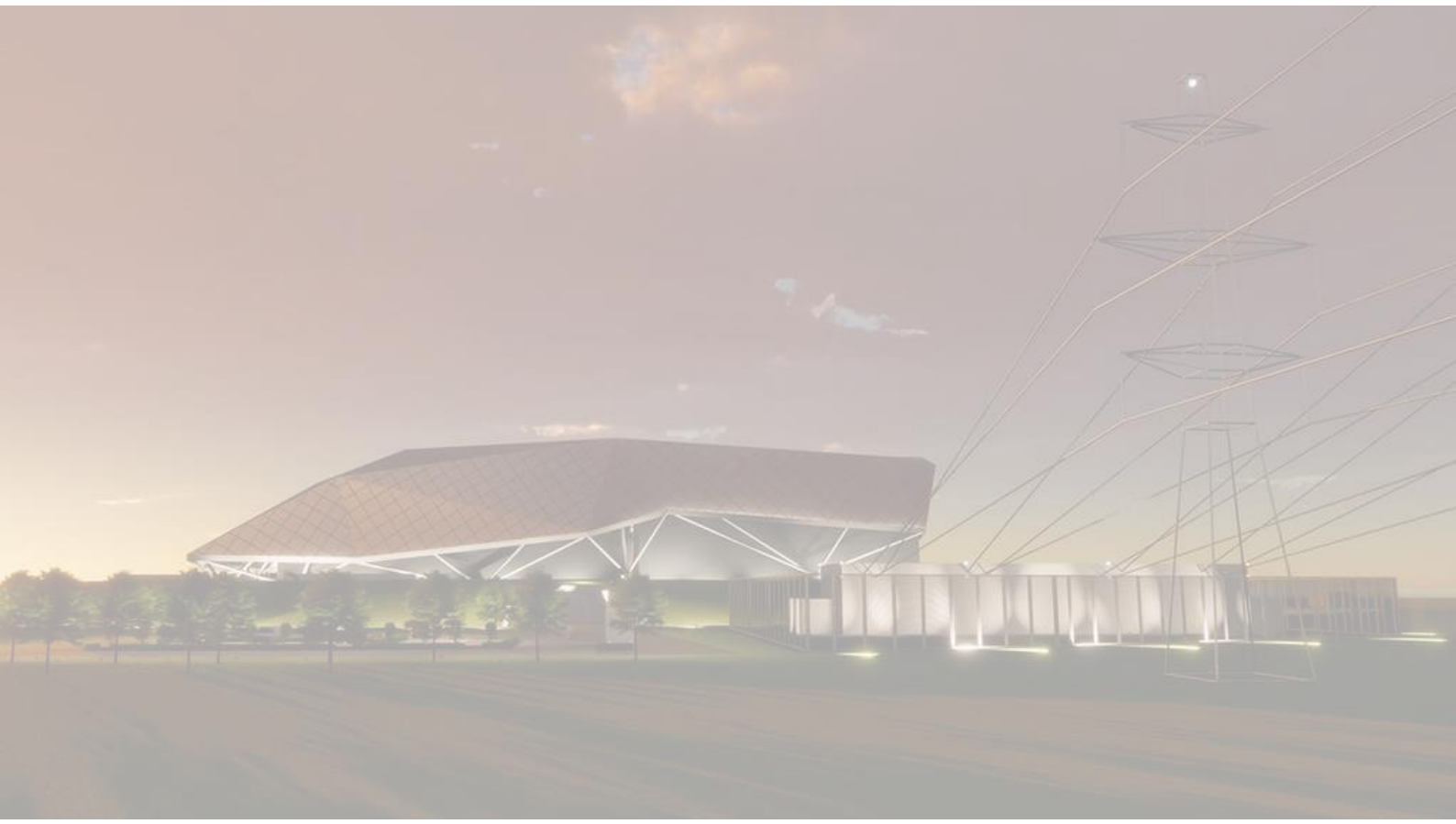
# Supplier Cyber Security Standard

## Standard Owner: Head of Security



# Table of Contents

## 1. Introduction

In today's interconnected digital landscape, ensuring robust cyber security measures is paramount for safeguarding sensitive information and maintaining operational integrity. As suppliers play a critical role in the supply chain, it is essential to establish comprehensive cyber security standards that address potential vulnerabilities and threats. This standard outlines the fundamental principles and practices that suppliers must adhere to, ensuring a secure and resilient partnership. By implementing these standards, we aim to protect our mutual interests, foster trust, and enhance the overall security posture of our collaborative efforts

## 2. Purpose

The purpose of this standard is to describe the Rolls-Royce Small Modular Reactor (SMR) Supplier Cyber Security Standard and supports the S4.3 Integrated Management System (IMS) processes which describe our approach to the approval and assurance of suppliers.

## 3. Scope

This Supplier Cyber Security Standard applies to all suppliers, vendors, and third-party service providers who engage with our organisation. The standard encompasses the following areas:

- **Context of the Organisation**. This area focuses on the broader environment in which the organisation and its suppliers operate. It includes an analysis of regulatory requirements, organisational structure, and stakeholder expectations.
- **Leadership and Management for Security**. This area focuses on the roles and responsibilities of organisational leaders in establishing and maintaining a robust cyber security posture. This theme emphasises the importance of executive commitment to security, the development of clear policies and procedures, and the allocation of resources to support security initiatives. It also highlights the need for continuous monitoring, assessment, and improvement of security practices, as well as fostering a culture of security awareness throughout the organisation.
- **Organisational Culture**. This area focuses on promoting shared values, beliefs, and behaviours that prioritise cyber security. It involves encouraging open communication about security issues, providing regular training and awareness programs, and recognising and rewarding secure practices. By embedding security into the organisational culture, employees at all levels become active participants in maintaining and enhancing the organisation's cyber security posture.
- **Management of Human Performance**. This area focuses on optimising the effectiveness and efficiency of individuals within the organisation to enhance cyber security. This theme involves setting clear performance expectations, providing necessary training and resources, and implementing performance monitoring and feedback mechanisms.
- **Cyber Security and Information Assurance (CS&IA)**. This area focuses on protecting the organisation's information assets from cyber threats and ensuring the integrity, confidentiality, and availability of data. This theme involves implementing robust security measures, such as encryption, access controls, and regular security assessments. It also includes developing incident response plans, conducting audits, and ensuring compliance with relevant regulations and standards.
- **Workforce Trustworthiness**. This area focuses on the importance of ensuring that employees and contractors are reliable and adhere to the organisation's security policies. This theme involves conducting thorough background checks, implementing strict access controls, and fostering a culture of integrity and accountability. It also

includes regular monitoring and auditing of employee activities to detect and prevent potential security breaches.

# 4. Supplier Requirements

## 4.1. Context of the Organisation

- To ensure the highest level of cyber security within our supply chain, Rolls-Royce SMR requires suppliers to provide detailed information regarding their operations, product development, assembly processes, and cyber security measures. This standard aims to create transparency and foster trust between Rolls-Royce SMR and its suppliers.

  - **Countries of Operation**

  Suppliers must provide a comprehensive list of countries in which they operate, including locations where they have offices, sell products, or conduct any business activities. For each country, suppliers should describe the nature of their activities, such as sales, marketing, customer support, or other relevant operations. This information helps Rolls-Royce SMR understand the global footprint of its suppliers and assess potential cyber security risks associated with different regions.

  - **Product Manufacturing and Development**

  Suppliers are required to list the countries where their products, including hardware, software, firmware, or components, are manufactured or developed. For each country, suppliers should describe the specific activities conducted, such as research and development, production, testing, or quality assurance. This information is crucial for Rolls-Royce SMR to evaluate the security measures in place during the product lifecycle and ensure compliance with international standards.

  - **Product Assembly**

  Suppliers must provide a list of countries where their products are assembled. For each location, suppliers should describe the assembly processes and any associated activities, such as final testing, packaging, or distribution. Understanding the assembly locations and processes allows Rolls-Royce SMR to identify potential vulnerabilities and implement appropriate security controls.

  - **Cyber Security Breach History**

  Suppliers are required to disclose any cyber security breaches they have experienced in the last five years. This includes providing detailed information about the breach, the response actions taken, and the initiation of their incident response plan. Suppliers should outline the steps they took to mitigate the breach, restore security, and prevent future incidents. This transparency is essential for Rolls-Royce SMR to assess the supplier's resilience and readiness to handle cyber threats.

  - **Cybersecurity Risk Insurance**

  Suppliers must confirm whether they have cybersecurity risk insurance. If they do, they should provide details about the coverage, including the scope and limits of the policy. Cybersecurity risk insurance is an important aspect of a supplier's overall risk management strategy, and having this coverage demonstrates a proactive approach to mitigating potential cyber security risks.

## 4.2. Leadership and Management for Security

  - **Governance and Leadership.**

  Suppliers must ensure that their Board of Directors has clearly defined roles and responsibilities related to security. This includes establishing accountability for security decisions and actions at the highest level of the organisation. Security must be treated

as a priority in strategic decision-making and leadership. Suppliers should demonstrate a commitment to integrating security considerations into their overall business strategy. Mechanisms must be in place to ensure the Board receives up-to-date information on security threats and risks. This includes regular briefings, reports, and access to relevant security intelligence. The Board must have appropriate membership and competence to assess and act effectively on security information. This includes having members with relevant security expertise and experience.

- **Capable Organisation.**

Suppliers must collect data from a range of sources, including performance indicators, staff feedback, event investigations, and both independent and self-assessments. This comprehensive data collection supports informed decision-making and continuous improvement. An independent security oversight function or internal regulation function must be in place with the capability, capacity, and authority to confirm that the security function can perform its role effectively. A robust security governance structure must be established within the organisation. This includes a clear security organisational structure with corresponding roles and responsibilities, ensuring organisational resilience. Suppliers must maintain a design authority and a core security and intelligent customer capability to retain knowledge of security facilities, equipment, and arrangements.

- **Organisational Learning.**

A framework for organisational learning must be in place to systematically identify and correct deficiencies in security. This includes policies for encouraging staff to report security deficiencies and improvement opportunities. The organisation should focus on corrective action rather than blaming personnel. This approach fosters a culture of continuous improvement and accountability. Suppliers are encouraged to actively seek lessons learned from other organisations and incorporate these insights into their security practices. Regular de-briefings on recent security issues should be conducted to draw lessons identified and refresh staff understanding of security practices. Sufficient training must be provided for staff and management to recognise and report problems. Adequate resources should be allocated to support the reporting and resolution of security deficiencies.

- **Assurance Processes.**

An independent assurance function with clearly defined terms of reference must be established. Personnel undertaking assurance should be demonstrably independent from the operational line of management. The scope of internal assurance must be clearly explained, with ownership and understanding at the Board and Executive Management Level. An independent, suitably qualified, and experienced team of assessors must be in place to conduct security assessments. Mechanisms must be in place to identify under-performance and gaps in good practice, ensuring continuous improvement in security standards.

## 4.3. Organisational Culture

- **Maintenance of a Robust Security Culture.**

To maintain a robust security culture, suppliers must have a comprehensive security policy that emphasises quality and high performance. This policy should be effectively communicated to all personnel, ensuring that everyone understands and adheres to the security standards. An independent governance regime, led by the board, is essential to support a strong nuclear security culture, reinforced by management systems and organisational structures. Security expectations must be clearly defined

and communicated, with qualified security personnel in place to uphold these standards.

Continuous monitoring and regular reviews of security performance are crucial for identifying areas for improvement and incorporating lessons learned. Suppliers should implement performance metrics, conduct audits, and utilise feedback mechanisms to assess and enhance security practices. By fostering a culture of continuous learning and adaptation, suppliers can ensure a resilient and secure supply chain partnership with Rolls-Royce SMR.

## 4.4. Management of Human Performance

- **Identification and Analysis of Security Tasks and Roles.**

Suppliers must adopt a systematic approach to identifying tasks important to security. This involves a thorough analysis of all roles, including non-security specific roles, that contribute to the overall security posture. The identification process must encompass roles provided by contract or agency staff as well as direct employees, recognising the diverse contributions to security. By understanding the various tasks and roles involved, suppliers can ensure comprehensive coverage of security responsibilities.

- **Sufficiency and Competence of Persons Delivering Security.**

Staffing arrangements must cater to various levels of experience within the security function, ensuring a balanced and capable team. These arrangements should consider periods of normal operation, heightened threat levels, security events, and the requirements of contingency plans. It is essential to factor in time for training and personnel development, as well as the impact of leave and sickness absence, to determine appropriate staffing levels. Security exercises play a crucial role in validating the adequacy of staffing arrangements, supporting claims that staffing arrangements are sufficient to respond to challenging and resource-intensive scenarios.

## 4.5. Cyber Security and Information Assurance

- **Effective Cyber and Information Risk Management.**

Suppliers must design, document, and implement a comprehensive CS&IA risk framework, with ownership correctly positioned within the business. There should be a clear understanding across the organisation on how CS&IA risks are identified and managed, with established lines of defence and clarity over roles and responsibilities. Executive leadership must actively participate in and lead CS&IA risk management, understanding risk tolerance. Those accountable in the risk framework should not have conflicting objectives. Information assets must be identified, categorised, and clearly owned across the organisation, with oversight and leadership in the categorisation process. The risk assessment and analysis process should be threat intelligence-led, considering risks from partners, suppliers, customers, and other third parties, and compiled into a risk register or log. This process should allow for the identification and communication of both strategic and tactical risks. Auditing and oversight of the risk treatment process are essential, with documented and approved treatment decisions. Accepted risks must be correctly documented and approved at an appropriate level. Policies, standards, and procedures should be amended based on the risk framework output, incorporating behavioural controls. Cyber risk management must be embedded across the business, with risk owners understanding the risks they own and levels of residual risk. Regular reviews of the risk framework should be conducted, with alterations made in response to changes in legal and regulatory requirements.

- **Information Security.**

The organisation must maintain a register that adequately identifies information and associated assets. There should be mechanisms in place for identifying information and associated assets in third-party contracts, including their sensitivity. An established method for assessing third-party CS&IA arrangements is essential, ensuring that these arrangements manage down the supply chain appropriately. Continuous assessment and review of CS&IA arrangements for third-party companies must be conducted. Processes for managing the closure of contracts and securely destroying information and associated assets are crucial, requiring evidence of asset transfer and destruction reflected in asset and risk registers. Adequate protections must be in place for assets or information remaining with third parties post-contract closure. All systems, services, and applications running on computing systems should be scanned externally and internally for vulnerabilities on a recurring basis, with applications scanned for vulnerabilities prior to new releases. A process to remediate security risks identified by customers or industry-recognized vulnerability research organisations within a pre-negotiated timeframe is necessary. The organisation must have a business continuity plan (BCP) to support ongoing operations of systems, and the scope of equipment and/or services provided to the customer, with all components of the BCP reviewed at least annually and updated as needed to reflect changes.

- **Physical Protection of Information.**

The physical security measures must be part of a layered approach based on a comprehensive risk assessment that considers all relevant threats derived from credible threat information and intelligence. This risk assessment should be reviewed periodically to ensure that the controls in place remain commensurate with the threat. The organisation must identify and develop a suite of protective security recommendations to address identified risks. Removable media should be thoroughly scanned for malware before use or receipt from any source. The organisation must have a clear understanding of the risks associated with remote working and consider implementing a re-use and disposals policy. Records documenting the lifecycle of storage media and assets should be maintained, and single points of failure within the infrastructure must be identified. Detection capabilities should be monitored appropriately, and an alarm response force should be in place. All physical security measures must be adequately supported by procedural and personnel measures. The organisation should have a suitable in-contract monitoring process to ensure that security controls are maintained and remain commensurate with the risks they address. Additionally, an assurance plan for physical security measures should be established to ensure ongoing effectiveness.

- **Preparation for and Response to Cyber Security Incidents.**

The Incident Response Plan must be based on a clear understanding of security risks to networks and information systems (IT/OT) and consider risks from the supply chain and customers, with supporting documentation for such incidents. Senior management sponsorship is essential, including necessary approvals, authorities, and resources to execute the plan. The plan should be documented and integrated with wider organisational and supply chain response plans, communicated and understood by relevant business areas, and reviewed periodically or when the threat landscape changes. Arrangements for engaging external support must be documented, and assurance activities for the highest category systems should be completed at least annually. The plan must include advice on ransomware payments, recent and relevant training for the Cyber Incident Response Team (CIRT), and exercises that test all parts of the response cycle. The organisation should identify critical data, personnel, software applications, devices, systems, and facilities, utilise relevant threat intelligence for efficient alerting, and have compensatory measures for critical devices that cannot generate logs. The severity of incidents must be gauged, with processes for assigning

initial handlers and responders, understanding limitations of the incident response capability, and maintaining up-to-date network architecture diagrams. Familiarity with incident reporting requirements and processes is crucial, along with monitoring staff responsible for analysis, investigation, and reporting of alerts, defined roles and skills for monitoring staff, and routine testing of the monitoring service's capability to detect cyber incidents. The organisation should identify major incident types impacting operations, create separate containment strategies, have forensic capabilities or third-party arrangements, procedures for restoring key systems, SLAs with third-party vendors for system recovery, and a documented incident review process to capture and act upon lessons learned, sharing vulnerabilities on a need-to-know basis.

### 4.6. Workforce Trustworthiness

- **Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security.**

Staff occupying roles with responsibility for personnel security must be suitably qualified and experienced personnel (SQEP). Training, learning, development conditions of service, and exit policies should support the organisation's coordinated approach to personnel security. Line managers must be properly informed and trained on ongoing personnel security arrangements to ensure effective implementation and maintenance of security protocols.

- **Pre-employment screening and National Security Vetting.**

Pre-employment control, vetting, and ongoing personnel security arrangements must comply with the Personnel Security Policy. These arrangements should ensure that the organisation is assured of the veracity of checks completed by any organisation from which it shares or transfers its pre-employment screening data. This guarantees that all personnel security measures are thorough and reliable, maintaining high standards of security.

## 5. Supplier Response

To respond to this standard, suppliers must first thoroughly read and understand the Rolls-Royce SMR Supplier Cyber Security Assessment (CSA) Standard. Following this, they should complete the supplied Supplier Security Assessment Questionnaire, which is divided into six sections, all of which must be completed. For each requirement, the supplier should respond with either "yes" (the requirement is met), "no" (the requirement is not met), or "N/A" (the supplier believes the requirement is not applicable to the scope of work and associated purchase order supporting the contract). For each "yes" response, the supplier must document the level of maturity (based on the Capability Maturity Matrix (CMM) levels) that they believe the controls meeting each of the objectives are performing at. Additionally, the supplier should provide any supporting information within the comments section and upload evidence to support the claims aligned with each "yes" and maturity level response. This comprehensive approach ensures that Rolls-Royce SMR can accurately assess the supplier's security posture and compliance with the standard.

## 6. Certifications

If you have any valid certifications or attestations for information and cyber security standards, you can use them to demonstrate compliance with the Rolls-Royce SMR Supplier Cyber Security Assessment (CSA) Standard. For each relevant requirement in the CSA, you can enter the details of your certification or attestation in the comments box. Make sure to include a copy of the certification or the certification ID as part of the evidence. This helps Rolls-Royce SMR verify your compliance with the security standards. The certifications or attestations that can be used include:

- SOC2 Type 2

- ISO 27001
- Cyber Essentials/Cyber Essentials Plus
- CSA STAR CAIQ
- NPSA CAPPS
- Other comparable industry certifications

By providing this information, you help ensure that your security measures meet the required standards.

## 7. Non conformance

If a supplier is unable to comply with any of the above requirements, they must promptly notify Rolls-Royce SMR and provide a detailed explanation of the specific areas of non-compliance. The supplier should outline the reasons for non-compliance, any potential risks associated and propose a plan for remediation or alternative measures to address the gaps. Rolls-Royce SMR will review the provided information and work collaboratively with the supplier to determine an appropriate course of action, ensuring that security standards are upheld, and risks are mitigated effectively. Open communication and proactive problem-solving are essential to maintaining a secure and resilient supply chain partnership.

## 8. Reporting

If any of the above certifications or attestations change, suppliers must report these changes to Rolls-Royce SMR as part of their regular business operations. In the event of an incident or breach involving any Rolls-Royce SMR supplier, the supplier must report the incident along with a business impact assessment related to Rolls-Royce SMR information/data to the Security Operations Center and Rolls-Royce SOC (UK.SOC@Rolls-Royce.com and security@rolls-royce-smr.com) within 24 hours of becoming aware of, or reasonably suspecting, an information security event or incident has occurred. Suppliers must provide Rolls-Royce SOC with reports of the investigation undertaken and findings, including any relevant Indicators of Compromise (IoCs). Additionally, suppliers must promptly take all reasonable steps necessary to contain the incident, mitigate its impact, and prevent its recurrence. They must inform Rolls-Royce SMR of the corrective actions taken and provide a plan of further remedial action and timescales, with agreement on any joint actions required by the supplier and Rolls-Royce SMR.

## 9. Glossary

| Term | Definition |
|---|---|
| BCP | A Business Continuity Plan is a strategic outline that details the procedures and processes an organisation must follow to maintain or quickly resume mission-critical functions during and after a disruption or disaster. |
| CIRT | A Cyber Incident Response Team is a group of professionals responsible for preparing for, detecting, and responding to cyber security incidents. Their goal is to mitigate the impact of incidents and restore normal operations as quickly as possible. |
| CMM | The Capability Maturity Model is a framework that assesses the maturity of an organisation's processes in various domains. It helps organisations improve their processes by providing a structured path for incremental improvements. |
| CS&IA | Cyber Security & Information Assurance refers to the practices and processes designed to protect information systems from cyber threats and ensure the confidentiality, integrity, and availability of data. |
| Cyber Essentials | A UK certification scheme designed to help organisations protect themselves against common online threats. |
| Cyber Essentials Plus | An advanced certification under the Cyber Essentials scheme, including internal assessment and external vulnerability testing. |
| CSA STAR CAIQ | Cloud Security Alliance's Security, Trust, Assurance and Risk (STAR) Consensus Assessment Initiative Questionnaire (CAIQ). |

| | |
|---|---|
| IMS | An Integrated Management System combines multiple management systems (such as quality, environmental, and health and safety) into a single cohesive framework, allowing an organisation to streamline processes and improve overall efficiency. |
| Indicators of Compromise (IoCs) | Pieces of evidence that suggest a security breach, including suspicious network traffic, unusual file changes, or unexpected system behaviour. |
| IT | Information Technology encompasses the use of computers, networking, storage, and other physical devices, infrastructure, and processes to create, process, store, secure, and exchange all forms of electronic data. |
| NPSA CAPPS | National Protective Security Authority's (NPSA) Critical Asset Protection and Preparedness Survey. |
| OT | Operational Technology refers to the hardware and software systems used to monitor and control physical processes, devices, and infrastructure, such as those found in manufacturing, energy, and transportation industries. |
| Security Operations Center (SOC) | A centralised unit that deals with security issues on an organisational and technical level. |
| SLA | A Service Level Agreement is a formal contract between a service provider and a customer that outlines the expected level of service, including performance metrics, responsibilities, and guarantees. |
| SQEP | A Suitably Qualified and Experienced Person is an individual who possesses the necessary qualifications, skills, and experience to perform a specific role or task effectively and safely. |
| CSA | A Supplier Cyber Security Assessment is a comprehensive evaluation of a supplier's security practices and controls. It helps organisations ensure that their suppliers meet the required security standards and mitigate potential risks in the supply chain. |