURPOSE OF THIS GUIDANCE DOCUMENT ............................................................ 7

3. RESPONSIBLE PERSON OBLIGATIONS UNDER NISR 2003 AND OTHER LEGISLATION ............................................................................................................................ 7

4. HOW TO APPLY THE QUESTION SETS ........................................................................... 8

5. APPLICATION OF THE KEY SECURITY PLAN PRINCIPLES (KSYPP) TO THE PLAN . 8

6. STRUCTURE OF THE SECURITY PLAN ............................................................................. 10

7. THE SECURITY CASE ........................................................................................................... 13

8. CLAIMS AND ARGUMENTS ................................................................................................. 18

9. ANNEXES ............................................................................................................................. 20

10. AMENDMENTS TO THE APPROVED SECURITY PLAN ...................................................... 20

11. MANAGING THE PLAN ...................................................................................................... 20

ANNEX A – QUESTION SETS ................................................................................................. 22
Version Control

Changes may need to be made to this document as time moves on, for example amending minor typing errors, or accommodating any significant changes affecting the Office for Nuclear Regulation (ONR).

For this reason the website version is the only authorised version.

To avoid any confusion and provide some form of version control over the guidance, every page in this paper copy is marked as ‘uncontrolled if not viewed on ONR website’. This signals that at a future date the information may change, and it is the responsibility of each individual to cross reference any copy with the most up to date version published on the ONR website.

Where amendments are made to the document, these will be published on the ONR website with an audit trail and, where possible, stakeholders will be alerted to the changes.

Revision History

<table>
<thead>
<tr>
<th>No</th>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>July 2019</td>
<td>Original Issue (Vers 1.0)</td>
</tr>
</tbody>
</table>
1. **FOREWORD**

The Office for Nuclear Regulation (ONR) is the independent regulator of nuclear safety and civil nuclear security across the UK. ONR introduced a new security regulatory framework in March 2017 to facilitate the shift from the prescriptive regulatory regime to an outcome focused security framework. This guidance, the Security Assessment Principles (SyAPs) together with supporting Technical Assessment Guides (TAGs) provides the essential foundation for the introduction of outcome focused regulation for all constituent security disciplines: physical; personnel; transport; and cyber security and information assurance.

Outcome-focused security regulation supports clarity that responsibility for ownership and control of civil nuclear security rests with dutyholders. The fundamental principles in SyAPs enable the dutyholders to deliver the defined security outcomes, with ONR holding them to account for that delivery. Outcome-focused regulation allows greater flexibility in approach and encourages innovation in security solutions that provide effective and robust protection against the modern threat environment, whilst working in harmony with business processes and maximising opportunities for adding value. The SyAPs support this flexibility enabling alternative approaches to those defined in the fundamental principles to be applied when justified.

Notwithstanding the flexibility that SyAPs encourages within the civil nuclear industry, it is recognised that for those smaller dutyholders with low category sites the effort of developing outcome focused SyAPs aligned security plans, often with limited capacity and capability, needs to be proportionate to the risk. Consequently, this document has been produced to provide a more focused set of non-prescriptive guidance to assist those dutyholders produce a security plan which meets regulatory expectations and the dutyholders legal obligations. This approach is designed to facilitate ONR’s assessment and approval process and should reduce regulatory burden and disproportionate costs.

This document does not replace SyAPs and dutyholders should continue to refer back to SyAPs (and the associated Technical Assessment Guides (TAG)) when necessary. The content of the document and questions set at the Annex and Appendices are guidance and should not be seen as prescriptive in any manner. The guidance provided here is considered suitable for dutyholders to develop a proportionate security plan aligned with SyAPs and relevant good practice. However, it remains the dutyholder’s responsibility to ensure their security plan demonstrates how the standards, procedures and arrangements are adequate to ensure security at their site.

There is the opportunity for this document to be used by the wider Civil Nuclear Industry as the basis of a guidance document for the production of SyAPs aligned security plans but recognising that work would need to be undertaken to ensure that the question sets were appropriate for the level of risk concerned. This is for industry to take forward if required.

---

Paul Fyfe  
Deputy Chief Nuclear Inspector (Civil Nuclear Security and Safeguards)

---

1 Low category sites referred to in Version 1 of this document and the question set at Annex A specifically applies to Category IV dutyholders.
2. THE PURPOSE OF THIS GUIDANCE DOCUMENT

2.1 This document will support dutyholders’ efforts to create proportionate and effective nuclear security plans for approval.

2.2 Dutyholders should not take any of the content within this as direction or prescription by the Office for Nuclear Regulation (ONR). This guidance and the accompanying question set must not be viewed as a template by dutyholders and following either document does not guarantee approval of the plan.

3. RESPONSIBLE PERSON OBLIGATIONS UNDER NISR 2003 AND OTHER LEGISLATION

3.1 The ONR is the independent regulator of nuclear safety and civil nuclear security across the UK. ONR uses the SyAPs, together with supporting Technical Assessment Guides (TAGs), to guide regulatory judgements and recommendations when undertaking assessments of dutyholders’ security submissions such as site security plans and transport security statements. Underpinning the requirement for these submissions, and ONR’s role in their approval, are the legal duties placed on organisations subject to the Nuclear Industries Security Regulations (NISR) 2003.

3.2 NISR Regulation 4 requires the responsible person to have a security plan approved by the ONR in place at all times for each nuclear premise they are responsible for. The security plan must describe in writing the standards, procedures and arrangements adopted or to be adopted to ensure the security of the nuclear premises, and other aspects of Regulation 4(2).

3.3 Under SyAPs there will be the possibility to reduce regulatory burden by using notifications under Regulations 7 and 8 to manage amendments to the plan, Temporary Security Plans (TSPs) and the reporting of event and matters under Regulation 10(5)(i) and (j). However, unique processes will need to be developed for this purpose and it may be more advantageous for the smaller dutyholders to retain existing arrangements. This should be discussed further with ONR when producing the plan.

2 SyAPs states that ‘an effective security plan should be: (a) recorded in a dynamic suite of documents, easily accessible and understandable by those who need opt use them; (b) managed through formal processes; and (c) reviewed periodically on a defined basis.’ [RASYP 7 – Security Plan Maintenance para 292 p 78 refers]
4. **HOW TO APPLY THE QUESTION SETS**

4.1 **What are the Question Sets?**

The Question Sets Annexes document contain a set of guided questions, based upon Relevant Good Practice (RGP) which is designed to support dutyholders to create proportionate SyAPs-aligned nuclear security plans that meet their operational needs and subsequent approval by ONR.

4.2 **What is the relationship between the Question Set, the SyAPs and TAGs?**

This document does not replace SyAPs but is intended to provide dutyholders with guidance that enables them to meet their legal obligations and proportionally achieve relevant outcomes described in SyAPs. Dutyholders should always refer back to SyAPs (and the associated Technical Assessment Guides (TAG)) when necessary.

4.3 Dutyholders must also remember that nothing contained within this guidance, or SyAPs, removes the requirement for plans and arrangements to comply with legal obligations (for example those specified within the Nuclear Industries Security Regulations (NISR) 2003).

5. **APPLICATION OF THE KEY SECURITY PLAN PRINCIPLES (KSyPP) TO THE PLAN**

5.1 **What are the KSyPP?**

The Key Security Plan Principles (KSyPP) are a set of nuclear security principles that should be applied across all arrangements. Dutyholders will need to demonstrate how they have applied these principles in a sensible and proportionate fashion to their arrangements and explain this within the approved plan. The KSyPP are:

---

5.2 How to Demonstrate Consideration of the KSyPP within the Plan

The KSyPP are universal principles and are not tied to any specific security function or Fundamental Security Principle (FSyP) or Security Delivery Principle (SyDP). For this reason dutyholders may wish to ‘frontload’ the claim and argument of their application throughout the plan in the Security Case. In order to do this dutyholders may wish to state each KSyPP in turn and summarise how they have applied this principle to their arrangements – signposting out to the appropriate FSyP and/or body of evidence as appropriate. Alternatively dutyholders may wish to demonstrate how they apply these principles across the body of the security plan as appropriate.
6. STRUCTURE OF THE SECURITY PLAN

6.1 General

Dutyholders may wish to consider breaking their security plans down into a number of parts as per the diagram at Figure 2. Although this structure is not mandatory, it is simple and efficient and should enable dutyholders to develop the required content.

6.2 Relationship between the Plan and the Wider Arrangements

The arrangements referred to in this guide are the sum of the plan submitted for approval and the arrangements which are referenced as evidence from within the plan. Changes to either of these elements should be done in accordance with a proportionate Change Management Process. This process being explained within, or referenced from, the plan submitted for approval.

FIGURE 2 – DUTYHOLDERS APPROVED ARRANGEMENTS
6.3 **Security Plan Change Management**

Following approval, the content of the security plan and supporting documentation (the evidence) may need to be amended as a result of changes to the PPS design solution, in response to facility / site re-categorisation or proposals to achieve the security outcome by other means, engineered, administrative or operator action. It may also require to be amended to reflect changes to the organisational structure or to roles important to security. As all of the proposed changes have the potential to undermine the basis on which the plan was approved, but not all to the same degree, the arrangements should allow for a proportionate level of change control that is commensurate with the potential impact on security. Dutyholders should consider developing arrangements to control such changes and allow for ONR’s approval prior to amendment of the plan and subsequent implementation. These arrangements should be described / referenced in the security plan.

6.4 **Possible Components of the Plan**

The dutyholder may wish to consider a security plan structure that ‘describes in writing the standards, procedures and arrangements adopted or to be adopted by the responsible person’ as having three parts:

- Security Case;
- Claims & Arguments (for each of the 10 FSyP); and,
- Annexes (including the Security Improvement Schedule).
6.5 Evidence

A body of supporting evidence will be referenced from within the main body of the plan as required (further evidence will also be contained within the plan’s own annexes). The degree to which ONR will need to be notified about changes to this body of evidence (and the approved plan itself) will be determined by the dutyholder’s ONR-approved process for managing changes and amendments to the plan and security arrangements [see para 8.5 below].

6.6 The Audience

The audience for your plan should be key stakeholders (for example employees and those who routinely work on the site) in the first instance, rather than the site inspector. An effective approved nuclear security plan, with appropriate protective marking should be a useful internal document for dutyholders to manage and communicate how and why nuclear security is delivered across their site.
6.7 **Required Outcome and Posture**

A key principle of outcome-focused regulation is that it is driven not by prescription but by the outcome and security effects delivered by the system as a whole. Within SyAPs the outcome required is specified for each categorisation of site within the Official Sensitive Annexes. These annexes also contain additional guidance on the indicative postures dutyholders are expected to achieve from key components of the security system itself.

7. **THE SECURITY CASE**

7.1 **The Security Case**

The Security Case may be used to establish the justification for the dutyholder’s nuclear security arrangements. There should be a clear line of logic that runs through the Security Case itself and in turn from the Security Case into the claims and arguments for each FSyP.

7.2 The Security Case can be used to provide the context for dutyholder arrangements and provides the justification for all the subsequent claims and sub-claims that will be made in the main section of the plan under each FSyP.

7.3 **Structure and Content**

The Security Case may contain the following elements:

7.4 **Context**

This may include an explanation of the site, its function and how it operates. Where the site is located and any effect the physical environment may have on the security arrangements.

7.5 **Potential Targets**

The Security Case could summarise what the site holds (NM/ORM and SNI/OT/IT) and does (operations and processes) that make it subject to regulation and a potential target for malicious acts.

7.6 **Threats**

The Security Case should explain who may wish to conduct a malicious act against the site both from the DBT. Other local credible threats are not required from a regulatory perspective but could also be included if it adds benefit from as business perspective.

7.7 **The Required Outcome**

In the event that a threat actor carries out a malicious act against a target, the case should state the required outcome from the totality of the site’s security system (and what the dutyholder understands that to mean).

7.8 The dutyholder may wish to include:

- **KSyPP**

---

RGP suggests that an explanation of how each of the KSyPP\(^5\) has been considered and where it has been applied in the delivery security effect could be included within the Security Case.

- **Security Improvement Schedule (SIS) Development Process\(^6\)**

If there are significant shortfalls in the arrangements to deliver the required security outcome against the identified threats, this gap and the plan to close it will be included within the SIS. The SIS (or a similar gap analysis/security shortfall) must be included within the security plan. The dutyholder may wish to explain, within the Security Case, the process for how identified gaps will be closed (by details recorded in the SIS), appropriate interim compensatory measures implemented and then signpost to the SIS as an appropriately classified annex to the security plan.

7.9 The structure of the Security Case may look like this:

**FIGURE 4 – SECURITY CASE STRUCTURE**

7.10 **Plan Management**

Dutyholders may also wish to include, within the Security Case component an explanation of how the plan is to be maintained, the process by which changes are made (including the scale

---

\(^5\) Refer to SyAPs 2017 Edition Version 0 pp 61 – 69 for more detail on the KSyPP.

\(^6\) The SIS is used to record standards, procedures and arrangements *to be adopted* in accordance with Regulation 4(2).
by which the importance of such changes is determined) as well as a clear statement regarding ownership of the document.

7.11 **Context**

The context section may be used to place the dutyholder’s site in an appropriate context such that it summarises the key influences on the ‘standards, procedures and arrangements’ employed by the site to deliver the required security effect. Dutyholders may consider some of the following to be relevant for inclusion:

**FIGURE 5 - ILLUSTRATIVE SECURITY CASE CONTENT**
7.12 **Target Identification.** Dutyholders should identify all potential targets: Nuclear Material (NM), Other Radioactive Material (ORM), Sensitive Nuclear Information (SNI) (including operational technology/information technology), and nuclear facilities that may constitute a vital area alone or in combination. A judgement will be required as to the level of detail that can be summarised within the main body and if a separate detailed annex (at a higher classification) would be appropriate. Dutyholders may consider using a table similar to the following:

<table>
<thead>
<tr>
<th>Target ID</th>
<th>Type</th>
<th>Qty</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>01a</td>
<td>ORM</td>
<td>1</td>
<td>See Annex B (O-S) Ser 22</td>
</tr>
<tr>
<td>01b</td>
<td>SNI</td>
<td>2</td>
<td>See Annex B (O-S) Ser 24</td>
</tr>
</tbody>
</table>

7.13 **Categorisation for Theft & Sabotage**

Dutyholders will need to demonstrate that material has been accurately categorised for theft in accordance with the table in NISR. They should also demonstrate that they have considered the sabotage risk, even if discounted. Dutyholders may wish to consider more detailed arguments (including referencing out to evidence) within FSyP 6 in the main body and restrict the content of the Security Case to a summary.

---

7. Dutyholders for smaller sites should consider that SyAPs states that ‘Vital areas may be identified where there is no NM/ORM present, for example on generating power stations where systems are essential to maintain control, containment or cooling’ SyAPs SyDP 6.2.

8. Dutyholders may find the clear process and flowchart at Appendix A to TAG 6.2 useful as the basis for their process.
7.14 **Threat Identification**

The UK Design Basis Threat (DBT) articulates the threats to be considered (including the cyber threat). Dutyholders may also consider other local threats and potential hazards if appropriate and proportionate to do so. Dutyholders may consider using a table similar to the following:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Summary</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Terrorist – Lone Wolf</td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>Terrorist – 50% of DBT</td>
<td></td>
</tr>
<tr>
<td>T3</td>
<td>Terrorist – 100% of DBT</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Organised Criminal Gang</td>
<td></td>
</tr>
<tr>
<td>P1</td>
<td>Lone Anti-Nuclear Protestor</td>
<td></td>
</tr>
<tr>
<td>etc</td>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

7.15 **Prioritised Threat & Vulnerability Analysis**

Dutyholders may wish to create a simple matrix that considers the threat (by previously identified grouping) against each target set and attribute a level of risk. This matrix may include both physical and cyber threats and target groups in a single table.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Targets 01a</th>
<th>Targets 01b</th>
<th>Targets 01c</th>
<th>Targets 02a</th>
<th>Targets 03a</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Terrorist – Lone Wolf</td>
<td>LOW</td>
<td>VERY LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>C</td>
<td>Organised Criminal Gang</td>
<td>VERY LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>P1</td>
<td>Lone ANP</td>
<td>VERY LOW</td>
<td>LOW</td>
<td>MODERATE</td>
<td>LOW</td>
</tr>
</tbody>
</table>

7.16 Dutyholders may wish to develop a risk categorisation model which can be used to prioritise the risk in a transparent and credible manner but also to explain the process to the plan’s audience and ONR inspectors.
The detailed rationale behind the risk assessments could be contained within the main body of the Security Case or consolidated within a separate annex. Classification issues for the Security Case can be avoided by making sure that only target references (and not full details of type, quantity and location of inventory) are used in the main body.

In smaller sites it may be appropriate to confirm that the relevant areas or zones of the site/facility meet the indicative postures contained with the Official Annex as per the Site Categorisation. For example:

<table>
<thead>
<tr>
<th>Area/Zone/Facility</th>
<th>Effect Required</th>
<th>Indicative Posture</th>
<th>Compliance Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Area</td>
<td>Delay</td>
<td>Routine</td>
<td>Compliant</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detect</td>
<td>Routine</td>
<td>Compliant</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assess</td>
<td>Routine</td>
<td>Compliant</td>
<td></td>
</tr>
<tr>
<td>Unauthorised Access Controls</td>
<td>Routine</td>
<td>Temporary Issue</td>
<td></td>
<td>See Annex A SIS serial 23.2</td>
</tr>
<tr>
<td>Insider Threat Mitigation</td>
<td>Routine</td>
<td></td>
<td>Compliant</td>
<td></td>
</tr>
</tbody>
</table>

Summary of Arrangements

Although the detail of the security arrangements will be covered by the claims, arguments and evidence under each FSyP that follow, dutyholders may wish to summarise their overall approach to achieving the required outcome within the Security Case.

8. CLAIMS AND ARGUMENTS

8.1 FSyP Claims and Arguments

Dutyholders could use the claims, arguments and evidence approach to demonstrate compliance within their security plan and in doing so ‘the thread from claims through argument to evidence should be clear’. This approach has been used within nuclear safety for some time and dutyholders may wish to utilise SQEP with experience of it from a safety perspective in the development of their nuclear security claims and arguments.

8.2 Structure and Content

Dutyholders may wish to use the claims and sub-claims set out in the questions set to create the framework for the structure of the main body of the approved plan. The process of building...
arguments to support claims is hierarchical. Demonstrating appropriate arrangements requires the dutyholder to demonstrate compliance across ten FSyPs. Each FSyP is further broken down (within the questions set appendices to Annex A) into one or more sub-claims. Dutyholders can build arguments to demonstrate how they satisfy sub-claims; the sum of those sub-claims will then demonstrate compliance with each FSyP.

8.3 Dutyholders are free to structure the content of the claims and arguments as they deem appropriate. The dutyholder may wish to adopt a simple text structure with an FSYP claim being stated followed by the first sub claim. Under each sub-claim the argument is made in paragraphs. Evidence is referenced out as footnotes or hyperlinks, or any other appropriate method. Once the argument for one sub claim is complete the next sub claim is stated and the argument is made for it. This structure (with the relationship between claim/sub-claim, argument, evidence and annexes) is summarised in the diagram below:

FIGURE 6 – RELATIONSHIP OF CLAIMS AND ARGUMENTS

8.4 Development of Arguments

Dutyholders will recognise that across the ten FSyPs a broad range of SQEP expertise will be required to craft the arguments and identify appropriate evidence. Dutyholders may wish to distribute FSyPs or SyDPs sub-claims out to the most appropriate person to develop the argument. The argument is the dutyholder’s succinct explanation of how their arrangements deliver the claim.
8.5 **Presentation of Evidence**

All claims must be justified by appropriate arguments. All arguments must be validated by relevant evidence. The evidence can either be included within, or referenced from within, the plan. Dutyholders should ensure that the ‘golden thread’ that runs from the claim, through the argument to the supporting evidence is clear.

9. **ANNEXES**

9.1 **Use of Annexes.** Dutyholders may wish to consider using annexes to the approved plan for three reasons (which are likely to overlap):

9.2 **Clarity.** A means of including supplementary information and detail that would overly complicate or detract from the main body of the plan.

9.3 **Classification.** Secondly, as a means of managing security classification issues where the creation of one or more annexes at a level protective marking above that of the main body of the approved plan protects the accessibility and utility of the main body. For example, detailed discussion of target groupings (location, type and quantity) may be contained with an annex with a lower classification summary being included within the main body of the document.\(^\text{10}\)

9.4 **Compartmentalisation.** The application of the ‘need to know’ principle may require placing information in an annex with a more limited distribution. For example, in addition to the classification issues, it may be sensible to place the SIS within a discrete folder to manage access to it. This would also provide the benefit of a more focused application of the change management procedure to a single annex (rather than a large document) when the SIS requires updating.

10. **AMENDMENTS TO THE APPROVED SECURITY PLAN**

10.1 In order to reduce regulatory burden and maximise the benefit of outcome-focused regulation, dutyholders may wish to develop a process for categorising amendments to the security plan based on risk, using a methodology that is consistent, repeatable and identifies the significance of the impact if ill-conceived or poorly executed (see paragraph 6.3). Under this process only the highest categories would go to ONR for approval but the dutyholder would still be required manage all changes. In such cases, assessment of these arrangements will form part of ONR’s approval of the security plan and a Regulation 7(2) notification would be issued. This process would not apply to non-regulated arrangements.

10.2 Alternatively, if dutyholders do not develop such a process, they will be required to submit all amendments to the approved security plan to ONR in accordance with Regulation 6(1)(b).

11. **MANAGING THE PLAN**

11.1 **Security Plan Maintenance**

Dutyholders are required to maintain and regularly review (on a defined basis) the security plan\(^\text{11}\) (and associated arrangements). Further guidance can be sought from the Regulatory

\(^{10}\) ONR Classification Policy for the Civil Nuclear Industry (Vers 8.01) dated Nov 17

\(^{11}\) See SyAPs ‘RASyP 7 – Security Plan Maintenance’ for further guidance.
Assessment of Security Plans (RASyP) section within SyAPs (in particular RASyP 7) but dutyholders should note that their plans will should be reviewed under a range of circumstances including, but not limited to, changes to facility risk from a change in NM/ORM or SNI holdings or modifications to operating processes.

11.2 Security Plan Ownership

SyAPs RASyP 8 provides further guidance on the ownership arrangements for the security plan. It should be ‘understandable, useable and clearly owned by those with direct responsibility for security’\(^\text{12}\).

11.3 Protective Marking

In order to maximise the utility of the plan dutyholders should ensure that its classification is proportionate to the threat posed by the information. The ONR Classification Guide provides guidance on the application of classification levels.

\(^\text{12}\) SyAPs RASyP 8 p79 refers.
ANNEX A – QUESTION SETS

A-1. **Structure of the Annex**
This Annex contains ten appendices each containing a question set for each Fundamental Security Principle (FSyP). The questions sets have been further broken down into sub-claims around each Security Development Principle (SyDP). Under each sub-claim dutyholders are provided with guidance on the construction and content of arguments and suggested sources of potential evidence to support and substantiate those claims.

A-2. **Application of the Question set by Dutyholders**
The question sets are provided for guidance only. The content is neither exhaustive nor is there an expectation that dutyholders will answer every question. Dutyholders should only answer those questions which are appropriate to their circumstances and do so in a manner and with a level of detail that is proportionate to the level of risk associated with their site, the security outcome required (tempered by their statutory obligations) and the needs of the their internal audience.

A-3. **Further Guidance and Information**
These questions sets are provided on the assumption that dutyholders are familiar with both the Security Assessment Principles (SyAPs) and the relevant Technical Assessment Guides (TAGs). If dutyholders require further guidance or clarification on how to development arguments for each sub-claim they may wish to revert to these sources in the first instance.
### FSyP 1 – Leadership and Management for Security

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyP 1</strong> Claim: We have established 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.</td>
</tr>
<tr>
<td><strong>SyDP 1.1: Governance &amp; Leadership</strong> Sub-Claim: Our directors, managers and leaders at all levels focus the organisation on achieving and sustaining high standards of security and of delivering the characteristics of a high reliability organisation.</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- The organisation and Leadership Team (including a Board where appropriate) are structured, highlighting any specific roles and responsibilities for security.
- It is determined that the leadership team and Board (where appropriate) is competent to assess and act effectively on security information including current threat and risks.
- The leadership team and Board (where appropriate) ensures that security is given equal priority to safety when providing strategic direction and leadership.
- Roles, accountabilities, standards and expectations of behaviour for nuclear security are made clear to staff and how compliance with security standards and expectations is monitored. This should be evidenced through an appropriate reference including the management information available and how it is used.
- Security is integrated into your management system.

Your arguments may be supported by evidence contained within the following:

- Your company security policy
- Role profiles
- Board Terms of Reference
- Minutes of board meetings
- Nuclear baseline for security
<table>
<thead>
<tr>
<th>Sub-Claim: We are adequately resourced to implement and maintain our security undertakings</th>
</tr>
</thead>
</table>

Your arguments should explain how:

- You have determined you have sufficient competent resource available to deliver your security arrangements and how security related roles are identified. It should encapsulate how you identify and rectify security knowledge gaps and ensure knowledge capture, transfer and retention to preserve unique knowledge and skills.
- Your organisation provides resilience of security roles.
- You control changes to your organisational structure and resource for security
- You identify opportunities to improve security performance and expand the knowledge of the facility.

Your arguments may be supported by evidence contained within the following:

- Your company security policy
- Nuclear baseline / security organisational structure
- Security resilience strategy / plan
- Security knowledge management plan
- Security management information / security KPIs
Sub-Claim: All of our decisions regarding security are informed, rational, objective, transparent and prudent.

Your arguments should explain how:

- Your nuclear security decision-making processes:
  - enable prudent and timely decisions to be made at the appropriate level by competent personnel with the necessary authority, understanding of security arrangements and the means to ensure that their decisions are implemented,
  - are appropriately transparent, auditable, consistent, simple, flexible, open to challenge.
- Your decision-making processes consider available options using relevant good practice.
- Active challenge and the promotion of a questioning attitude by staff and contractors is managed.

Your arguments may be substantiated by evidence contained within the following:

- Your company security policy
- Board Terms of Reference
- Minutes of board meetings
- Letters of delegated authority
- Nuclear baseline
<table>
<thead>
<tr>
<th>Sub-Claim: We are a learning organisation who utilise a wide range of sources to continually improve our leadership, organisational capability, our management systems, our security performance and decision making.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your arguments should explain how:</td>
</tr>
<tr>
<td>• Deficiencies in security performance are systematically identified, reported, investigated and corrected and how staff are encouraged to report them.</td>
</tr>
<tr>
<td>• Security events meeting the criteria stipulated in NISR Regulation 10 are reported to ONR.</td>
</tr>
<tr>
<td>• Lessons are identified and learned from security events including identification of root causes, trending and reporting to senior leaders.</td>
</tr>
<tr>
<td>• Security performance is monitored.</td>
</tr>
<tr>
<td>Your arguments may be supported by evidence contained within the following:</td>
</tr>
<tr>
<td>• Company security policy</td>
</tr>
<tr>
<td>• Security event reporting policies</td>
</tr>
<tr>
<td>• Security event reporting log</td>
</tr>
<tr>
<td>• Policies on investigation and learning from events</td>
</tr>
<tr>
<td>• OPEX reports</td>
</tr>
<tr>
<td>SyDP 1.5: Assurance Processes</td>
</tr>
<tr>
<td>------------------------------</td>
</tr>
<tr>
<td><strong>Sub-Claim:</strong> We have an evidence-based assurance process in place which informs our governance process, challenge is welcomed across our organisation and informs security strategy.</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- You have nuclear security assurance processes in place to ensure compliance with relevant standards, procedures and arrangements for security.
- Information reported to senior management and used to support continuous improvement.

Your arguments may be supported by evidence contained within the following:

- Your company security policy
- Security performance reports to the Board
- Internal assurance strategy and policies
- Internal Assurance reports on security
- Internal assurance security review plan
- Performance against security Metrics (KPIs)
**FSyP 2 – Organisational Culture**

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyp 2</strong></td>
</tr>
</tbody>
</table>

**SyDP 2.1: Maintenance of a Robust Security Culture**

Your arguments should explain how:

- Your nuclear security policy is integrated into the overall management system.
- Arrangements are in place to assess/review and improve security culture.
- You address any cultural issues identified.
- Your internal assurance arrangements are used to validate your security culture.

Your arguments may be supported by evidence contained within the following:

- Company Nuclear security policy
- Internal reporting process for events and matters.
- Security culture assessment programme, methodology and reports (eg CPNI SeCURE 4).
- Organisational culture action / implementation plans.
### FSyP 3 – Competence Management

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyp 3</strong></td>
</tr>
<tr>
<td><strong>SyDP 3.1: Analysis of Security Roles and Associated Competencies</strong></td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- You identify the roles and associated security competence requirements for all members of the workforce who have responsibility for operations which might affect security

Your arguments may be supported by evidence contained within the following:

- Your company security policy / policies
- Your nuclear baseline
- R2A2 (Roles, Responsibilities, Accountabilities, Authorities) for security roles
- Human and organisational factor reports on security
- Job role/ task analysis
- Training needs analysis for security
### SyDP 3.2: Identification of Learning Objectives and Training Needs

**Sub-Claim:** We have a process to ensure security training requirements are identified.

Your arguments should explain how:

- You determine the training that is necessary to develop and maintain the required level of competence for all staff.
- You determine the training that is necessary to develop and maintain the required level of competence for persons with specific responsibility for security.

Your arguments may be supported by evidence contained within the following:

- Your nuclear baseline
- R2A2 (Roles, Responsibilities, Accountabilities, Authorities) for security roles
- Training needs analysis for security
- Training packages
- Individual security role training profiles

### SyDP 3.3: Measurement of Competence

**Sub-Claim:** We have implemented arrangements to deliver the necessary security training.

Your arguments should explain how:

- You deliver necessary security training
- You measure or assess how those persons with security responsibilities are competent to perform their role.
- You measure the effectiveness of security training

Your arguments may be supported by evidence contained within the following:

- Training needs analysis for security
- Your training assessment policy and associated training databases
- R2A2 (Roles, Responsibilities, Accountabilities, Authorities) for security roles
- Individual security role training profiles
<table>
<thead>
<tr>
<th>SyDP 3.4: Organisation of and Support to the Training Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sub-Claim:</strong> We monitor and record the effectiveness of our security staff. We give due priority to training and competence assurance of security roles.</td>
</tr>
<tr>
<td>Your arguments should explain how:</td>
</tr>
<tr>
<td>- You are resourced and organised to deliver a training function.</td>
</tr>
<tr>
<td>- You ensure trainers are competent.</td>
</tr>
<tr>
<td>Your arguments may be supported by evidence contained within the following:</td>
</tr>
<tr>
<td>- Your nuclear security policy</td>
</tr>
<tr>
<td>- Training needs analysis for security</td>
</tr>
<tr>
<td>- R2A2 (Roles, Responsibilities, Accountabilities, Authorities) for security training roles</td>
</tr>
<tr>
<td>- Your training assessment policy and associated training record databases</td>
</tr>
<tr>
<td>- R2A2 (Roles, Responsibilities, Accountabilities, Authorities) for security roles</td>
</tr>
<tr>
<td>- Individual security role training profiles</td>
</tr>
</tbody>
</table>
# FSyP 4 – Nuclear Supply Chain Management

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyP 4</strong></td>
</tr>
</tbody>
</table>

**SyDP 4.1: Procurement and Intelligent Customer Capability**

Sub-claim: We maintain an 'Intelligent Customer' capability for all work carried out on our behalf by suppliers that may impact upon nuclear security.

Your arguments should explain how:

- How you have processes in place to make sure that you are an intelligent customer of those goods and services which may have an impact on nuclear security.
- Your Supply Chain strategy accommodates the specific needs of nuclear security.
- Those responsible for advising the supply chain security needs (including the drafting of operational requirements) are suitably SQEP and the process is assured.
- You create specifications as part of your procurement process.
- Explanation of how you protect against introduction of counterfeit, fraudulent or suspect items into the security regime if appropriate and necessary to do so.

Your arguments may be supported by evidence contained within the following:

- Generic contractual requirements.
- Quality assurance documents/processes.
- Arrangements to mitigate the risks of counterfeit, fraudulent and suspect items.
- Service level agreements.
- Security and/or technical specifications and operational requirements.
**SyDP 4.2: Supplier Capability**

Sub-claim: We evaluate and confirm that suppliers have the organisational and technical capability, capacity and culture to deliver items or services to the specification prior to placing any contract where such work may have an impact on nuclear security.

Your arguments should explain how:

- Suppliers of goods or services that have significance for the delivery of nuclear security, are themselves competent, have an appropriate level of oversight over their own supply chain and suitable Quality Plans.

Your arguments may be supported by evidence contained within the following:

- Quality plans
- Design plans
- Supplier accreditations (e.g. ISO 9001)
- Manufacturing, fabrication and inspection records
Sub-claim: We conduct effective oversight and assurance of our supply chain.

Your arguments should explain how:

- The security function is able to conduct assurance of the supply chain for the procurement of significant items or services.
- Contractual obligations are placed upon suppliers by the organisation in order to minimise the risk, to an acceptable level, of the introduction of CFSI into the supply chain.
- Your organisation is able to provide the necessary assurances to the board that no additional risk is being accrued by security via its supply chain.

Your arguments may be supported by evidence contained within the following:

- Oversight and assurance processes
- Procurement processes
- Contracting Authority Assurance reports
- Security Aspects Letters
- Technical Specifications
<table>
<thead>
<tr>
<th>SyDP 4.4: Commissioning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sub-claim:</strong> We subject any facility, system or process that may affect security to testing and a commissioning plan before bringing it into operation or returning it to service.</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- Significant procurements of security-related services or components of the physical or cyber system (directly linked to the delivery of the required security outcome) are brought into service and commissioned in line with the Operational Requirement.
- Significant items or services required to deliver the security outcome have been procured with appropriate consideration given to the whole life of the capability (for example in terms of maintenance, training, personnel and financial support).

Your arguments may be supported by evidence contained within the following:

- User acceptance test results.
- Post implementation review reports.
- Snagging and error reports.
- Operational procedures.
- Maintenance manuals.
- Risk assessments.
### FSyP 5 – Reliability, Resilience and Sustainability

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyP 5</strong></td>
</tr>
<tr>
<td><strong>SyDP 5.1: Reliability and Resilience</strong></td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- You identify the relative importance of components to security; this may include formal a categorisation and classification process.
- You ensure defence in depth in security measures so that you are not reliant on one single part of the system to deliver the security function. Explain how related dependencies are identified (such as personnel or power supplies) and have an appropriate level of redundancy.
- You obtain significant assurances of the reliability and resilience of systems provided by other duty holders that play a significant role in the delivery of your required security functions output.
- Implement contingency arrangements and compensatory measures when required.

Your arguments may be supported by evidence contained within the following:

- Detection parameters and probabilities.
- Mean time between failures.
- UPS and backup power capabilities.
- Contingency arrangements.
- Spares strategy.
- Adversary path analysis and vulnerability assessments.
- CPNI security equipment classes.
<table>
<thead>
<tr>
<th>Sub-claim: Security structures, systems and components (SySSC) receive regular and systematic Examination, Inspection, Maintenance and Testing (EIMT).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your arguments should explain how:</td>
</tr>
<tr>
<td>• You ensure that SySSC are appropriately examined, maintained, inspected and tested in accordance with their importance to security. There should be a clear relationship between the significance of the component and the priority or frequency of its testing and maintenance.</td>
</tr>
<tr>
<td>• You obtain significant assurances about the EIMT regime from other dutyholders or suppliers when their systems play a significant role in the delivery of your required security output or from the service providers if the delivery of your own capability is sub-contracted out.</td>
</tr>
<tr>
<td>• You will ensure that SySSC are maintained, inspected and tested by SQEP.</td>
</tr>
<tr>
<td>Your arguments may be supported by evidence contained within the following:</td>
</tr>
<tr>
<td>• Maintenance schedules, instructions and records.</td>
</tr>
<tr>
<td>• Inspection and testing schedules.</td>
</tr>
<tr>
<td>• Call-out contracts and agreements.</td>
</tr>
<tr>
<td>• Security system configurations.</td>
</tr>
<tr>
<td>• Temporary security plans and arrangements.</td>
</tr>
<tr>
<td>• Quality plans.</td>
</tr>
<tr>
<td>SyDP 5.3: Sustainability</td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td><strong>Sub-claim:</strong> We ensure that the constituent parts of our nuclear security regime are sustained and supported over time to ensure they continue to deliver the required outcomes.</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- Security is planned for the medium to longer term (which may include the process for allocating operational and capital expenditure).
- Security planning (and its associated resourcing) is afforded an appropriate level of senior leadership/board level attention. You could also explain how these managers are SQEP to a level that enables them to make these decisions.
- Key decisions relating to sustainable security planning are recorded.
- The Security Enhancement Schedule (SIS) (or similar formal enhancement process) is driven by the threat, endorsed at an appropriately senior level, has the right level of oversight and is sufficiently resourced throughout its lifespan.
- Security planning is reviewed to ensure that it meets your changing requirements over time whilst remaining focussed on achieving the require security output.
- Security management and resource planning is related to wider business risk management processes.

Your arguments may be supported by evidence contained within the following:

- Security budgets
- Legacy system strategy and replacement
- Succession planning
- Knowledge management
- System performance
- Risk assessments
## FSyp 6 – Physical Protection Systems (PPS)

<table>
<thead>
<tr>
<th><strong>Questions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyp 6</strong></td>
</tr>
<tr>
<td>Claim: We have implemented and maintain a proportional physical protection system that integrates technical and procedural controls to form layers of security that build defence-in-depth and are graded according to the potential consequence of a successful attack.</td>
</tr>
</tbody>
</table>

| **Sub-claim:** We have undertaken a characterisation of our site and facilities in order to determine the categorisation for theft. |
| **SyDP 6.1: Categorisation for Theft** |
| Your arguments should explain how: |
| 1. The methodology used to determine your categorisation for theft that makes clear that you understand how this shapes the security arrangements you have in place to deliver the required security outcome. |
| 2. You are assured that the process was conducted by individuals who were suitably SQEP. |
| 3. An analysis of the type and form of NM/ORM to be protected from theft has been conducted. |
| 4. The planning assumptions that underpin the categorisation are kept under review. |
| 5. There is a process in place to review this categorisation when the way in which the inventory is stored, processed or handled or the inventory changes at your site. |

Your arguments may be supported by evidence contained within the following:

- Waste stream information.
- Environmental permits.
- Accounting principles.
- NM/ORM inventory lists.
- NM balance figures.
- Accountancy and control plans.
- Radioactive source registers.
- Regular reviews of the plan.
Sub-claim: We have undertaken a characterisation of our site and facilities in order to determine the categorisation for sabotage.

Your arguments should explain how:

- The Vital Area Assessment (VAA) was conducted by SQEP personnel and the methodology used.
- You are able to confirm that your site contains only baseline areas. This assessment shapes the overall design of your security system and influences how you deliver the required security outcome.
- How safety systems make a contribution to the delivery of the required security outcome.

Your arguments may be substantiated by evidence contained within the following:

- VAA Methodology.
- VAA Report.
- Safety cases.
- An analysis of the type and form of NM/ORM and associated processes to determine the relative attractiveness for sabotage and/or vulnerabilities (e.g. it may be easier to realise radiological consequences from sabotaging an unsealed source than a sealed source).
- Engineering documents.
- Inventory information.
- Utilities plans and information.
| SyDP 6.3: Physical Protection System Design |

Sub-claim: We have designed and implemented a physical protection system that builds defence in depth and meets the required security outcome based on the categorisation for theft and sabotage.

Your arguments should explain how:

- The process by which you have reviewed the threats to your assets, taken the findings of the categorisations for theft and sabotage has informed the design the PPS.
- The key components of your PPS compare against the indicative postures contained within SyAPs and justification of any gaps.
- The design of the PPS delivers the necessary outcome.
- If you are a member of a UK MOD supply chain, an indication of the effect that MOD policy (JSP 440/List X) and/or Security Aspects Letters (SAL) have had on the design of your PPS.

Your arguments may be supported by evidence contained within the following:

- PPS design specifications and operational requirements.
- Building plans and construction specifications.
- CPNI classifications of security equipment.
- Configuration and locations of security equipment.
- Operational procedures.
- Utilities and backup provision.
<table>
<thead>
<tr>
<th>SyDP 6.4: <em>Vulnerability Assessments (VA)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sub-claim:</strong> We have satisfied ourselves that our physical protection system achieves the required security outcome by undertaking vulnerability assessments.</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- The process(es) you use to conduct a structured and systematic vulnerability assessment to validate the PPS and provide assurance that it delivers the required outcome and are proportionate to the risk, categorisation of the site and the security outcome required.
- You make adjustments to the PPS as a result of routine work or changes to inventory.
- Your methodology for managing the security enhancement programme or security improvement schedule (SIS) is informed by vulnerability assessments.

Your arguments may be supported by evidence contained within the following:

- Vulnerability Assessment Reports.
- Adversary path analysis.
- Security exercise reports.
<table>
<thead>
<tr>
<th>SyDP 6.5: Adjacent or Enclave Nuclear Premises</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-claim: We have given consideration to the effects of adjacent or enclave nuclear premises on the maintenance of our nuclear security and our impact on theirs.</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- (For adjacent sites) the adjacent site’s PPS impacts upon your site and vice versa. You may also wish to explain how any identified risks are mitigated through collaboration.
- (For enclave sites) you rely upon the components of the PPS provided by the site within which you are located.
- You are assured that shared components (including services) of the PPS deliver the security outcome that you expect them to and have sufficient resilience.
- Communication and governance arrangements are in place to facilitate collaborative working with co-owners of shared services.
- Any process of review (including the triggers and supporting management arrangements) used by both sites to ensure that when the situation changes at either site there is no negative impact upon the PPS of either site is managed.

Your arguments may be supported by evidence contained within the following:

- Memoranda of Understanding (or similar arrangements).
- Plans detailing shared security or safety services.
- Contingency plans and emergency arrangements.
### FSyP 7 – Cyber Security and Information Assurance

<table>
<thead>
<tr>
<th>FSyp 7</th>
<th>Claim: We have implemented and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyDP 7.1: Effective Cyber and Information Risk Management</td>
<td>Sub-Claim: We maintain arrangements to ensure that CS&amp;IA risk is managed effectively.</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- Your risk management approach ensures the security of SNI (and the associated IT assets) over the course of its lifecycle.

Your arguments may be supported by evidence contained within the following:

- Information Assets Register.
- Critical Digital Asset Register.
- Risk Appetite Statement.
- CSIA Roles & Responsibilities (may include Information Asset Owners, CISO and SIRO).
- Risk Management Methodology (such as ISO 27001 or IRAM2).
Sub-Claim: We maintain the confidentiality, integrity and availability (CIA) of sensitive nuclear information and associated assets.

Your arguments should explain how:

- Your Information Security Policy and underpinning arrangements deliver CIA for SNI (and associated assets).
- You identify and assure classified contracts. This should include:
  - the arrangements used to assess nuclear security maturity for third party companies;
  - how any supply chain issues are identified and the results of any assessments are fed back by adequate reporting;
  - Describe your processes to manage the closure of contracts with third party companies involving information and associated assets.

Your arguments may be supported by evidence contained within the following:

- Information Security Policy.
- Company Classification Policy.
- Information Asset Register.
- Classified Contracts Register.
- Supplier Assurance Reports.
**SyDP 7.3: Protection of Nuclear Technology and Operations**

<table>
<thead>
<tr>
<th>Sub-Claim: We ensure our operational technology (OT) and information technology (IT) assets are secure and resilient to cyber threats.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your arguments should explain how:</td>
</tr>
<tr>
<td>- You can demonstrate that the selection of technical cyber security controls is based upon a risk assessment and is aligned with the SyAPs and provides defence in depth. Including:</td>
</tr>
<tr>
<td>- how you have selected the correct Cyber Protection System (CPS) outcomes for your facility's digital assets;</td>
</tr>
<tr>
<td>- the mechanisms in place for identifying and testing control implementations; and,</td>
</tr>
<tr>
<td>- how you provide resilience and assurance of your system security controls.</td>
</tr>
<tr>
<td>Your arguments may be supported by evidence contained within the following:</td>
</tr>
<tr>
<td>- Information Security Policy.</td>
</tr>
<tr>
<td>- SyOPs, User Access Policy, Social Media Policy, Network Access Policy.</td>
</tr>
<tr>
<td>- Risk Management document set.</td>
</tr>
<tr>
<td>- IT Penetration Test or ‘Healthcare’ Results.</td>
</tr>
<tr>
<td>- System monitoring reports.</td>
</tr>
</tbody>
</table>
**SyDP 7.4: Physical Protection of Information**

**Sub-Claim:** We ensure we have the appropriate physical protection measures to protect our information and associated assets against a wide range of threats.

Your arguments should explain how:

- You deliver physical security measures to protect your information and associated assets.
- You assure the physical security measures that protect your information and associated assets.

Your arguments may be supported by evidence contained within the following:

- Details of your physical security control measures (which may include areas such as pass system (visitors and employees), PIN system, keys, non-business hours arrangements, visitor access, security guards, alarm system, CCTV, incoming/outgoing mail arrangements, facilities management arrangements, information storage arrangements, disposal and destruction of hard copy info and removable media, use of info archiving services, arrangements for managing risk of SNI within supply chain).
- Classified Material Assessment Tool (CMAT) results.
- Audit or assurance reports
<table>
<thead>
<tr>
<th>SyDP 7.5: Preparation for and Response to Cyber Security Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sub-Claim:</strong> We have well-tested plans, policies and procedures which reduce our vulnerability to cyber security incidents, non-malicious leaks and other disruptive challenges.</td>
</tr>
<tr>
<td>Your arguments should explain how:</td>
</tr>
<tr>
<td>- You identify and manage credible cyber and information security incidents and how your arrangements are tested</td>
</tr>
<tr>
<td>- The business demonstrates that each IT/OT system is supported by independently verified documentation that identifies the risks to that system and confirms that those risks have been mitigated to an acceptable level.</td>
</tr>
<tr>
<td>Your arguments may be supported by evidence contained within the following:</td>
</tr>
<tr>
<td>- Cyber &amp; Information Security Incident Management Policy.</td>
</tr>
<tr>
<td>- Organisational Learning.</td>
</tr>
<tr>
<td>- Cyber &amp; Information Security Incident Log.</td>
</tr>
<tr>
<td>- Exercise Plans and Records.</td>
</tr>
</tbody>
</table>
FSyP 8 – Workforce Trustworthiness

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyP 8</strong></td>
</tr>
<tr>
<td>Claim: We have implemented and maintain a regime of workforce trustworthiness to reduce the risks posed by insider activity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SyDP 8.1: Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-Claim: We ensure that human resources, occupational health and security departments cooperate to facilitate effective screening, vetting and ongoing personnel security arrangements for the workforce (staff and contractor community).</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- You implement and maintain on-going personnel security management arrangements and procedures to remain assured about your employees and contractors and to mitigate the risks from well-placed insiders.
- Occupational health processes take security factors into consideration when considering workforce ailments, balancing the common law duty of medical confidentiality against disclosure and how any thresholds that the OH representative advises are considered.
- (For NSV holders) relevant information would be shared with the NSV sponsor.

Your arguments may be supported by evidence contained within the following:

- Corporate security policy covering oversight of personnel security arrangements.
- Appropriate records of meetings between departments with responsibilities for workforce trustworthiness.
- Employee assistance programmes and/or reporting hotlines agreements and arrangements.
- Tender and contract award document related to personnel security expectations.
- Induction course material which covers conditions of service and associated policies.
<table>
<thead>
<tr>
<th><strong>SyDP 8.2: Pre-employment Screening and National Security Vetting</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sub-Claim:</strong> We deliver the appropriate combination of recruitment checks and vetting to satisfy ourselves of the honesty and integrity of their potential workforce (staff and contractor community).</td>
</tr>
<tr>
<td>Your arguments should explain how:</td>
</tr>
<tr>
<td>- You have implemented the BPSS process so that it is compliant with the minimum standards as published in Cabinet Office guidance and the relevant SyAPs Annexes.</td>
</tr>
<tr>
<td>- Your processes are used to determine the level of NSV clearance (where required).</td>
</tr>
<tr>
<td>- Assurances are sought to complete a meaningful Employee Record Check in support of any National Security Vetting application and outcomes are be recorded and dealt with appropriately.</td>
</tr>
<tr>
<td>Your arguments may be substantiated by evidence contained within the following:</td>
</tr>
<tr>
<td>- Policies and procedures to demonstrate compliance with Cabinet Office guidance and ONR requirements.</td>
</tr>
<tr>
<td>- Training records for personnel security courses attended by HR staff and other relevant stakeholders (i.e. CPNI courses).</td>
</tr>
<tr>
<td>- Arrangements for verifying the veracity of supply chain workforce trustworthiness check.</td>
</tr>
<tr>
<td>- Procedures demonstrating how conditions of employment or caveats are managed.</td>
</tr>
</tbody>
</table>
Sub-Claim: We implement and maintain on-going personnel security management, arrangements and procedures to remain assured about our workforce and to mitigate the risks from insiders.

Your arguments should explain how:

- Your facility supports effective National Security Vetting (NSV) and ongoing personnel security arrangements for the workforce (staff and contractor community). This should include how the appropriate combination of recruitment checks and vetting are delivered so that the honesty and integrity of potential employees is satisfactorily assessed.
- NSV holders are made aware/reminded of when they are required to complete Change of Personal Circumstances (CPC) questionnaires and the need to seek travel advice when travelling overseas on either business or pleasure (including briefing/debriefing arrangements and how is this information shared with the NSV sponsor).
- You ensure that requests for a renewal of a NSV clearance are generated in good time before the current clearance expires.
- Appropriate arrangements are in place to ensure appropriate actions are taken on termination of employment.
- You actively manage a clearance which has been issued with a caveat or condition of employment. (including how any outcomes are communicated to the NSV sponsor).

Your arguments may be supported by evidence contained within the following:

- Arrangements to report information that affects the integrity of the clearance.
- Appropriate records of meetings between departments with responsibilities for workforce trustworthiness.
- Employee assistance programmes and / or reporting hotlines agreements and arrangements.
- Initiatives to publicise an ongoing personnel security culture.
SyDP 8.3: Ongoing Personnel Security

Sub-Claim: We implement and maintain on-going personnel security management, arrangements and procedures to remain assured about our workforce and to mitigate the risks from insiders.

Your arguments should explain how:

- Supportive employment policies and assistance programmes are promoted in the workplace.
- The security function collaborates with appropriate functions (e.g. HR and training) to develop the content of induction programmes, the annual learning and development strategy, and the content of staff surveys.
- Arrangements are in place to communicate when staff are working under duress and how they are communicated to staff so that they are always aware about how to enact them.
- (For NSV holders) HR processes take account of the potential security consequences of HR interventions (including exit interviews) and where concerns arise, how they discussed with the security function and communicated to the NSV sponsor.
- Data on the number and volume of calls to Employee Assistance programmes and Benevolent Funds is shared with HR, OH and security, particularly to support ongoing personnel security themes and any overarching personnel security strategy.
- (For NSV holders) Processes are in place to support the NSV Sponsors requirement to ensure that DV holders complete an ASAF.
- (For NSV holders) Triage process are in place for ASAF’s between the NSV sponsor and the facility so immediate mitigations can be put into place rather than waiting on the completion of the ONR assessment.
- (For NSV holders) The drug and alcohol testing policy enables positive results for NSV holders to be reported both internally and to the NSV sponsor.

Your arguments may be supported by evidence contained within the following:

- Arrangements to report information that affects the integrity of the clearance.
- Appropriate records of meetings between departments with responsibilities for workforce trustworthiness.
- Employee assistance programmes and / or reporting hotlines agreements and arrangements.
- Initiatives to publicise an ongoing personnel security culture.
**FSyP 9 – Policing and Guarding**

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyp 9</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SyDP 9.1: CNC Response Force</strong></th>
<th>Sub-claim: We facilitate CNC deployment if appropriate to achieve the required security outcome.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Your arguments should explain how:</td>
</tr>
<tr>
<td></td>
<td>- The CNC are not required to deliver your security outcome if this is the case.</td>
</tr>
<tr>
<td></td>
<td>- You would facilitate a CNC response force should their deployment at your site be necessary in response to a specific threat or event (for example by establishing appropriate liaison, assurance and communication arrangements with them).</td>
</tr>
<tr>
<td></td>
<td>Your arguments may be supported by evidence contained within the following:</td>
</tr>
<tr>
<td></td>
<td>- MoUs or similar</td>
</tr>
<tr>
<td></td>
<td>- Security contingency plans</td>
</tr>
</tbody>
</table>
**Sub-claim:** We facilitate local police forces’ provision of support by way of assistance to the CNC or delivering a response to the site in respect of terrorist, criminal or protest activity.

Your arguments should explain how:

- You understand the statutory duties of the local police in relation to your security arrangements and this understanding has informed your assumptions concerning the police response to an incident on your site.
- The local police to play a part in the delivery of your security outcome and what arrangements you have in place to facilitate this.
- The CTSA has provided advice in the production of the security regime and continues to offer security and threat updates as necessary.

Your arguments may be supported by evidence contained within the following:

- Security contingency plans.
- Details of the arrangements you have in place to ensure that the local police force are familiar with the security arrangements on your site and have sufficient information to enable them to make an informed decision about how best to respond to reports of a security incident.
- Details of procedures in place to facilitate the participation of the local police to observe and/or participate in security exercises.
- Security exercise reports.
- Op SHIELDING meeting minutes.
Sub-claim: We employ civilian security guards to provide the unarmed guarding who conduct nuclear security operations as described in the site security plan such as patrolling, access control and searching; and, who deliver or enable the immediate response to a security event.

Your arguments should explain how:

- The Civilian Guard Force (CGF) contributes to the required security outcome by the delivery of effective and efficient guarding.
- The CGF should act, communicate, report and liaise with other stakeholders (including the local police) in the event of a security or safety event.
- Conservatism and resilience is built into the guarding model, including their ability to respond to different CT response levels.
- CGT arrangements provide confidence that the security outcomes will be delivered during industrial disputes.
- Appropriate arrangements are in place to manage additional issues where the GCF is a shared resource with another dutyholder or organisation (see also FSyP 6).

Your arguments may be supported by evidence contained within the following:

- Roles and responsibilities.
- Service level and performance level agreements.
- Training records.
- CGF deployment orders, policies and procedures.
- Security guard force equipment.
- Performance monitoring and management.
- Security exercise reports.
# FSyP 10 – Emergency Preparedness and Response

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSyP 10</strong></td>
</tr>
<tr>
<td><strong>SyDP 10.1: Counter Terrorism Measures, Emergency Preparedness and Response Planning</strong></td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- Security arrangements are adjusted in response to changes in the Government Response Level in order to maintain the required security effect and how these changes communicated in an efficient and effective manner.
- Your response to a cause-agnostic incident delivers the necessary PPS Response and Required Effect\(^\text{13}\).  
- The processes for communicating with the offsite response and reporting an incident within an appropriate timeframe (depending on the security outcome required).
- Potential conflicts between safety and security emergency response expectations are identified and mutually resolved.

Your arguments may be supported by evidence contained within the following:

- Security contingency response plan.
- Emergency preparedness and response arrangements.
- Counter-terrorism plan with incremental measures.
- Accounting procedures for personnel in the event of an incident.
- Media Plan.
- Exercise Reports.

---

\(^\text{13}\) See O-S Annex to SyAPs.
<table>
<thead>
<tr>
<th>SyDP 10.2: Testing and Exercising the Security Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-claim: We have implemented an exercise regime to train personnel and test the efficacy of our nuclear security contingency plans.</td>
</tr>
</tbody>
</table>

Your arguments should explain how:

- Your exercise regime trains your personnel.
- Your exercise regime tests the efficacy of your nuclear security contingency plans.
- You ensure, through exercising and testing, that all personnel with responsibility for delivering the PPS security outcome and required effect are tested and able to demonstrate competency.
- The frequency of your testing and exercising activity is justified.
- Operational Experience (OPEX) is captured and shared.
- You develop the scenarios to test the full scope of your Security Contingency Plan.

Your arguments may be supported by evidence contained within the following:

- Training programmes.
- Staff competencies.
- Security exercise objectives and scenarios, including joint safety/security aspects.
- Security exercise planning arrangements.
- Security exercise reports.
- the process for capturing and sharing learning both within the site and from external organisations.
- Scenario Documentation.
<table>
<thead>
<tr>
<th>SyDP 10.3: Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-claim: We have structures and processes in place to ensure effective command, control and communications arrangements during and post nuclear security events.</td>
</tr>
<tr>
<td>Your arguments should explain how:</td>
</tr>
<tr>
<td>- Key stakeholders for emergency response (for example on-call staff, Home Office police, site owners or neighbouring businesses) are identified and an explanation of how you would maintain an appropriate level of communication with them during an incident.</td>
</tr>
<tr>
<td>- Your reporting arrangements will deliver the PPS response outcome and required security effects for any security incident.</td>
</tr>
<tr>
<td>- Your reporting arrangements satisfy your obligations under statutory regulation.</td>
</tr>
<tr>
<td>- All responders would work together in the event of an emergency (including who has overall control and any circumstances where this changes).</td>
</tr>
<tr>
<td>- The contribution from external responders for the required security outcome would be facilitated.</td>
</tr>
<tr>
<td>- Alternate arrangements are in place for control and communication if the primary location you plan to use is unavailable or unusable.</td>
</tr>
<tr>
<td>- You would maintain arrangements for extended durations.</td>
</tr>
<tr>
<td>Your arguments may be supported by evidence contained within the following:</td>
</tr>
<tr>
<td>- Communications plans and protocols.</td>
</tr>
<tr>
<td>- Administrative arrangements.</td>
</tr>
<tr>
<td>- Training relating to command and control.</td>
</tr>
<tr>
<td>- Security contingency plans.</td>
</tr>
<tr>
<td>- Security exercise reports.</td>
</tr>
</tbody>
</table>