UK SPACE AGENCY

Risk Assessment Workshop

Risk Assessment

When delivering a digital service, you need to identify, analyse and evaluate the potential cyber security risks. It is important to embed risk analysis and evaluation into digital delivery processes to continuously be aware of the highest priority risks.

- For more context into risk management from UK Government, please read The Orange Book – Management of Risk – Principles and Concepts.

- The gov.uk portal lists multiple frameworks including ISO, NCSC, and NIST. As a standard, the MoD uses the NIST framework, specifically 'NIST 800-30: Guide for Conducting Risk Assessments', as well as following industry best practises.

- This is used to support the risk assessment process and provide an established process to follow.

- For this workshop, we will do a run through of the NIST 800-30 risk assessment process, looking at both adversarial and non-adversarial risk.

The Senior Responsible Officer (SRO)

- The official description:
  - As set out by JSP 440 Leaflet 5C, it is the duty or the SRO to ensure Delivery Teams (DTs) are following Secure by Design (SbD) policy, ensure cyber risk is defined and published for the DT, and ensure that cyber risks are actively managed throughout the capability life cycle. The SRO must ensure delivery is underpinned by formal risk management framework.
- What this means:
  - The SRO is the person responsible for signing off on risk
  - The SRO should have an agreed risk appetite, and review if expected risk changes
  - All Security Working Group (SyWG) decisions should be signed off by the SRO (or SRO representative)
  - The SRO should be the last sign-off for security documentation

Note: the SRO does not need to be cyber qualified

Risk Appetite

A project's risk appetite is the level of cyber security risk the Senior Responsible Owner (SRO) and service owner are willing to accept. They need to take responsibility for creating a statement they're comfortable with. This should be in line with your organisation's risk acceptance thresholds.

The following steps help to create a risk appetite:

1. Summarise your project scope
   - Should be done in business case

2. Align with the organisation's risk appetite
   - Relevant elements of the org risk appetite should be included

3. Determine relevant security threats
   - Include malicious and unintentional

4. Determine the required constraints
   - Determine rules to be put in place to prevent unacceptable risks and cyber threats

5. Communicate the security risk appetite
   - Statement should be SRO approved and shared with relevant parties

NIST Risk Assessment

The gov.uk portal lists multiple frameworks including ISO, NCSC, and NIST. As a standard, the MoD uses the NIST framework, specifically ‘NIST 800-30: Guide for Conducting Risk Assessments’, amongst others.

NIST identifies four primary steps in the risk assessment process:

1. Preparation
2. Assessment
3. Communication
4. Monitoring and Maintenance

Scenario Company: Ping Floyd

Company Overview:

- Team Size: 15–25 personnel
- Project – Keep Talking: Satellite communications via CubeSat constellation
- Fleet: 5 CubeSats, each contributing 20% of total service functionality
- Mission: Deliver modular, resilient, and secure satcom services
- Sector Ambition: Expanding into defence and tactical communications markets

Differentiators:

- Distributed Architecture: No single point of failure
- Agile & Scalable: Rapid deployment and mission flexibility
- Defence-Ready: Built with security, redundancy, and reliability in mind

Step 1: Preparation

"By failing to prepare, you are preparing to fail"
- Benjamin Franklin

It is important to develop context of the risk assessment, including assumptions, constraints, and priorities.

- **Identify the Purpose** – Why is this risk assessment being conducted? How are the results of the risk assessment going to be used?
- **Identify the Scope** – What factors need to be considered in the risk assessment? What organisational tiers should this risk assessment apply to?
- **Identify Assumptions/Constraints** – Describe the operational environment in which your organisation works
- **Identify Information Sources** – What sources did you consult to find information about the threats/vulnerabilities being considered?
- **Identify Risk Model and Analytic Approach** – How do you plan to measure your risk assessment (e.g., quantitative, qualitative)? Will you be focused on the threats, the vulnerabilities, or the impacts?

Step 2: Assessment

This is the step to conduct the risk assessment, ultimately developing a prioritised list of risks. These will be scored based on several risk characteristics, including likelihood and impact. The key characteristics set out in NIST 800-30 are:

- Threat Source
- Threat Event
- Vulnerabilities and Predisposing Conditions
- Likelihood of Occurrence
- Magnitude of Impact
- Overall Risk Score

This workshop will run through the process of scoring each of these given characteristics using the NIST 800-30 annexes, one each for adversarial and environmental risk.

NIST-800-30-Risk-Assessment-Template

NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments

NIST Risk Assessment Template [w/ Example]

Step 3: Communication

When the risk assessment is complete, this should be brought to appropriate personnel and raised in the next Security Working Group. It should also be noted in the Security Management Plan and SbD Self Assessment Tracker in the relevant sections.

Step 4: Monitoring and Maintenance

A risk assessment is never one-and-done. As with Secure By Design, sustained vigilance and regular updates are required to stay current with policy, updates, and the ever-evolving threat landscape.

Example Adversarial Risk

Threat Event (E5)	Threat Source (D2)	Capability (D3)	Intent (D4)	Targeting (D5)	Relevance (E4)	Likelihood of Attack Initiation (G2)	Vulnerabilities and Predisposing Conditions (F5)	Severity and Pervasiveness (F2)	Likelihood Initiated Attack Succeeds (G4)	Overall Likelihood (G5)	Level of Impact (H2 H3)	Risk (I2)
Malicious Software Insertion - Adversaries insert malware into satellite firmware or ground control systems during development or supply chain stages, enabling sabotage or data exfiltration.	Group - Established	Moderate	Moderate	High	Moderate	Low	Moderate	Moderate	High	Moderate	Moderate	Moderate

Example Non-Adversarial Risk

Threat Event (E5)	Threat Sources (D2)	Range of Effects (D6)	Relevance (E4)	Likelihood of Event Occurring (G3)	Vulnerabilities and Predisposing Conditions (F5)	Severity and Pervasiveness (F2)	Likelihood Event Results in Adverse Impact (G4)	Overall Likelihood (G5)	Level of Impact (H2 H3)	Risk (I2)
Orbital debris collision - Accidental collision with space debris damages or destroys UK-owned or partnered satellites, impacting service continuity, and increasing debris proliferation	Environmental - Natural or man made disaster	Low	High	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate

Any Questions?