Supplier Compliance and Evidence Matrix

The purpose of this document is to provide Suppliers with a guide to the evidence required to demonstrate compliance to legal and regulatory requirements in your contract.

How To Use This Matrix

Use this table to identify the requirements that apply to your contract and determine the evidence you need to provide for each applicable requirement.

1. **Identify the data classifications, system access, services and regulatory requirements relevant to your contract.**
2. **Review every matching scenario; more than one may apply.**
3. **Confirm the listed cyber security clauses are included in your contract.**
4. **Provide current evidence and complete any required remediation or risk process.**

- **Supplier check:** Ensure you meet every applicable legal or regulatory requirement. If evidence is missing, expired or identifies a gap, follow the action in Column 4 and contact your Rolls-Royce point of contact.

Supplier Compliance and Evidence Matrix

1. Data, access or regulatory scenario	2. When this applies	3. Contract cyber security requirements	4. Evidence you must provide
US Defence controlled data – Federal Controlled Information	Federal contract data not intended for public release	Federal Acquisition Regulation (FAR) and Defence Federal Acquisition Regulation Supplement (DFARS)	Where Cybersecurity Maturity Model Certification (CMMC) Level 1 is specified by the contract, provide evidence that the FAR 52.204-21 self-assessment is completed, and that the CMMC Level 1 self-assessment result/affirmation has been entered in Supplier Performance Risk System (SPRS). Link to CMMC resources: **https://dowcio.war.gov/CMMC/Resources-Documentation/**
US Defence controlled data – Controlled Unclassified Information	Sensitive government data requiring safeguarding (e.g., technical drawing, defense data)	DFARS/NIST 800-171	Where CMMC Level 2 is specified by the contract, perform the NIST SP 800-171 self assessment and enter the score in the Department of Defense (DoD) SPRS (the score must not be older than 3 years), or present a valid certificate. Where CMMC Level 3 is specified by the contract, the supplier must present a valid certificate that covers the applicable contract scope and remains valid. If not fully compliant: Supplier must present System Security Plan (SSP) / Plan of Actions and Milestones (POAM). POAMs supporting Conditional CMMC must be completed and closed within 180 days.
UK Defence **Ministry of Defence (MoD) Cyber Security MoD (CSM) v3 Level: Very Low / Low**	Information that is created, processed, sent or received which could cause no more than moderate damage if compromised and must be defended against a broad range of threat actors with differing capabilities using nuanced protective controls	DEFCON 658 02/22 / DefStan 05-138 (Issue 3) - Level: Very Low / Low	DefStan 05-138 v3: Provide the Supplier Assurance Questionnaire (SAQ) email response from MoD confirming compliance and Cyber Essentials Certificate. Link to SAQ: **https://forms.cloud.microsoft/Pages/ResponsePage.aspx?id=7WB3vlNZS0iuldChbfoJ5Tv4OR9pb0BHial1Ag-WKXVUOFk3Sk9SS0JDQ0FRWjhYNDhTVldHUDJaNy4u** Link to SAQ guidance: **https://www.gov.uk/guidance/cyber-security-model-question-sets** If the Supplier does not meet MoD SAQ compliance or hold Cyber Essentials certificate, they must complete a Cyber Implementation Plan (CIP) detailing the non-compliant controls and include a forecast compliance date. The CIP must also provide the action plan from the IASME Cyber Essentials Readiness Tool, and track the actions to completion. Link: **https://iasme.co.uk/articles/introducing-the-cyber-essentials-readiness-tool/**
UK Defence **MoD CSM v3 Level: Moderate / High**	OFFICIAL information that contains sensitive information and is marked "-SENSITIVE" Unintended disclosure or compromise of MoD data or systems can lead to moderate damage and in exceptional circumstances it could lead to a threat to life (i.e., safety consequence)	DEFCON 658 02/22 / DefStan 05-138 (Issue 3) - Level: Moderate / High	DefStan 05-138 v3: SAQ email response from MoD confirming compliance and Cyber Essentials Plus Certificate. Link to SAQ: **https://forms.cloud.microsoft/Pages/ResponsePage.aspx?id=7WB3vlNZS0iuldChbfoJ5Tv4OR9pb0BHial1Ag-WKXVUOFk3Sk9SS0JDQ0FRWjhYNDhTVldHUDJaNy4u** Link to SAQ guidance: **https://www.gov.uk/guidance/cyber-security-model-question-sets** If the Supplier does not meet MoD SAQ compliance or hold Cyber Essentials Plus certificate, they must complete a Cyber Implementation Plan (CIP) detailing the non-compliant controls and include a forecast compliance date. The CIP must also provide the action plan from the IASME Cyber Essentials Readiness Tool, and track the actions to completion. Link: **https://iasme.co.uk/articles/introducing-the-cyber-essentials-readiness-tool/**

Supplier Compliance and Evidence Matrix

1. Data, access or regulatory scenario	2. When this applies	3. Contract cyber security requirements	4. Evidence you must provide
UK Defence CSM v4 Level 0	Assigned where there is a very low level of assessed cyber risk. It requires Supplier organisations to demonstrate basic cyber security practices.	DEFCON 658 07/26 / DefStan 05-138 (Issue 4) – Level 0	Present a valid Defence Cyber Certificate (DCC) Level 0 that covers the applicable contract scope. If the Supplier does not fully meet the Level 0 requirements, they must contact their Rolls-Royce point of contact to request and complete a Cyber Improvement Plan (CIP) with non-compliant controls and include a forecast compliance date. Link to Supplier Cyber Protection Service (SCPS): **https://www.supplier-cyber-protection.service.gov.uk/scps** Link to CSM guidance: **https://www.gov.uk/guidance/cyber-security-model** If the Supplier does not hold a Cyber Essentials Certificate then the supplier must also complete IASME Cyber Essentials Readiness Tool for all critical systems in scope of the contract and include action completion dates within the CIP. Link: **https://iasme.co.uk/articles/introducing-the-cyber-essentials-readiness-tool/**
UK Defence CSM v4 Level 1	Assigned where there is a low to moderate level of assessed cyber risk. It requires suppliers to demonstrate a comprehensive cyber security programme with good practices.	DEFCON 658 07/26 / DefStan 05-138 (Issue 4) – Level 1	If compliant, present a valid DCC for Level 1 that covers the applicable contract scope and remains valid. If the Supplier does not fully meet the Level 1 requirements, they must contact their Rolls-Royce point of contact to request and complete a CIP with non-compliant controls, and include a forecast compliance date. Link to SCPS: **https://www.supplier-cyber-protection.service.gov.uk/scps** Link to CSM guidance: **https://www.gov.uk/guidance/cyber-security-model** If the Supplier does not hold a Cyber Essentials certificate, then the supplier must also complete IASME Cyber Essentials Readiness Tool for all critical systems in scope of the contract, and record the action completion dates within the CIP. Link: **https://iasme.co.uk/articles/introducing-the-cyber-essentials-readiness-tool/**
UK Defence CSM v4 Level 2	Assigned where there is a high level of assessed cyber risk. It requires suppliers to demonstrate advanced cyber security oversight and planning which drives robust organisational and cyber practices.	DEFCON 658 07/26 / DefStan 05-138 (Issue 4) – Level 2	If compliant, present a valid DCC Level 2 that covers the applicable contract scope and remains valid. If the Supplier does not fully meet the Level 2 requirements, they must contact their Rolls-Royce point of contact to request and complete a CIP with non-compliant controls, and include a forecast compliance date. Link to SCPS: **https://www.supplier-cyber-protection.service.gov.uk/scps** Link to CSM guidance: **https://www.gov.uk/guidance/cyber-security-model** If the Supplier does not hold a Cyber Essentials Plus certificate, then the supplier must also complete IASME Cyber Essentials Readiness Tool for all critical systems in scope of the contract, and record the action completion dates within the CIP. Link: **https://iasme.co.uk/articles/introducing-the-cyber-essentials-readiness-tool/**

Supplier Compliance and Evidence Matrix

1. Data, access or regulatory scenario	2. When this applies	3. Contract cyber security requirements	4. Evidence you must provide
UK Defence CSM v4 Level 3	Assigned where there is a substantial level of assessed cyber risk to a Supplier. It requires suppliers to demonstrate expert cyber security capabilities that apply a 'defence in depth' methodology to appropriately protect the organisation against new and evolving threats.	DEFCON 658 07/26 / DefStan 05-138 (Issue 4) – Level 3	If compliant, present a valid DCC Level 3 that covers the applicable contract scope and remains valid. If the Supplier does not fully meet the Level 3 requirements, they must contact their Rolls-Royce point of contact to request and complete a CIP with non-compliant controls and include a forecast compliance date. Link to SCPS: **https://www.supplier-cyber-protection.service.gov.uk/scps** Link to CSM guidance: **https://www.gov.uk/guidance/cyber-security-model** If the Supplier does not hold a Cyber Essentials Plus certificate, then the supplier must also complete IASME Cyber Essentials Readiness Tool for all critical systems in scope of the contract, and record the action completion dates within the CIP. Link: **https://iasme.co.uk/articles/introducing-the-cyber-essentials-readiness-tool/**
German Federal Government Defence - **Verschlusssache-Nur für den Dienstgebrauch (VS-NfD)** **VS-NfD classified information is German Federal Government classified data that is for official use only**	German restricted/classified data where unauthorised disclosure could harm public interests VS-NfD classified information is German Federal Government classified data that is for official use only	BSI Zulassung	BSI generally approves specific IT-security products, not the supplier. Request the applicable security-supervision evidence and details of the exact BSI-approved products, versions and scope used for VS-NfD from the Federal Office for Information Security (BSI) For Approved Cryptography requirements, evidence of the verification of BSI-approved encryption deployment is required on all devices within the applicable contract and approved security scope.
Australian Government - Defence Industry Security Program (DISP)	Official Business Information: UNOFFICIAL / OFFICIAL / OFFICIAL:Sensitive PROTECTED / SECRET / TOP SECRET	Australia Department of Defence: ASDEFCON (Australian Strategic Defence Contracting)	If compliant to DISP Membership level, provide official proof of membership at the required level per domain (entry to level 3). Cyber Posture: Annual Security Report (ASR) via the DISP Member Portal. Technical controls: Evidence of ASD Essential Eight implementation at Maturity Level 2 (applies to all DISP members).
NATO Data (all security classifications)	Joint-alliance defense contracts involving data classified as: NATO RESTRICTED (NR) / NATO CONFIDENTIAL (NC) / NATO SECRET (NS) / NATO COSMIC TOP SECRET	NATO General Provisions and Intellectual Property Clauses	NATO RESTRICTED clearance requirements vary by the supplier's nation. The Declaration of Eligibility is issued by the supplier's home country National Security Authority (NSA/DSA/MoD). FSC (Facility Security Clearance): Certified clearance for the physical premises handling NATO Confidential or above. Where a Security Aspects Letter (SAL) is issued, provide evidence demonstrating compliance with its project-specific security instructions.

Supplier Compliance and Evidence Matrix

1. Data, access or regulatory scenario	2. When this applies	3. Contract cyber security requirements	4. Evidence you must provide
Rolls-Royce sensitive data (e.g., Export Control, Personal Data, IP, etc.) or access to systems (including: Rolls-Royce sensitive data (e.g., Export Control, Personal Data, IP, etc.) or access to highly controlled systems)	Rolls-Royce classified data and information: Export Controlled, Personal Data, Sensitive Personal Data, Intellectual Property (IP), Rolls-Royce Private, Rolls-Royce Strictly-Private Access to GAD	Minimum Cyber Security Standard (MCSS)	Compliance to MCSS: Self-attestation MCSS compliance (e.g., document or letter that demonstrates self-assessment completed). If not fully compliant, the Supply Chain Cyber Security Team will assess risks arising from non-compliant requirements. If above risk appetite, a risk acceptance form must be signed by the Rolls-Royce business risk owner.
EU / UK GDPR	Personal Data and/or Sensitive Personal Data	Data Protection Agreement	On request by your Rolls-Royce point of contact, the supplier provides the applicable data processing agreement and documented technical and organisational measures. Certification (for example, ISO 27001 or ISO/IEC 27018:2019) can be used as supporting evidence.
EU NIS2 – High Impact **[Note: not fully implemented]**	Within scope of EU NIS2 regulations (Art. 21): Suppliers who have administrative access to Rolls-Royce networks, hosting data or providing vital operational uptime: High Risk: Managed Service Providers (MSP) and Managed Security Service Providers (MSSP) Cloud and Data Centre Providers Core SaaS and Software Developers	MCSS or Power Systems TOM ISO27001 or SOC2 report	Where contractually required, provide a valid in-scope certificate or assurance report. By request from your Rolls-Royce point of contact, you may be asked to present evidence of risk assessment, supply-chain security, incident handling, continuity, vulnerability management and secure development, where relevant.
EU NIS2 – Medium Impact **[Note: not fully implemented]**	Within scope of EU NIS2 regulations (Art. 21): Suppliers who do not have direct network access but are critical to Rolls-Royce physical supply chain or business continuity Medium to High Risk: Just in Time logistics and transport partners, Specialised Industrial/ Manufacturing Subcontractors	MCSS or Power Systems TOM	By request from your Rolls-Royce point of contact, you may be asked to provide evidence of formal information or cyber security policy sign-off, supplier-risk assessment, incident handling, access control, vulnerability management and supply-chain security. This may also include a summary of your company Business Continuity/Disaster Recovery (BC/DR) plan.

Supplier Compliance and Evidence Matrix

1. Data, access or regulatory scenario	2. When this applies	3. Contract cyber security requirements	4. Evidence you must provide
EASA Part-IS	Suppliers who have been identified with responsibilities for managing Rolls-Royce Global Information Security Management System (ISMS), and protecting Safety critical data (i.e., Safety Group 1 - 3)	MCSS ISO 27001	If compliant, present evidence required by the contract plus self-attestation of MCSS compliance (contractual agreement), and on request you may be asked by your Rolls-Royce point of contact to demonstrate that supplier-related information security risks, interfaces, contractual controls, monitoring and incident reporting are managed within your organisation. If not fully compliant: Supply Chain Cyber Security Team will assess the security risks. If above risk appetite, a risk acceptance form must be signed by Rolls-Royce risk owner.
UK Cyber Resilience Pledge	Suppliers who operate within the UK.	Cyber Essentials certificate plus meet the Pledge requirements	If compliant, the Supplier has completed UK Cyber Resilience Pledge actions including presentation of valid Cyber Essentials certificate. If not fully aligned with the Pledge requirements, the Supplier must share their compliance action plan including target dates, and track actions to completion. If not Cyber Essentials Certified, the Supplier must complete the Cyber Essentials Readiness Tool assessment, share compliance action plan and track the actions through to certification. Link: **https://iasme.co.uk/articles/introducing-the-cyber-essentials-readiness-tool/**
Customer, industry or data specific requirements (e.g., finance – SWIFT)	As per the customer, industry or data specific requirements (e.g., ISO 27001)	As per requirements	Where compliant, the Supplier must provide the evidence specified by the applicable customer, legal or industry requirement, which may include certification, together with self-attestation of MCSS compliance where contractually required. If the Supplier is not fully compliant, the Supply Chain Cyber Security Team will assess risks. If above risk appetite, a risk acceptance form must be signed by Rolls-Royce business risk owner.