

ONR guidance

**Guide for smaller dutyholders to the application of the Security Assessment Principles**

ONR guidance

Guide for smaller dutyholders to the application of the Security Assessment Principles

**Authored by:** Inspector

**Approved by:** Head of Profession – Protective Security

**Approved by:** Head of Profession – CS&IA

**Issue number:** 2

**Published:** July 2025

**Next scheduled major review:** April 2030

**Document reference:** ONR-CNS-GD-003

**Record reference:** ONRHH-822789359-20901

**Revision Commentary**

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 2.0 | * Figure 1 updated to reflect SyAPs 2022 edition (p.7) * Update to relevant threats as per current DBT (p.14) * Added “Competent Authorities” section (p.18) * Addition of “Context” paragraph under each FSyP (Annex A) * Addition of “ONR expectations” paragraph for each SyDP (Annex A) * FSyP 3 updated to reflect SyAPs 2022 edition (A-7 to A-10) * Addition of SyDP 6.5, 6.6 & 6.7 (A-20 to A-21) |

Contents

[1. Foreword 4](#_Toc202968491)

[1.1. Purpose 5](#_Toc202968492)

[1.2. Responsible person obligations under NISR 2003 and other legislation 5](#_Toc202968493)

[1.3. How to apply question sets 6](#_Toc202968494)

[1.4. Application of the Key Security Plan Principles (KSYPP) to the plan 7](#_Toc202968495)

[1.5. Structure of the Security Plan 8](#_Toc202968496)

[1.5.1 The Security Case 10](#_Toc202968497)

[1.5.2 Claims and Arguments 15](#_Toc202968498)

[1.5.3 Annexes 16](#_Toc202968499)

[1.6. Amendments to the Approved Security Plan 17](#_Toc202968500)

[1.7. Managing the Plan 17](#_Toc202968501)

[1.8. Competent Authorities 18](#_Toc202968502)

[Glossary and Abbreviations 19](#_Toc202968503)

[Annex A – Question Sets A-1](#_Toc202968504)

# Foreword

1. The Office for Nuclear Regulation (ONR) is the UK's independent nuclear regulator, with the legal authority to regulate nuclear safety, civil nuclear security and safeguards, and conventional health and safety. 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.
2. 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.
3. Notwithstanding the flexibility that SyAPs encourages within the civil nuclear industry, it is recognised that for those smaller dutyholders with low category sites[[1]](#footnote-1) 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.
4. This document does not replace SyAPs and dutyholders should continue to refer back to SyAPs (and note the associated TAGs) 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 deliver 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 (SPA) are adequate to ensure security at their site.

## Purpose

1. This document will support dutyholders’ efforts to create proportionate and effective nuclear security plans[[2]](#footnote-2) for approval.
2. Dutyholders should not take any of the content within this as direction or prescription by 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.

## Responsible person obligations under NISR 2003 and other legislation

1. ONR is the UK's independent nuclear regulator, with the legal authority to regulate nuclear safety, civil nuclear security and safeguards, and conventional health and safety. ONR uses the SyAPs, together with supporting 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.
2. NISR 2003 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. 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 events 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.

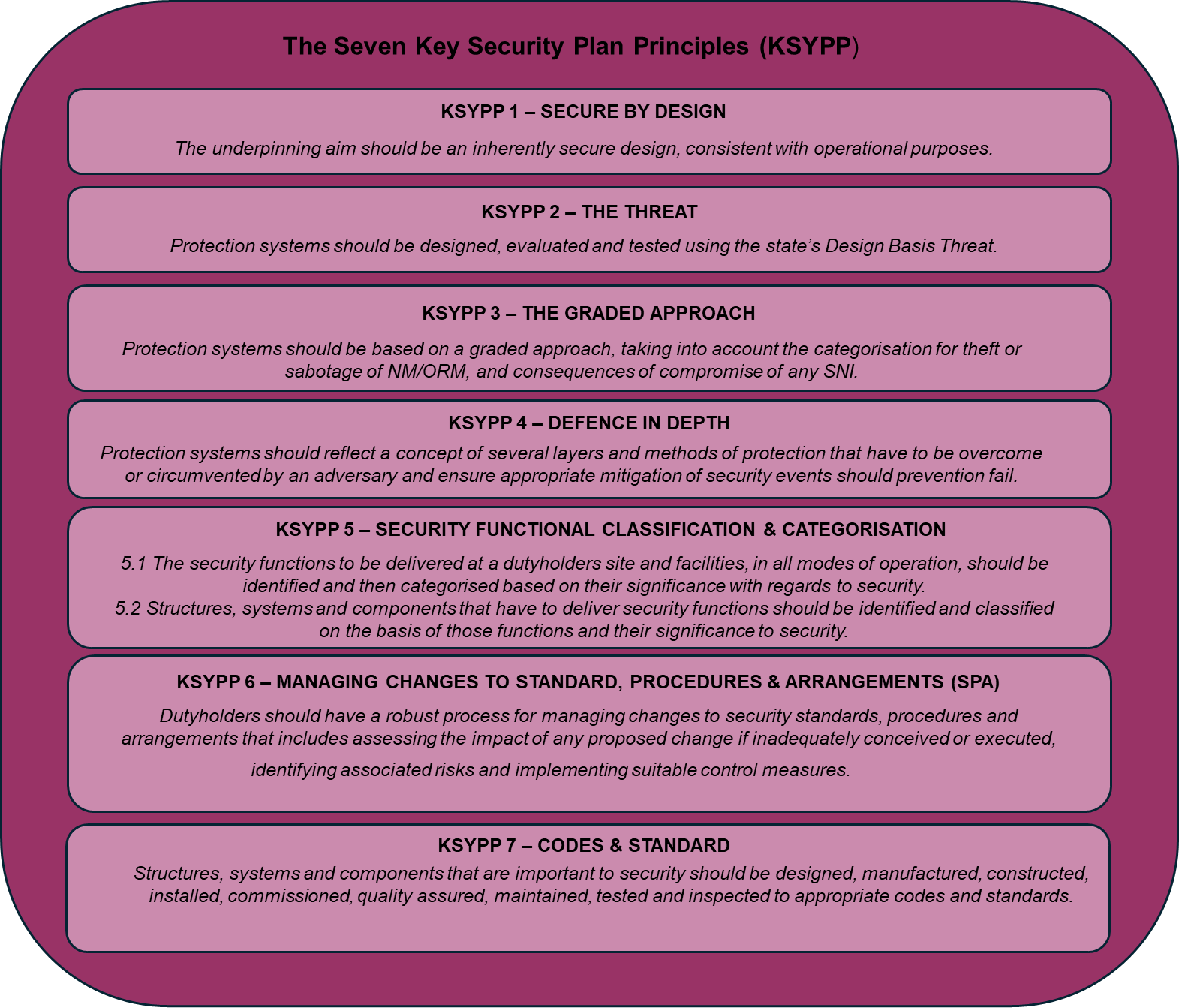
## How to apply question sets

1. What are the Question Sets? The Question Sets (Annex A) are 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.
2. What is the relationship between the Question Sets, 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 note the associated TAGs) when necessary.
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 NISR 2003)[[3]](#footnote-3) .

## Application of the Key Security Plan Principles (KSyPP) to the plan

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:

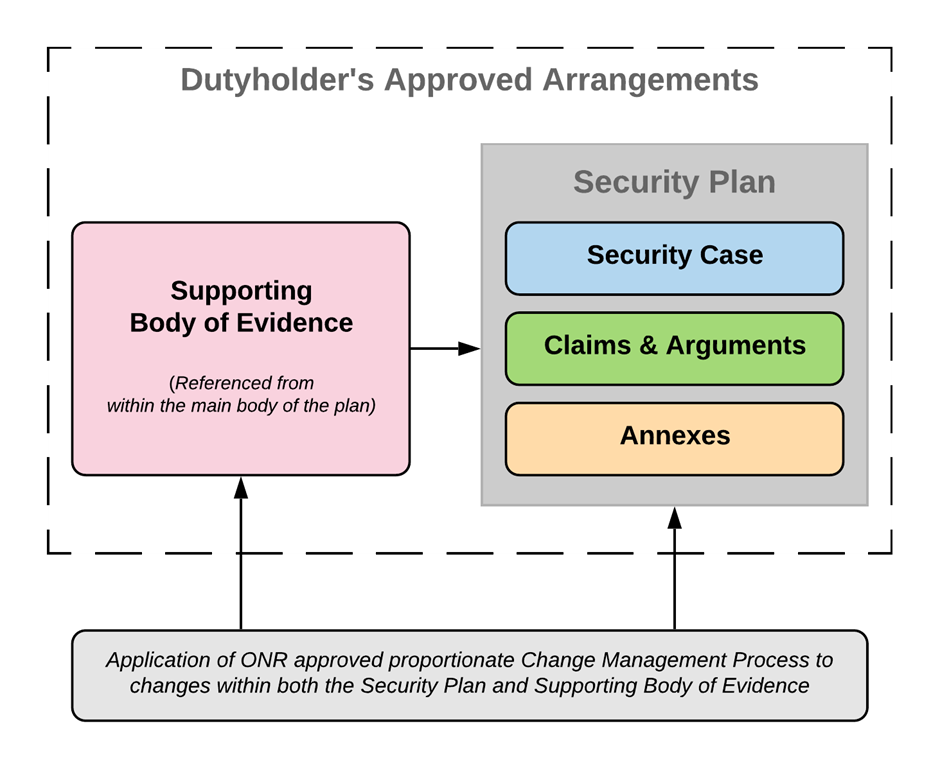
**Figure 1 - Key Security Plan Principles**



1. How to Demonstrate Consideration of the KSyPP within the Plan. The KSyPP are universal principles and are not tied to any specific security function, 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. Where possible dutyholders should cross reference throughout any case so as to avoid unnecessary duplication.

## Structure of the Security Plan

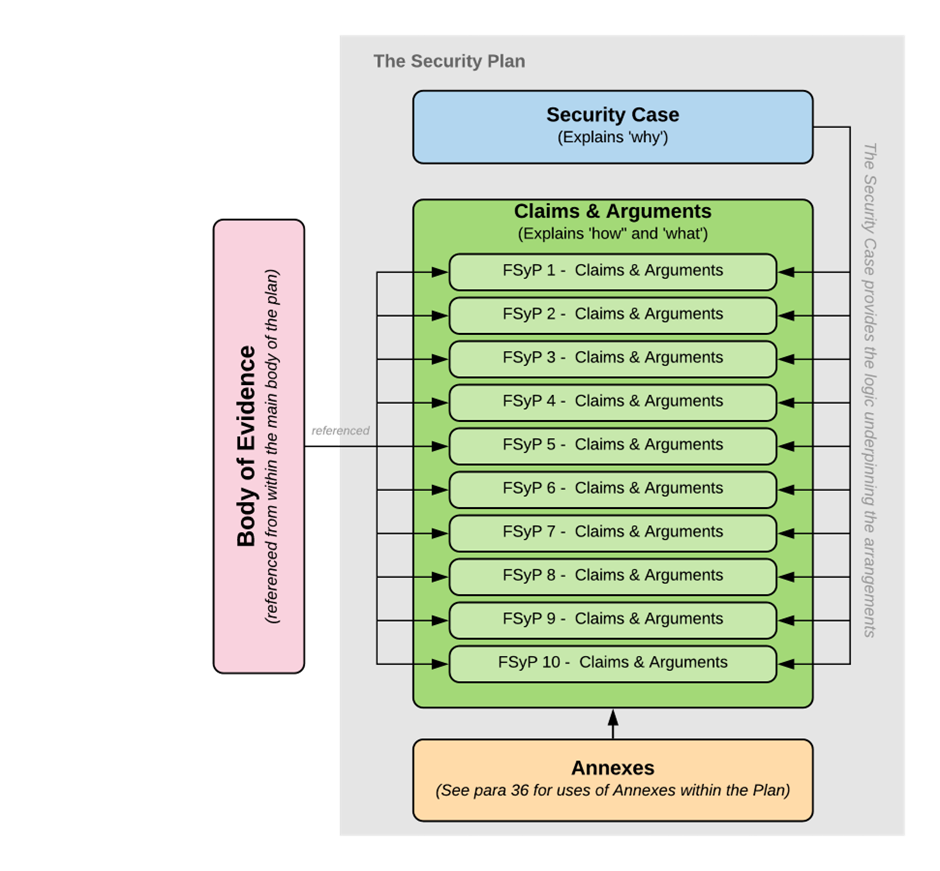
1. General. Dutyholders may wish to consider breaking their security plans down into a number of parts as per the diagram at Figure 2. Although this structure is not mandatory, it is simple and efficient and should enable dutyholders to develop the required content.
2. Relationship between the Plan and 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 – Dutyholder’s Approved Arrangements**

1. 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 physical and/or cyber protection system (PPS/CPS) 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.
2. 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).



**Figure 3 - Structure of a Security Plan**

1. 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. 43 below].
2. 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.
3. 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[[4]](#footnote-4).

### The Security Case

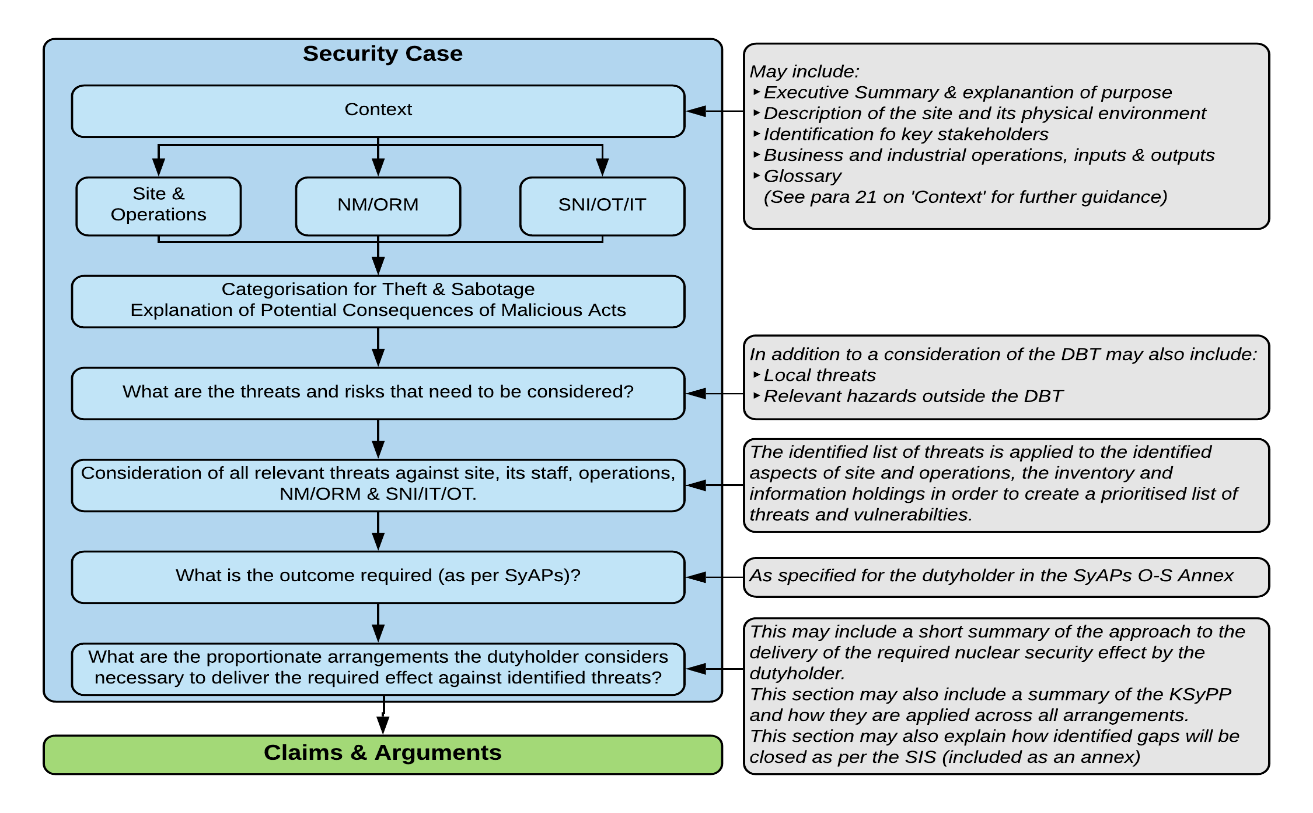
1. The Security Case. The Security Case may be used to establish the justification for the dutyholder’s nuclear security arrangements. There should be a clear line of logic that runs through the Security Case itself and in turn from the Security Case into the claims and arguments for each FSyP.
2. The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

* 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.
* Potential Targets. The Security Case could summarise what the site holds (Nuclear Material (NM) / Other Radioactive Material (ORM) and Sensitive Nuclear Information (SNI) / Operational Technology (OT) / Information Technology (IT)) and what it does (operations and processes) that make it subject to regulation and a potential target for malicious acts.
* Threats. The Security Case should explain who may wish to conduct a malicious act against the site as depicted within the DBT. Other local credible threats are not required from a regulatory perspective but could also be included if it adds benefit from a business perspective. Dutyholders may also take a similar approach to the identification of local threats that may be posed specifically to their site (i.e. criminal, protestors), although this is not a regulatory requirement.
* 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).

1. The dutyholder may wish to include:

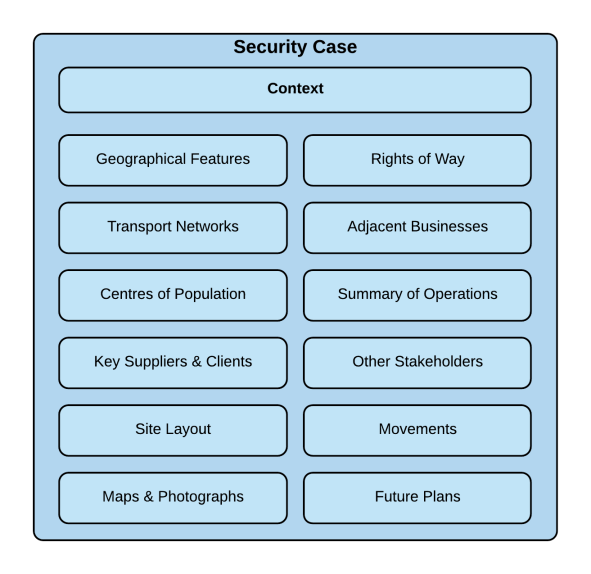
* KSyPP. RGP suggests that an explanation of how each of the KSyPP[[5]](#footnote-5) has been considered and where it has been applied in the delivery of security effect could be included within the Security Case.
* Security Improvement Schedule (SIS) Development Process[[6]](#footnote-6). If there are 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.

1. The structure of the Security Case may look like this:



**Figure 4 - Security Case Structure**

1. 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 by which the importance of such changes is determined) as well as a clear statement regarding ownership of the document.
2. 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 SPA 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**

1. Target Identification. Dutyholders should identify all potential targets: NM, ORM, SNI (including OT / IT) 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:

|  |  |  |  |
| --- | --- | --- | --- |
| Target ID | Type | Qty | Comment |
| 01a | ORM | 1 | See Annex B (O-S) Ser 22 |
| 01b | SNI | 2 | See Annex B (O-S) Ser 24 |

1. 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.[[7]](#footnote-7) 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.[[8]](#footnote-8)
2. 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:

|  |  |  |
| --- | --- | --- |
| Threat | Summary | Details |
| T1 | Terrorist – DBT Lone Actor |  |
| T2 | Terrorist – 50% of DBT INSIDER |  |
| C1T3 | Cyber – DBT Terrorist – 100% of DBT |  |
| etc | Cyber |  |

1. 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 attributes a level of risk. This matrix may include both physical and cyber threats and target groups in a single table.

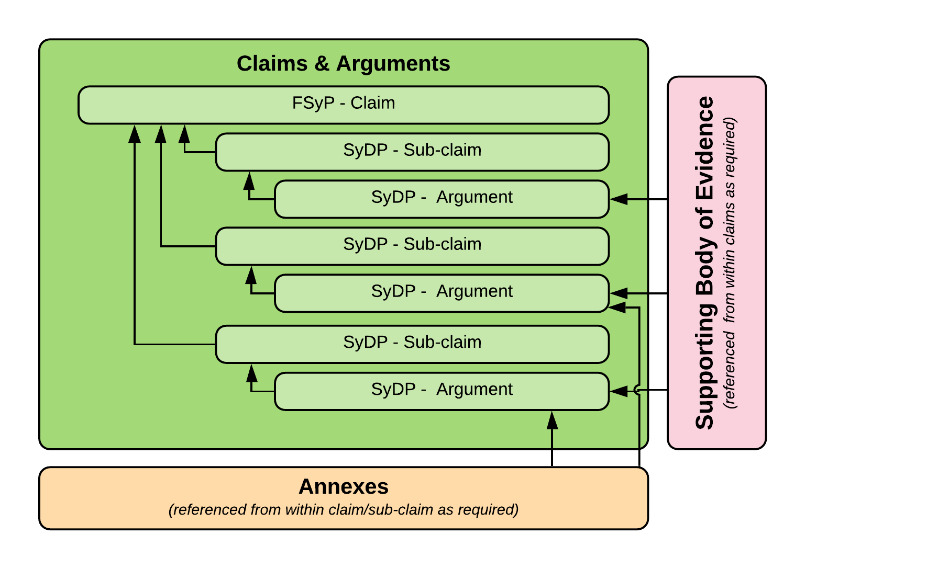
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Threats | | Targets | | | | |
| **01a** | **01b** | **01c** | **02a** | **03a** |
| T1 | Terrorist – DBT Lone Actor | LOW | VERY LOW | LOW | LOW | LOW |
| C1 | Cyber – DBT Organised Criminal Gang | VERY LOW | LOW | LOW | LOW | LOW |
| T2P1 | INSIDER Lone ANP | VERY LOW | LOW | MODERATE | LOW | LOW |

1. 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.
2. 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.
3. In smaller sites, it may be appropriate to confirm that the relevant areas or zones of the site/facility meet the indicative postures contained within the Official-Sensitive - SNI Annex as per the Site Categorisation. For example:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Area/Zone/Facility | Effect Required | Indicative Posture | Compliance Status | Comment |
| Storage Area | Delay | Routine | Compliant |  |
| Detect | Routine | Compliant |  |
| Assess | Routine | Compliant |  |
| Unauthorised Access Controls | Routine | Temporary Issue | See Annex A SIS serial 23.2 |
| Insider Threat Mitigation | Routine | Compliant |  |

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

### Claims and Arguments

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’.[[9]](#footnote-9) 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.
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.
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**

1. 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.
2. 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.

### Annexes

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

* Clarity. A means of including supplementary information and detail that would overly complicate or detract from the main body of the plan.
* Classification. Secondly, as a means of managing security classification issues where the creation of one or more annexes at a protective marking level 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 within an annex, with a lower classification summary in the main body of the document.[[10]](#footnote-10)
* 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.

## Amendments to the Approved Security Plan

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 17). Under this process only the highest categories would go to ONR for approval, but the dutyholder would still be required to 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.
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).

## Managing the Plan

1. Security Plan Maintenance. Dutyholders are required to maintain and regularly review (on a defined basis) the security plan[[11]](#footnote-11) (and associated arrangements). Further guidance can be sought from the Regulatory Assessment of Security Plans (RASyP) section within SyAPs (in particular RASyP 7) but dutyholders should note that their plans 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.
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’.[[12]](#footnote-12)
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 Policy for the Civil Nuclear Industry[[13]](#footnote-13) provides guidance on the application of classification levels.

## 1.8. Competent Authorities

1. Throughout this guidance, references are made to competent authorities who provide subject matter expert guidance on physical and cyber security solutions. Although ONR are the Competent Authority for Nuclear Security, the National Protective Security Authority (NPSA) is the UK National Technical Authority (NTA) for physical protective security. The UK NTA for cyber security is the National Cyber Security Centre (NCSC). Dutyholders are encouraged to consult NPSA and NCSC guidance on physical and cyber security, for additional insights and RGP into protective and cyber controls. Both agencies provide a wealth of resources and training packages that can help dutyholders meet the requirements set within their security plans, ensuring adequate protection of NM and ORM.

# Glossary and Abbreviations

CA Competent Authority

CPPNM Convention on the Physical Protection of Nuclear Material

CS&IA Cyber Security and Information Assurance

DBT Design Basis Threat

FSyP Fundamental Security Principle

HCVA High Consequence Vital Area

HMG His Majesty’s Government

IAEA International Atomic Energy Agency

LAA Limited Access Area

MFES Manual Forced Entry Standard

MOU Memorandum of Understanding

NCSC National Cyber Security Centre

NISR Nuclear Industries Security Regulations

NM Nuclear Material

NPSA National Protective Security Authority

NSS Nuclear Security Series

NSV National Security Vetting

NTA National Technical Authority

ONMACS ONR Nuclear Material Accountancy, Control and Safeguards

ONR Office for Nuclear Regulation

ORM Other Radioactive Material

PPS Physical Protection System

SNI Sensitive Nuclear Information

SPF Security Policy Framework

SyAP Security Assessment Principle

SyDP Security Delivery Principle

SySSC Security System, Structure or Component

TAG Technical Assessment Guide

VA Vulnerability Assessment

VAI Vital Area Identification

# Annex A – Question Sets

1. Structure of the Annex. This Annex contains ten sections, each containing a question set for one Fundamental Security Principle (FSyP). The question sets have been further broken down into sub-claims around each Security Delivery 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.

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 their internal audience.

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**

|  |  |
| --- | --- |
| FSyP 1 | Claim: We have established and maintain organisational security capability underpinned by strong leadership, robust governance, and adequate management and accountability of security arrangements incorporating internal and independent evidence-based assurance processes.  *Context: Dutyholders should create a culture where security is a priority at all organisational levels, with clear accountability, robust management structures, and evidence-based assurance processes to maintain compliance and effectiveness.* |
| **SyDP 1.1***: Governance & Leadership* | 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. |
| *ONR Expectations: ONR expects dutyholders to establish strong governance and leadership that clearly focus the organisation on achieving high security standards and a positive security culture. This involves setting and enforcing security strategies, policies and objectives throughout the organisation, ensuring a direct chain of accountability up to board level.*  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, including 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. |
| **SyDP 1.2:** *Capable Organisation* | Sub-Claim: We are adequately resourced to implement and maintain our security undertakings. |
| *ONR Expectations: ONR expects dutyholders to maintain an organisation with sufficient capability, people, structure and processes to implement and uphold all security measures.*  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. |
| **SyDP 1.3***: Decision Making* | Sub-Claim: All of our decisions regarding security are informed, rational, objective, transparent and prudent. |
| *ONR Expectations: ONR expects decisions affecting security to be informed, rational and made with security as a top priority, supported by transparent and prudent processes. Dutyholders should ensure that when key decisions are made, that they have considered all relevant information, that they take into account the opinions of other specialisms and that staff are empowered to take timely action in the interests of security without undue delay.*  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, and 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. |
| **SyDP 1.4***: Organisational Learning* | 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. |
| *ONR Expectations: ONR expects dutyholders to operate as learning organisations, continually improving their security arrangements by learning from internal and external experiences/training.*  Your arguments should explain how:   * Deficiencies in security performance are systematically identified, reported, investigated and corrected and how staff are encouraged to report them. * Security events meeting the criteria stipulated in NISR 2003 Regulation 10 are reported to ONR. * Lessons are identified and learned from security events including identification of root causes, trending and reporting to senior leaders. * Security performance is monitored.   Your arguments may be supported by evidence contained within the following:   * Company security policy. * Security event reporting policies. * Security event reporting log. * Policies on investigation and learning from events. * Operational Experience (OPEX) reports. |
| **SyDP 1.5***: Assurance Processes* | Sub-Claim: We have an evidence-based assurance process in place which informs our governance process; challenge is welcomed across our organisation and informs security strategy. |
| *ONR Expectations: ONR expects dutyholders to implement evidence based assurance processes that provide confidence at all management levels, up to and including the board, and that security plans and controls are working appropriately.*  Your arguments should explain how:   * You have nuclear security assurance processes in place to ensure compliance with relevant standards, procedures and arrangements (SPA) for security. * Information is 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**

|  |  |
| --- | --- |
| FSyP 2 | Claim: We encourage and embed an organisational culture that recognises and promotes the importance of security.  *Context: Dutyholders should endeavour to foster a positive security culture throughout the organisation, where all personnel understand and value their role in maintaining security. Dutyholders should seek to embed security into everyday practices, encouraging staff to take ownership of security responsibilities and contribute to the identification and mitigation of threats.* |
| **SyDP 2.1***: Maintenance of a Robust Security Culture* | *ONR Expectations: ONR expects dutyholders to cultivate and maintain a robust security culture across the entire organisation, led by a visible commitment from the board and senior management teams. A strong security culture means every employee and contractor understands that credible threats exist, that the security of the site is paramount, and that each of them has a role to play in maintaining security onsite and further afield.*  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. * Organisational culture action / implementation plans. |

**FSyP 3 – Management of Human Performance**

|  |  |
| --- | --- |
| FSyP 3 | Claim: We have implemented and maintain effective arrangements to ensure the human contribution to delivery of security is understood and appropriately designed (to include tasks, competence, staffing, workspace, equipment and administrative control), implemented and resourced.  *Context: It is essential that all personnel whose activities have the potential to impact on nuclear security are able to deliver their role reliably. Therefore, robust arrangements for identifying reliance upon humans to deliver security, and assuring that these actions are suitably supported, is essential for an organisation to achieve secure operations.* |
| **SyDP 3.1***: Identification and Analysis of Security Tasks and Roles* | Sub-Claim: We have undertaken a systematic approach to the identification and analysis of all tasks important to security, which demonstrates that tasks assigned to those with security roles are designed so that they can be effectively delivered. |
| *ONR Expectations: ONR expects dutyholders to use a systematic approach to identify all tasks that are important to security and analyse those tasks to ensure they can be performed reliably by people in designated security roles.*  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. * You performed a proportionate task analysis to identify Tasks Important to Nuclear Security (TINS), using a simplified risk-based approach to ensure tasks critical to maintaining security are assigned appropriate personnel. * Those tasks that are required for: the protection of Nuclear Material (NM), Other Radioactive Material (ORM) and associated facilities against acts of theft and sabotage; security tasks involved with the transport of nuclear and radioactive material by Class A and B carriers; tasks required to protect confidentiality, integrity and availability of SNI; and security tasks required to support nuclear safety events, have been clearly documented and are accessible to relevant staff. * The identification of TINS considered tasks completed by direct employees as well as contracted elements of the workforce whose activities may impact upon nuclear security * You assigned a proportionate analysis of these tasks, focusing on tasks that are considered most important to the delivery of nuclear security functions. * You substantiated the suitability of the design of the security measure including the Security Structure, System or Component (SySSC), and actions required for operation and maintenance of the SySSC, to reliably deliver the relevant security function.   Your arguments may be supported by evidence contained within the following:   * Your company security policy / policies. * Your nuclear baseline. * R2A2 (Roles, Responsibilities, Accountabilities, Authorities) Task register detailing key activities, their purpose, and associated risks. * Human and organisational factor reports on security. * Job role/ task analysis. * Training needs analysis for security and those with security responsibilities outside of their normal job role. |
| **SyDP 3.2***: Sufficiency and Competence of Persons Delivering Security* | Sub-Claim: We can demonstrate by analysis that we understand the numbers and competencies of personnel required to deliver all security functions, and that we have a systematic approach to identification of training needs and competence management. |
| *ONR Expectations: ONR expects dutyholders to have enough qualified and capable personnel at all times to carry out all security functions, supported by a systematic training and competence management program.*  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. * Appropriate numbers of Suitably Qualified and Experienced Personnel (SQEPs) are in place to control activities that could impact on nuclear security, under all foreseeable circumstances throughout the life cycle of the process or facility. * You have determined the appropriate staffing design that has taken into consideration factors such as shift-working hours, SQEP of the team design, and management structures within the teams responsible for nuclear security.   Your arguments may be supported by evidence contained within the following:   * Your nuclear baseline is a possible means by which you may demonstrate that your organisational structure, staffing and competencies are, and remain, suitable and sufficient to manage nuclear security throughout the full range of its business * R2A2 for security roles. * Training needs analysis for security. * Training logs for mandatory security training. * Training packages. * Individual security role training profiles. |
| **SyDP 3.3***: Suitable and Sufficient workspaces, equipment and user interfaces* | Sub-Claim: We ensure suitable analysis is undertaken to demonstrate that workspaces, equipment and user interfaces are designed to match human capabilities, support reliable human performance and the delivery of security functions. |
| *ONR Expectations: ONR expects dutyholders to design and provide work environments, tools and interfaces that support reliable human performance in security tasks by matching human factors requirements.*  Your arguments should explain how:   * You have evaluated workspaces to confirm they enable effective task performance without unnecessary complexity or risk. * You have assessed equipment, ensuring it is user-friendly and tailored to the site’s security needs. * You have taken into account tasks that require human interaction and have mitigated against the risk of human error. * You have considered the physical and psychological fatigue imposed on staff due to factors associated to the equipment and user interface required for the required task and environmental factors such as heating, lighting and noise.   Your arguments may be supported by evidence contained within the following:   * Workplace assessments. * Maintenance schedules. * R2A2 for security roles. * Staff engagement reports. |
| **SyDP 3.4***: Suitable and Sufficient Procedures and Administrative controls* | Sub-Claim: We provide sufficient procedures and administrative controls, which are designed to minimise the likelihood of human error and support reliable delivery of security functions. |
| *ONR Expectations: ONR expects dutyholders to have well-designed and controlled security procedures and administrative controls that guide personnel in performing security tasks correctly, thereby minimising the chance of human error.*  Your arguments should explain how:   * You have developed straightforward procedures and administrative controls that align with regulatory requirements and are easy to understand for staff. * You have identified relevant procedures and administrative controls and clearly define where this has been included as part of your security plan or the appropriate references. * You ensure proportionate levels of internal assurance and governance, ensuring that relevant procedures and administrative controls are updated as and when required.   Your arguments may be supported by evidence contained within the following:   * Internal assurance templates and checklists. * Change logs for relevant procedures and administrative controls. |

**FSyP 4 – Nuclear Supply Chain Management**

|  |  |
| --- | --- |
| FSyP 4 | Claim: We implement and maintain effective supply chain management arrangements for the procurement of products or services related to nuclear security.  *Context: Dutyholders should seek assurances that the supply chain supporting nuclear security is reliable and trustworthy. Dutyholders must implement robust procurement and oversight processes to ensure suppliers meet security requirements, and vulnerabilities within the supply chain are identified and mitigated.* |
| **SyDP 4.1***: Procurement and Intelligent Customer Capability* | Sub-claim: We maintain an ‘Intelligent Customer’ capability for all work carried out on our behalf and by suppliers that may impact upon nuclear security. |
| *ONR Expectations: ONR expects dutyholders to act as an intelligent customer whenever they procure items or services that could impact nuclear security. This means that the dutyholder retains full responsibility for security and has enough in-house understanding to specify security requirements, oversee supplier work and ensure the delivered products or services meet the needs within the security plan.*  Your arguments should explain 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. * 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. |
| *ONR Expectations: ONR expects dutyholders to evaluate suppliers’ capabilities and commitment to security before entrusting them with work that could affect 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. |
| **SyDP 4.3***: Oversight of Suppliers of Items or Services that may Impact on Nuclear Security* | Sub-claim: We conduct effective oversight and assurance of our supply chain. |
| *ONR Expectations: ONR expects dutyholders to maintain active oversight and assurance of their supply chain to ensure continued security compliance and performance.*  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 Counterfeit, Fraudulent and Suspect Items (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. |
| **SyDP 4.4***: Commissioning* | Sub-claim: 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. |
| *ONR Expectations: ONR expects dutyholders to thoroughly test and commission any new or modified security system, facility or process before it is relied upon for nuclear security. A defined commissioning plan should be part of the security arrangements, detailing how systems or structures will be tested against the security design requirements and who is responsible for each commissioning activity.*  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**

|  |  |
| --- | --- |
| FSyP 5 | Claim: We have designed and support our nuclear security regime to ensure it is reliable, resilient and sustained throughout the entire lifecycle.  *Context: The Dutyholder should aim to establish a security regime that remains effective and resilient under all circumstances. They should emphasise the importance of designing security measures that can withstand disruptions, ensuring long-term sustainability of security arrangements, and evidence the ability to adapt to evolving threats and organisational changes.* |
| **SyDP 5.1***: Reliability and Resilience* | Sub-claim: Security structures, systems and components (SySSC) are designed to incorporate appropriate levels of reliability and resilience through ‘fail-secure’, redundancy, diversity and segregation. There are appropriate contingency arrangements in place to ensure continuity of security provision. |
| *ONR expectations: ONR expects all SySSC to be designed, qualified and maintained for high reliability and resilience, such that they perform their security function under all expected conditions and if they fail, they do so in a secure manner.*  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 dutyholders that play a significant role in the delivery of your required security functions output. * You 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. * Uninterruptible power supply (UPS) and backup power capabilities. * Contingency arrangements. * Spares strategy. * Adversary path analysis and vulnerability assessments. * NPSA security equipment classes. |
| **SyDP 5.2***: Examination, Inspection, Maintenance and Testing* | Sub-claim: Security structures, systems and components (SySSC) receive regular and systematic Examination, Inspection, Maintenance and Testing (EIMT). |
| *ONR Expectations: ONR expects dutyholders to implement a structured program of regular EIMT for all security-related equipment and systems, to ensure they remain fit for purpose.*  Your arguments should explain how:   * 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. * 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. * You will ensure that SySSC are maintained, inspected and tested by SQEP personnel.   Your arguments may be supported by evidence contained within the following:   * Maintenance schedules, instructions and records. * Inspection and testing schedules. * Call-out contracts and agreements. * Security system configurations. * Temporary security plans and arrangements. * Quality plans. |
| **SyDP 5.3***: Sustainability* | Sub-claim: 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. |
| *ONR Expectations: ONR expects dutyholders to plan and allocate resources so that every element of their nuclear security regime can be sustained over the long term, thereby continuously achieving required security outcomes.*  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 Improvement 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 focused on achieving the required 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)**

|  |  |
| --- | --- |
| FSyP 6 | 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.  *Context: The Dutyholder should establish and maintain robust physical protection measures that deter, detect and delay potential adversaries. By integrating technical and procedural controls, dutyholder should ensure that multiple layers of security provide defense-in-depth and are proportional to the consequences of potential threats.* |
| **SyDP 6.1***: Categorisation for Theft* | Sub-claim: We have undertaken a characterisation of our site and facilities in order to determine the categorisation for theft. |
| *ONR Expectations: ONR expects dutyholders to perform a thorough characterisation of the nuclear and radioactive materials at their site in order to determine the correct security categorisation for theft of those materials. This categorisation process should follow the prescribed guidelines (such as those in SyAPs annexes) that consider the quantity and the chemical/physical form of the NM and ORM.*  Your arguments should explain how:   * The methodology used to determine your categorisation for theft makes clear that you understand how this shapes the security arrangements you have in place to deliver the required security outcome. * You are assured that the process was conducted by individuals who were suitably SQEP. * An analysis of the type and form of NM/ORM to be protected from theft has been conducted. * The planning assumptions that underpin the categorisation are kept under review. * 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 itself, 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. |
| **SyDP 6.2***: Categorisation for Sabotage* | Sub-claim: We have undertaken a characterisation of our site and facilities in order to determine the categorisation for sabotage. |
| *ONR Expectations: ONR expects dutyholders to identify vital areas and conduct a detailed categorisation for sabotage by analysing which equipment, systems or materials, if deliberately damaged, could lead to serious radiological consequences. The process of Vital Area Identification (VAI) should be based on the potential impact of sabotage scenarios (as outlined in the Design Basis Threat (DBT) and SyAPs annexes) and not limited to areas that contain nuclear material (i.e. critical safety systems in alternative facilities that, if damaged, could cause a release).*  Your arguments should explain how:   * The VAI 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:   * VAI methodology. * VAI 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 (PPS) that builds defence in depth and meets the required security outcome based on the categorisation for theft and sabotage. |
| *ONR Expectations: ONR expects dutyholders to design an integrated PPS that provides layered, defence-in-depth protection, meeting the required security outcomes for the site’s theft and sabotage categories. The PPS should incorporate a balanced mix of security measures (i.e. deterrence, detection, delay, assessment, response capabilities and insider threat mitigations), all of which should be tailored to achieve the specified outcomes graded by the severity of the consequences (higher consequences demand more stringent protection).*  Your arguments should explain how:   * The process by which you have reviewed the threats to your assets, and taken the findings of the categorisations for theft and sabotage, has informed the design of the PPS. * The key components of your PPS compare against the indicative postures contained within SyAPs, and provide 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/Facility Security Clearance) 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. * NPSA classifications of security equipment. * Configuration and locations of security equipment. * Operational procedures. * Utilities and backup provision. |
| **SyDP 6.4***: Vulnerability Assessments (VA)* | Sub-claim: We have satisfied ourselves that our physical protection system achieves the required security outcome by undertaking vulnerability assessments. |
| *ONR Expectations: ONR expects dutyholders to routinely conduct vulnerability assessments on their PPS to verify its effectiveness and identify any weaknesses. These assessments should be systematic and use proven methods to simulate adversary actions and stress-test the security arrangements.*  Your arguments should explain how:   * The process(es) you use to conduct a structured and systematic vulnerability assessment provides assurance that the PPS delivers the required outcome and is 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 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. |
| **SyDP 6.5***: Adjacent or Enclave Nuclear Premises* | 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. |
| *ONR Expectations: ONR expects dutyholders of nuclear sites that are co-located or adjacent to another to coordinate their security arrangements, giving mutual consideration to how one site’s activities or threats could affect the other.*  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 is managed, to ensure that when the situation changes at either site there is no negative impact upon the PPS of either site.   Your arguments may be supported by evidence contained within the following:   * Memorandum of Understanding (or similar arrangements). * Plans detailing shared security or safety services. * Contingency plans and emergency arrangements. |
| **SyDP 6.6:**  *Nuclear Construction Sites* | Sub-claim: We have ensured that we have implemented a physical protection system designed to ensure its activities cannot be exploited by an adversary to incorporate a latent defect or to pose a threat to an adjacent site. |
| *ONR Expectations: ONR expects dutyholders to implement tailored physical protection measures for nuclear construction sites to prevent adversaries from exploiting the construction phase to compromise future security or nearby facilities.*  Your arguments should explain how:   * You have implemented effective physical protection systems at the construction site to prevent adversaries from exploiting construction activities. This should also consider measures that have been implemented to avoid any latent defects being maliciously introduced in structures or components during building and ensuring the construction site cannot be used as a springboard to threaten an adjacent nuclear facility. * If the construction site is next to or within another nuclear site, you should describe how security arrangements consider the adjacent operating site’s protection. * The security measures will scale with the project’s progress; ONR expects a graded approach to security even during construction. * Security mitigations should be implemented in advance of each new risk phase.   Your arguments may be supported by evidence contained within the following:   * Construction site security plan and procedures. * Risk assessments and vulnerability studies. * Incremental security implementation records. * Personnel vetting and access control documentation. * Compliance and coordination records between relevant departments. |
| **SyDP 6.7:**  *Protection of Nuclear Material During Offsite Transportation* | Sub-claim: We maintain arrangements to ensure the protection of Category I-III quantities of nuclear material against theft and sabotage whilst in transit. |
| *ONR Expectations: ONR expects dutyholders to maintain robust security arrangements for the offsite transport of NM, commensurate with the category of material being moved, to guard against theft and/or sabotage in transit.*  Your arguments should explain how:   * Category I-III NM will be protected against theft and/or sabotage during transit. * You have taken into account critical measures like secure transport containers, escorts or guard force provisions. * You have tailored PPS measures to the category and risk posed to the material by theft/sabotage. * You have considered the legal requirements for the transportation of the material, both within and outside of the UK’s jurisdiction. * You have assessed the specific risks posed when transporting the nuclear material, including the proposed routes and how you have taken into account higher risk areas (i.e. through densely populated areas).   Your arguments may be supported by evidence contained within the following:   * Transport Security Statement and Plan. * Route risk assessments and procedures. * Compliance records. * Training and exercise documents. |

**FSyP 7 – Cyber Security and Information Assurance**

|  |  |
| --- | --- |
| FSyP 7 | 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.  *Context: Comprehensive CS&IA reflects the UK’s widest national security objectives (UK Cyber Security Strategy, Civil Nuclear Cyber Security Strategy) and ensures that the organisation’s most sensitive information and associated assets are protected. Effective Cyber Protection Systems (CPS) are capable of deterring, detecting, defending/defeating disruptive challenges (such as cyber attacks), facilitating mitigation of, and recovery from, any adverse effects. Done correctly, it minimises operational impact to enable efficient service delivery.* |
| **SyDP 7.1***: Effective Cyber and Information Risk Management* | Sub-Claim: We maintain arrangements to ensure that CS&IA risk is managed effectively. |
| *ONR Expectation: Risk management driven from Board level is fundamental to its effectiveness. Effective risk management is the process of understanding what assets the organisation has (and how important they are), how exposed they are to threats and vulnerabilities (the degree of risk), determining organisational tolerance for this risk and then taking steps to mitigate the risks to an acceptable level.*  Your arguments should explain how:   * Your risk management approach ensures the security of all critical assets as determined by the organisation. This should include, where applicable, SNI, IT and OT over the course of its lifecycle.   Your arguments may be supported by evidence contained within the following:   * Risk Appetite Statement. * CS&IA Roles & Responsibilities (roles may include Information Asset Owners, CISO, SIRO and others). * Information Assets Register, including a method of asset identification and categorisation process (please refer to the SyAPs sensitive-annexes). * A Critical Digital Asset Register. * Risk assessment approach (RGP includes ISO27001, IRAM2) including a control selection process. * Effective tiering of risks and appropriate risk treatment. * Ongoing assessment, monitoring and communication of risks. |
| **SyDP 7.2***: Information Security* | Sub-Claim: We maintain the confidentiality, integrity and availability (CIA) of sensitive nuclear information and associated assets. |
| *ONR Expectation: The process of determining which information and associated assets are considered relevant; hard copy SNI, computer-based systems that store, process, transmit, control, secure or access SNI should always be included; and technology stored or utilised on the premises in connection with activities involving NM or ORM relating to either nuclear safety or nuclear security, should always be considered.*  Your arguments should explain how:   * Your Information Security Policy and underpinning arrangements deliver CIA for SNI (and associated assets). This could include but not be exhaustive of:   + The organisational structure.   + Information asset identification and management.   + Risk assessment, treatment and management.   + Records retention.   + Third party management. * You identify and assure classified contracts by ensuring the arrangements to manage third party information security risks include risk assessment and contractual controls. This should include:   + The arrangements used to assess information 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;   + Your processes to manage the instigation, maintenance and closure of contracts with third party companies involving sensitive information and associated assets. |
| **SyDP 7.3***: Protection of Nuclear Technology and Operations* | Sub-Claim: We ensure our operational technology (OT) and information technology (IT) assets are secure and resilient to cyber threats. |
| *ONR Expectation: It is essential that dutyholders fully characterise their technology (which includes equipment and software utilised on nuclear premises in connection with activities involving NM/ORM) in accordance with ONR SyAPs and apply appropriate risk informed security controls.*  Your arguments should explain how:   * You can demonstrate that the selection of technical cyber security controls is risk informed and is aligned with the SyAPs or RGP to provide defence in depth. Including: * How you have selected the correct categorisation and outcomes for your facility's digital assets such as a) Computer Based Systems Important to Safety (CBSIS), (b) Computer Based Security Systems (CBSyS), (c) Nuclear Material Accountancy and Control (NMAC) Systems. * The mechanisms in place for identifying and testing control implementations; and, * How you provide resilience and assurance of your system security controls.   Your arguments may be supported by evidence contained within the following:   * Information Security Policy. * Operating Procedures, User Access Policy, Social Media Policy, Network Access Policy. * Risk management document set. * IT Penetration Test or ‘Healthcare’ Results. * System monitoring reports. |
| **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. |
| *ONR Expectation: Dutyholders should adopt appropriate physical protection measures to ensure that digital and non-digital information and associated assets are protected against a wide range of physical and non-physical threats.*  Your arguments should explain how:   * You deliver physical security controls to protect your sensitive information and associated assets. * The processes in place assure the physical security measures that protect your information and associated assets.   Your arguments may be supported by evidence contained within the following:   * Secure by design approaches used in determining appropriate requirements. * 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). * Surreptitious Threat Mitigation Process (STAMP) results. * Internal audits or assurance reports. |
| **SyDP 7.5***: Preparation for and Response to Cyber Security Incidents* | Sub-Claim: We have well-tested plans, policies and procedures to reduce vulnerability to cyber security incidents, non-malicious leaks and other disruptive challenges. |
| *ONR Expectation: It is critical that dutyholders ensure their security plan clearly details their arrangements to prepare for and respond to cyber security incidents, in support of maintaining effective CS&IA arrangements.*  Your arguments should explain how:   * Processes in place enable the identification and management of credible cyber and information security incidents and how your arrangements are tested, through all key stages of the incident response lifecycle. * 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. Dutyholders must be cognisant of the categorisation schema and outcomes in the SyAPs sensitive-annexes.   Your arguments may be supported by evidence contained within the following:   * Cyber & Information Security Incident Response Policy and Plans. * Incident notification and reporting arrangements. * Training and exercising. * Cyber & Information Security Incident Log. * Response and Recovery arrangements. * Organisational Learning. |

**FSyP 8 – Workforce Trustworthiness**

|  |  |
| --- | --- |
| FSyP 8 | Claim: We have implemented and maintain a regime of workforce trustworthiness to reduce the risks posed by insider activity.  *Context: Dutyholders should act to minimise the risks posed by insider threats, by ensuring the trustworthiness of the workforce. Dutyholders should implement pre-employment screening, ongoing personnel security measures and effective cooperation between departments to identify and mitigate risks posed by individuals with malicious intent.* |
| **SyDP 8.1***:*  *Co-operation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security* | Sub-Claim: We ensure that human resources (HR), occupational health and security departments cooperate to facilitate effective screening, vetting and ongoing personnel security arrangements for the workforce (staff and contractor community). |
| *ONR Expectations: ONR expects dutyholders to ensure that all internal departments involved in personnel security (such as HR, security and Occupational Health), work together seamlessly to implement effective screening, vetting, aftercare and ongoing personnel security for the workforce.*  Your arguments should explain how:   * You implement and maintain ongoing 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. |
| **SyDP 8.2***: Pre-employment Screening and National Security Vetting* | Sub-Claim: We deliver the appropriate combination of recruitment checks and vetting to satisfy ourselves of the honesty and integrity of our potential workforce (staff and contractor community). |
| *ONR Expectations: ONR expects dutyholders to carry out rigorous pre-employment screening and national security vetting (NSV) to verify the honesty, integrity and reliability of individuals before they are granted access to nuclear facilities or sensitive information.*  Your arguments should explain how:   * 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. * Your processes are used to determine the level of NSV clearance (where required). * Assurances are sought to complete a meaningful Employee Record Check in support of any NSV application and outcomes are recorded and dealt with appropriately.   Your arguments may be substantiated by evidence contained within the following:   * Policies and procedures to demonstrate compliance with Cabinet Office guidance and ONR requirements. * Training records for personnel security courses attended by HR staff and other relevant stakeholders (i.e. NPSA courses). * Arrangements for verifying the veracity of supply chain workforce trustworthiness check. * Procedures demonstrating how conditions of employment or caveats are managed. |
| **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. |
| *ONR Expectations: ONR expects dutyholders to implement ongoing personnel security measures to ensure that after initial vetting, the trustworthiness or employees and contractors is continually assessed and maintained.*  Your arguments should explain how:   * Your facility supports effective 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 are 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 this information is 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. * 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). * 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 these arrangements are communicated to staff so that they are always aware 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 are 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 Sponsor’s requirement to ensure that DV holders complete an Annual Security Appraisal Form (ASAF). * (For NSV holders) Triage processes are in place for ASAFs 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**

|  |  |
| --- | --- |
| FSyP 9 | Claim: We have effective guarding and policing arrangements, integrating the operations of relevant police forces e.g. Civil Nuclear Constabulary (CNC), British Transport Police (BTP), the Home Office Police Force (HOPF) and security guard services.  *Context: Dutyholders should ensure an effective use of policing and guarding resources to maintain site security. Dutyholders should work alongside local law enforcement, security guards and specialist resources (such as the Counter Terrorist Security Advisor (CTSA) or National Protective Security Authority (NPSA)) to provide an integrated response to potential threats.* |
| **SyDP 9.1***: CNC Response Force* | Sub-claim: We facilitate CNC deployment if appropriate to achieve the required security outcome. |
| *ONR Expectations: ONR expects dutyholders to fully support the deployment and readiness of the CNC at their site, so that an appropriate armed response is in place to meet the required security outcomes.*  Your arguments should explain how:   * 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).   Your arguments may be supported by evidence contained within the following:   * MoUs or similar. * Security contingency plans. |
| **SyDP 9.2***: Local Police Operations in Support of the Dutyholder* | 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. |
| *ONR Expectations: ONR expects dutyholders to cooperate with local HOPF to ensure that, in addition to the CNC, there is effective policing support for the nuclear site against threats as found in the UK DBT.*  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. * HOPF contribute to delivery of your mandatory 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. |
| **SyDP 9.3***: Security Guard Services* | Sub-claim: We employ civilian security guards to provide the unarmed guarding who conduct nuclear security operations as described in the security plan such as patrolling, access control and searching; and, who deliver or enable the immediate response to a security event. |
| *ONR Expectations: ONR expects dutyholders to employ and manage a professional unarmed security guard force to perform daily security operations (such as patrolling, access control, vehicle and personnel searches) and to serve as the first line of response in 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 are built into the guarding model, including their ability to respond to different counter terrorist (CT) response levels. * CGF 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**

|  |  |
| --- | --- |
| FSyP 10 | Claim: We have implemented and maintain effective security emergency preparedness and response arrangements which are integrated with the wider safety arrangements.  *Context: Dutyholders should conduct regular testing of their response arrangements and counter-terrorism measures, specific to their own site. Dutyholders should maintain detailed command and control structures, with individuals within the organisation being fully aware of their responsibilities and adequately trained to be able to effectively fulfil their function. Dutyholders should consider all threats as declared within the DBT when considering their emergency response arrangements; this should include not only physical security threats, but also cyber-related threats and insider risk. Smaller dutyholders should implement basic access controls, maintain clear identification procedures for personnel, and ensure robust perimeter security to mitigate common threat scenarios as outlined in the DBT.* |
| **SyDP 10.1***: Counter Terrorism Measures, Emergency Preparedness and Response Planning* | Sub-claim: We have in place incremental counter terrorism measures that can be implemented in response to changes in threat; and emergency preparedness & response (EP&R) arrangements to deal with any nuclear security event arising and the potential effects. |
| *ONR Expectations: ONR expects dutyholders to maintain scalable counter-terrorism measures and comprehensive security EP&R plans to address any nuclear security event as presented in the UK DBT and mitigate against the effects of such events.*  Your arguments should explain how:   * Your emergency response plans have been designed to address potential scenarios based on the DBT, ensuring readiness to respond effectively to a range of threat levels. * Your CT measures are proportionate to the threats identified in the DBT, covering likely tactics and approaches that may be employed by adversaries. * 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. * EP&R arrangements. * CT plan with incremental measures. * Memorandum of Understanding between dutyholder and Emergency Services outlining the expected response (proportionate to PPS Response and Required Effect). * Accounting procedures for personnel in the event of an incident. * EIMT schedule, ensuring equipment critical to emergency arrangements is of a good working order. * Media plan. * Exercise reports. |
| **SyDP 10.2***: Testing and Exercising the Security Response* | Sub-claim: We have implemented an exercise regime to train personnel and test the efficacy of our nuclear security contingency plans. |
| *ONR Expectations: ONR expects dutyholders to regularly test and exercise their security emergency response plans, to ensure that all individuals and organisations involved are well-prepared to act effectively during a real security event.*  Your arguments should explain how:   * Your exercises have been developed using scenarios aligned with the DBT, covering a range of likely threats and attack methods. Exercises should test responses to both physical and cyber threats as identified in the DBT. * You ensure that staff are trained effectively, and other relevant stakeholders are prepared to engage effectively with relevant threats such as unauthorised access and/or insider threats. * Regular drills/exercises conducted by site help to ensure that personnel are fully aware of their role and responsibilities in the event of an emergency. * 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. * OPEX is captured and shared. * You identify shortcomings and training needs throughout exercises and address this through continuous improvement. * 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. * Evidence of engagement encouraging multi-agency exercises including emergency services. * Evidence of response timings and points for improvement to allow for a robust response. * The process for capturing and sharing learning both within the site and from external organisations. * Scenario documentation. |
| **SyDP 10.3***: Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event* | Sub-claim: We have structures and processes in place to ensure effective command, control and communications arrangements during and post nuclear security events. |
| *ONR Expectations: ONR expects dutyholders to establish clear, robust command, control and communications (C3) arrangements to be used during a security incident and in the aftermath, ensuring that all responders can function in a well-coordinated manner.*  Your arguments should explain how:   * Key stakeholders for emergency response (for example on-call staff, HOPF, 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. * Your reporting arrangements will deliver the PPS response outcome and required security effects for any security incident. * Your reporting arrangements satisfy your obligations under statutory regulation. * All responders would work together in the event of an emergency (including who has overall control and any circumstances where this changes). * The contribution from external responders for the required security outcome would be facilitated. * Alternate arrangements are in place for control and communication, if the primary location you plan to use is unavailable or unusable. * You would maintain arrangements for extended durations. * You have a process for maintaining the sanctity of a crime scene after an incident. * You will return to business as usual after a serious incident.   Your arguments may be supported by evidence contained within the following:   * Communications plans and protocols. * Administrative arrangements. * Training relating to command and control. * Security contingency plans. * Security exercise reports. |

1. A site is categorised according to the quantity and type of nuclear material held at a site - typically a small dutyholder is one that holds Category IV material. [↑](#footnote-ref-1)
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 to use them; (b) managed through formal processes; and (c) reviewed periodically on a defined basis.’ [RASYP 7 – Security Plan Maintenance para 308 p 85 refers]. [↑](#footnote-ref-2)
3. An online version of NISR 2003 can be found at <http://www.legislation.gov.uk/uksi/2003/403/contents/made> [↑](#footnote-ref-3)
4. Official Sensitive Annexes to Security Assessment Principles 2022 Edition, Version 1.1 [↑](#footnote-ref-4)
5. Refer to SyAPs 2022 Edition Version 1 pp 64 – 75 for more detail on the KSyPP. [↑](#footnote-ref-5)
6. The SIS is used to record standards, procedures and arrangements ***to be adopted*** in accordance with Regulation 4(2). [↑](#footnote-ref-6)
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. [↑](#footnote-ref-7)
8. Dutyholders may find the clear process and flowchart at Appendix A to TAG 6.2 useful as the basis for their process. [↑](#footnote-ref-8)
9. SyAPs 2022 Edition Version 1 RASyP 4 – Security Plan Production – Outputs para 301 p82 - 83 refers. [↑](#footnote-ref-9)
10. ONR Classification Policy for the Civil Nuclear Industry (Issue 9) dated 15 Oct 24. [↑](#footnote-ref-10)
11. See SyAPs ‘RASyP 7 – Security Plan Maintenance’ for further guidance. [↑](#footnote-ref-11)
12. SyAPs RASyP 8, p86 refers.  
     [↑](#footnote-ref-12)
13. [ONR Classification Policy for the Civil Nuclear Industry](https://www.onr.org.uk/media/fyrdhw5g/onr-cnss-pol-001-the-nuclear-industries-security-regulations-2003-nisr-2003-classification-policy-for-the-civil-nuclear-ind.docx) [↑](#footnote-ref-13)