**ONR’s Experiences from Adopting an Outcome Focused**

 **Approach to Civil Nuclear Security Regulation**

M. Sims1

1Office for Nuclear Regulation (ONR), Redgrave Court, United Kingdom

Matt.sims@onr.gov.uk

Key Words: Outcome Focused Nuclear Security Regulatory Framework

**Abstract.** The purpose of this paper is to provide a narrative on the genesis of nuclear security regulation in the UK, capturing the dominant cultures and nature of interactions between the regulator and regulated at key stages of the transformation towards an outcome focused approach. The aim is share ONR’s learning from experience of the transition, providing insight into the successes, challenges, pitfalls and benefits in order to help inform the strategy of other regulatory bodies considering taking a similar journey.

1. **Introduction**
	1. In October 2001, the Office for Civil Nuclear Security was established as an independent security regulator within the Department for Trade and Industry. Following this, the UK enacted the Nuclear Industries Security Regulations (NISR) 2003[1] which OCNS was responsible for enforcing. Whilst these regulations are not inherently prescriptive in nature, the dominant culture of the time, combined with a lack of capability and capacity within the regulator and regulated bodies, led them to be implemented in a prescriptive fashion.
	2. In 2007, OCNS was transferred to the Nuclear Installations Inspectorate, part of the Health and Safety Executive responsible for nuclear safety. It is now a fully integrated part of the Office for Nuclear Regulation, which was itself created by The Energy Act 2013[2]. As part of this integration and to support a reinvigorated nuclear industry, ONR embarked on a transformation programme to move security regulation to a goal-setting approach. The first phase of this transformation was the publication of the National Objectives, Requirements and Model Standards document in 2012. This was followed by the Security Assessment Principles (SyAPs)[3], developed over three years and published in March 2017.
	3. SyAPs was designed to align with the well-established safety assessment principles in being outcome focused and providing ONR with a single regulatory framework which inspectors use to assess the adequacy of licensees’ arrangements, rather than a manual of prescriptive measures/model standards for licensees to adopt. This paper is intended to describe the journey from prescriptive to outcome focused nuclear security regulation and provide insight into successes, challenges and benefits that ONR have experienced along the way.
2. **Legislative Framework**
	1. In the late 1990s, it was recognised that the civil nuclear industries’ regulatory framework was not as robust as it should be and that the security regulator for the civil nuclear industry lacked independence because it was effectively part of an organisation that it regulated. Consequently the Office for Civil Nuclear Security was formed in October 2001 as an independent security regulator within the then Department of Trade and Industry (DTI). At the same time, work was initiated to improve the legislative basis on which it conducted its regulatory activity. The aim of this work was to produce a modern, comprehensive and effective regulatory system which was achieved with the enactment of NISR 2003. This legislation creates criminal offences for non-compliance and increased the scope to cover the protection of civil nuclear licensed sites and any other premises holding Category I-III quantities of nuclear material; transport security of Category I-III quantities of nuclear material; and, sensitive nuclear information wherever it is held in the UK.
	2. NISR 2003 does not prescribe the physical security measures that a licensee must adopt. Instead, the regulations require that each civil nuclear site must have a site security plan approved by ONR and describes the aspects or elements that the plan must cover. It also creates an offence for failure to comply with the standards, procedures and arrangements contained within an approved security plan.
3. **Development of Technical Guidance and Requirements Documents**
	1. Following publication of NISR, licensees were required to submit new security plans to the regulator for approval. The intent was for licensees to develop and justify their own arrangements. However, licensees were used to OCNS effectively acting as security advisor/consultancy and requested additional assistance to produce the plans. In response OCNS published a Technical Guidance Document (TGD), which set out model security standards that were graded according to site categorisation for theft or sabotage.
	2. The TGD held no legal status and was written in non-directive language to reflect that it was not meant to be complied with line-by-line. The content was based on the technical elements of previous regulation, early versions of IAEA Nuclear Security Series 13[4] and the Fundamental Principles and the intent was to provide a broad indication of security arrangements that licensees should consider. However, the reality was that licensees lacked capability to effectively design their own security solutions and instead submitted security plans that either referenced or copied verbatim the content of the TGD.
	3. The TGD was soon renamed the Technical Requirements Document (TRD), redrafted with directive language and presented as a prescriptive ‘check list’ for industry to follow thereby driving a culture of compliance without any serious thought by industry or regulator as to whether or not the TRD’s security requirements and standards were compatible with mitigating the risks pertaining to any given site. Its effect was to create a situation whereby industry did not have to understand or effectively manage its own risks – simply ‘doing what the regulator said’ was sufficient. Furthermore, the regulator was acting in a supervisory role for all aspects of security at licensed sites, was the security advisor and consultant and was responsible for the provision of security policy. This happened as a consequence of a range of factors, primarily a lack of security capability and capacity within licensee organisations and a pervasive culture of supervision that was a legacy from the time OCNS was the security department for the United Kingdom Atomic Energy Authority.
	4. Industry, therefore, was delivering security but not from a position of maturity, ownership and understanding. Furthermore, there was no need for such capability to be developed when the regulator was plugging the gaps. This meant security prioritisation within board level activities was far too low and its delivery played ‘second fiddle’ to safety.
	5. In many aspects the regulator (OCNS) perpetuated this state of affairs. As industry became ever less competent the regulator increased its security consultancy and supervision of security at licensed sites.
4. **Development of National Objectives, Requirements and Model Standards**
	1. In 2007. OCNS was transferred to the Nuclear Installations Inspectorate, part of the Health and Safety Executive responsible for nuclear safety. Initially, OCNS was administered from a separate office and effectively operated as a distinct business unit. Over time, integration improved, particularly as new security inspectors were recruited to work from the NII headquarters in Liverpool, which facilitated better communications and joint working practices.
	2. Driving the move for integration was a change in UK energy policy, which included nuclear new build and the UK government’s desire for the industry to be efficiently regulated. Consequently, OCNS was disestablished in 2012 and the functions of nuclear safety and security regulation were formerly brought together, along with safeguards and transport, to form the Office for Nuclear Regulation; an agency of the HSE. At this point, safety regulation was operating within an outcome focused regime, whereas security remained largely prescriptive. This difference of approach had the potential to hamper efficiency which resulted in a transformation programme to move security regulation to an outcome focused regime being initiated.
	3. In recognition of the challenges, a phased approach to the transition was proposed. The first phase was the publication of the National Objectives, Requirements and Model Standards (NORMS) document in 2012 to replace the Technical Requirements Document as the basis for assessment. NORMS placed an emphasis on meeting objectives and providing justification that arrangements were adequate rather than applying strict adherence to standards. In addition to the emphasis on objectives, there was an expectation that NORMS-aligned security plans would move beyond the current format of operational orders (the ‘what’) and provide more analysis of the ‘why’ and ‘how’. These elements were to be captured within a new front-end section of the security plan termed the Nuclear Security Case. This part was supported by the ‘what’, captured within the second part termed the ‘Integrated Protection Solution.’
	4. In 2014, a NORMS implementation review was conducted to inform the next phase of development. The industry commented that NORMS was an improvement on the TRD, however, its success in driving the required cultural change and progressing the journey towards outcome focused regulation was limited by the following factors:
5. The document was developed primarily by ONR. Industry were invited to comment prior to publication but had little opportunity to contribute during the early stages.
6. The timescales for development meant that there was insufficient stakeholder engagement to communicate the intent of the document and allow industry to make adequate preparations for its introduction.
7. The directive language from the TRD remained. Therefore it was unclear to both industry and ONR inspectors which elements were mandatory and where there was flexibility to incorporate innovation.
8. The document continued to set out a comprehensive suite of model standards which:
9. provided an easy route to demonstrate compliance without developing capability and justification that security arrangements were effective;
10. stifled innovation and continuous improvement and,
11. prevented transfer of security and risk ownership from the regulator to industry.
12. **Development of Security Assessment Principles**
	1. The comprehensive NORMS implementation review provided valuable feedback and insight into the successes and failures. This information was used to set the following objectives and success criteria for the subsequent iteration.



*1 - SyAPs project objectives*

* 1. Initially termed NORMS 2, the name was quickly replaced due to negative perceptions of the words ‘Requirements’ and ‘Model Standards’. In particular, the word Requirements is fundamentally synonymous with prescription and the term model standards was no longer appropriate given that they would not form part of the document for the reasons provided above. Consequently, ONR published the Security Assessment Principles (SyAPs) in 2017.
	2. Stakeholder engagement was fundamental from the document’s inception through to publication; indeed, the initial workshop with industry started with a blank piece of paper and many of the concepts developed that day made it through to the final publication. This ensured that the document’s intent and utility was fully understood by licensees, securing their support and the long development time allowed preparations to be made in anticipation of its publication. Part of this intent was to encourage industry to adopt aligned and complimentary arrangements that would satisfy the expectations of both security and safety regulation concurrently.
	3. In addition to the extensive engagement and development time, SyAPs was a radical departure from NORMS in two key areas. Firstly, it was written to be a document for ONR inspectors to use as the basis to underpin their judgement regarding the adequacy of licensees’ arrangements as opposed to being a list of requirements that must be adopted. Secondly, model standards were replaced with graded outcomes, meaning licensees were left with no option but to develop and justify the adequacy of their own solutions. A key aim of removing model standards was to transfer risk and ownership for security to licenses, thereby ensuring they became the controlling mind whilst encouraging innovation and efficiency through ONR’s adoption of an enabling approach to regulation.
	4. The development of graded outcomes was a significant challenge. Whilst it was clear for the highest category sites, where there needs to be a high level of confidence that even a worst case DBT attack will be defeated, more thought was required for lower risk sites to ensure that the outcomes wouldn’t drive disproportionate security measures. Ultimately, these outcomes were derived by designing hypothetical sites of each categorisation for theft and sabotage, protected by the complete suite of prescriptive model standards taken from NORMS. We then answered the question ‘What would be the optimum and realistic result that the security of this site could expect to achieve should it be subject to a DBT attack?’ The answer was then condensed to form the graded outcomes, which were fundamentally representative of the risk appetite of the model standards but in a non-prescriptive way.
	5. At this point, concern was raised over the level of capability within ONR and licensee organisations to effectively accommodate the radical departure from model standards. Therefore, a second exercise was undertaken to distil the prescriptive standards into a few descriptive sentences across the functions of detect, delay, assessment, access controls and insider mitigations. These descriptions were then assigned a security posture and mapped against the appropriate security outcome. These indicative postures support the security outcomes and have proved a useful tool both for licensees to justify their arrangements, and for ONR inspectors to identify potential gaps thereby informing a targeted assessment strategy.
	6. In addition to the removal of model standards, SyAPs significantly expanded regulatory expectations into strategic areas such as governance, leadership, competence management and supply chain assurance. Additionally, SyAPs was authored to allow publication in the interests of openness and transparency and to assist in communicating to a wider audience of people that would not typically have had access to security documentation, thereby improving security awareness.
	7. As with NORMS, the publication of SyAPs resulted in an expectation that licensees will develop new security plans. However, the expectation was that these plans would be based on a structure of claims, supported by arguments and substantiated by evidence. The development of such plans necessitated a significantly improved understanding of risk and robust approaches to demonstrate that security arrangements are adequate in the absence of prescriptive standards against which to benchmark. From the regulator’s perspective, a more robust and considered approach to assessment was implemented, whereby inspectors are required to form judgements based on fully justified decision making.
1. **Challenges and Learning**
	1. Developing SyAPs proved extremely challenging and resource intensive, in large part due to the extensive engagement and inherent complexity involved in the task. On publication of SyAPs, the original project team was disbanded on the assumption that much of the hard work had been completed. However, the reality was that document production was only the initial part of a far greater piece of work required to ensure effective implementation of regulation against it. Whilst this was recognized and a new team with adequate resourcing and robust project controls was reestablished, the implementation phase suffered from drift in the intervening period. Capability of this reformed team was undoubtedly enhanced through the addition of an experienced nuclear safety inspector to advise on alignment with safety processes and build on the learning from the implementation of outcome focused safety regulation. In a similar vein, we found that the level of quality and maturity of SyAPs-aligned security plans submitted to ONR for assessment was noticeably higher where the licensee had involved experienced safety professionals (such as members of the safety case team) in its development. Quality was also higher where licensees had involved their internal assurance teams in the sign-off process prior to submission to ONR.
	2. The initial implementation plan was for the civil nuclear estate to be operating with new SyAPs aligned plans by the end of 2019. It quickly became obvious that this delivery plan was too optimistic regarding the licensees’ ability to deliver ‘right first time’ security plans and underestimated the extent of iteration required to achieve balanced regulatory decisions. Consequently, the plan was revised to reflect timings that were more aligned to those commonly experienced for assessment of nuclear safety, whilst incorporating a degree of conservatism and structured in a way to provide some flexibility to move components.
	3. The project recognised that the capability of industry to develop SyAPs aligned security plans, and ONR’s ability to assess them, would be a major constraint. Following this recognition, a training needs analysis was performed and a comprehensive SyAPs Mechanics of Assessment course developed. This course was not only delivered to ONR inspectors, but was also opened to industry staffs responsible for security plan development to promote shared understanding and transparency of regulatory expectation. It will also be made available to other UK regulatory bodies wishing to implement outcome focused security regulation, particularly those with responsibilities under the Network and Information Systems Directive.
	4. Despite the high quality of the training, the initial package was theory based, or populated with safety assessment examples, because assessment of security plans had not occurred at that point and there was no operational experience available to underpin the course. Consequently, a further two-day workshop was delivered where lessons identified from initial assessments were shared to develop understanding and improve capability. The need for continuous improvement and a focus on consistency remains and is being supported by further divisional workshops, group and ‘one-to-one’ sessions. However, whilst the efforts spent on delivering quality training and sharing learning has greatly helped, the lack of familiarity with the new ways of working resulted in increased stress on ONR’s inspectors. It was therefore important for senior managers to provide clear messaging that SyAPs should be prioritized at the expense of other activity to ensure workloads remained manageable over the period of increased pressure. A dedicated assessment cadre could have helped reduce the impact.
	5. Linked to the above is culture, which combined with complexity and the associated requirement to build capability to address it, has been the most significant challenge to overcome. The majority of ONR security inspectors were used to regulating in a prescriptive environment against clearly defined requirements and models standards. Inspectors have found the required cultural and mindset change difficult and the project recognised the need to maintain efforts in this area to achieve and sustain the transition. Licensees have also recognised similar issues amongst their staff and ONR is regularly asked to provide technical guidance which, if delivered, risks returning to prescriptive regulation or regulatory capture. However, some ONR inspectors have similarly expressed a desire for more prescriptive guidance in some instances. To combat the need for further guidance the project team undertook a number of enabling interventions.
	6. During a lessons learnt activity, it became apparent that a number of low hazard and risk sites, with limited security capability and capacity, were likely to be facing disproportionate and prohibitive costs to develop and implement outcome focused, SyAPs aligned security plans and arrangements. The lessons learnt activity also identified that industry would benefit from a good practice guide on the production of a SyAPs security plan. Accordingly, ONR produced a guidance document to provide assistance in addressing the challenge for smaller licensees, which has received positive feedback. A similar document was also produced to assist the Class B Approved Carriers (i.e. organisations approved to transport Category III quantities of nuclear material) develop transport security statements to be assessed against SyAPs.
	7. There was a failing to recognise the effect that publication of SyAPs would have on other ONR security guidance and standards documents. For example, the previous NISR guidance document was incompatible with an outcome focused regulatory approach. The previous classification policy was also highly prescriptive and resource needed to be quickly diverted to ensure any other publications were identified, reviewed and either aligned or withdrawn.
	8. The legislation (NISR 2003) has also presented challenges. Whilst some elements facilitate an outcome focused approach, others do not. This was recognised relatively late in the project and considerable time was taken to consider and develop new ways of using the various instruments in the regulations to accommodate outcome focused regulation in a way that satisfies legislation to the lawyers agreement. Whilst suitable legal practices have been identified, it is likely that an amendment to the legislation will be required to take full advantage of an outcome focused regulatory regime. Earlier identification of this issue and communication with lawyers would have been advantageous.
2. **Benefits Realisation**
	1. The benefits of implementing an outcome focused approach should be considered to be sectoral rather specific to ONR. Some benefits will only be possible following amendment to the regulations and others are only likely to be realised in a five to ten year timescale. For example, as operations/processes change or current security equipment needs replacement due to end of life, the increased flexibility will open up more opportunity to develop innovative security solutions that are better harmonized with other business functions and maximize the use of new technology. Given the difficulty in measuring such benefits, ONR will be commisioning a technical support contract, making the use of subject matter experts in the field of benefits realisation to ensure they are fully captured and understood in a comprehensive study. However, other benefits are already evident and are summarized in the following paragraphs. This is an area that needs to be fully considered before the programme of change commences.
	2. The alignment of approach with safety allowed SyAPs to be built on many of the concepts and principles already established within the Safety Assessment Principles, using similar language and terminology wherever possible. This resulted in a document that landed with a broader audience than was previously the case and with security approaches/concepts that were understood by senior management and therefore more readily accepted. This top-level interest and buy-in to security has greatly improved its standing and culture within licensee organisations.
	3. Following on from this, the focus on higher level concepts/principles and lack of technical security detail also meant that the document could be published open source. This was a first for security regulatory guidance, which consequently could be freely and broadly communicated and celebrated, including incorporation within security education and awareness programmes.
	4. The alignment of approach also meant that existing processes in place to achieve safety regulatory expectations could simply be expanded to achieve the same for security. This has allowed greater integration and consistency between safety and security, resulting in enhanced efficiency. Examples include the nuclear baseline and supply chain assurance. Furthermore, this alignment has improved the safety and security interface within ONR, enabling far closer working between our cyber security and control and instrumentation specialists; emergency preparedness specialists; and, corporate interventions focused on issues of organisational effectiveness, leadership, governance and culture.
	5. Outcome focused regulation is also more flexible and future-proof. The UK new build programme potentially includes new and novel technologies, where existing model standards may have been inappropriate or stifled innovation and development. The added flexibility also has benefits in being more adaptive to changing threats. This is of particular relevance to cyber security, where the rapidly changing environment might otherwise result in continually updating model standards to chase emergent threats.
	6. The development and assessment of security plans against an outcome focused framework requires an uplift in capability. Consequently, we have significantly enhanced the skills and qualifications of ONR security inspectors. This was achieved by the award of a 14% pay enhancement for those successfully achieving a formal security management qualification accredited to Level 6 on the UK National Qualifications Framework. This element has now been subsumed within a new base rate with a concomitant expectation that new inspectors must have the requisite qualification to gain employment. Consequently, recent recruitment campaigns have benefited from a significant improvement in the caliber of applicants for new inspector positions.
	7. Due to the impact that regulator actions have on the regulated, we have also witnessed similar improvements to the competence of security teams within licensee organisations. This has resulted in an improved understanding of site risks together with more mature justification that they are effectively managed, which has improved confidence and assurance that security is adequate. This upskilling and professionalisation has also greatly contributed to improved security culture throughout the industry.
3. **Conclusion**
	1. Outcome focused approaches to regulation are inherently more complicated to implement than prescriptive approaches. The journey towards implementing an outcome focused regulatory regime may be more challenging where there is an existing prescriptive approach and compliance culture that has to be overcome. This challenge should not be underestimated; staff and industry need to be brought along on the journey through the provision of adequate support. In that regard, a robust training package is essential, as is effective activity to routinely capture and share lessons leant at the divisional, group and individual level.
	2. Given the challenges and complexity, a comprehensive change programme approach is highly recommended. Additionally, during delivery a dedicated, experienced project team with effective and robust governance should be considered to assist in providing focus on operational delivery, management of change, timely identification and resolution of risks and taking advantage of operational experience. This is important to ensure the project remains agile and adaptive to emergent issues, which may not have been predicted due to the nature of the work. The team should include both safety and security subject matter experts to ensure that a holistic and integrated approach is adopted; this is true not just for the regulator in developing the framework, but also the licensee in producing mature Claims/Argument and Evidence based security plans, which should also be subjected to scrutiny by internal assurance before submission to the regulator.
	3. Having stated the challenges and complexities, the rewards of implementing an outcome focused approach are likely to be especially worthwhile where the industry is large, diverse and/or growing to incorporate new nuclear power stations. It should be stressed that the rewards and benefits are evident for both the regulator and regulated. In particular, this type of approach is likely to be more capable to accommodate novel technologies and more responsive to changing threats. The latter is particularly true in the rapidly changing threat environment of cyber security. Even discounting these specific benefits, general improvements to culture, ownership, integration with safety and other business functions, regulatory efficiency and professionalisation of security are all facilitated by outcome focused regulation. ONR wishes all those willing to embark on the journey good luck and hope that the UK’s experiences described within this paper assist the venture.

**Appendix 1: References**

[1] The Nuclear Industries Security Regulations 2003, Statutory Instrument 2003 No.403

[2] The Energy Act 2013, Chapter 32

[3] OFFICE FOR NUCLEAR REGULATION, Security Assessment Principles for the Civil Nuclear Industry, 2017 Edition, Version 0 <http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf>

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, (INFCIRC/225/Revision 5) January 2011