CPNI

Centre for the Protection of National Infrastructure

RISK ASSESSMENT PROCESS

Guidance on the cyber-security risk assessment process for critical national infrastructures.

CONTENTS

FIGURES

TABLES

01. INTRODUCTION

This document provides a summary of a generic systems-driven risk assessment approach. As with all fields, risks assessment is evolving, but some recent perspectives can be found in the NCSC guidance[1].

02. SIGNPOSTING

This is the second detailed generic guide in the stack of resources for security-informed safety assurance. Figure 1 below shows its location in the set of guides (highlighted in red).

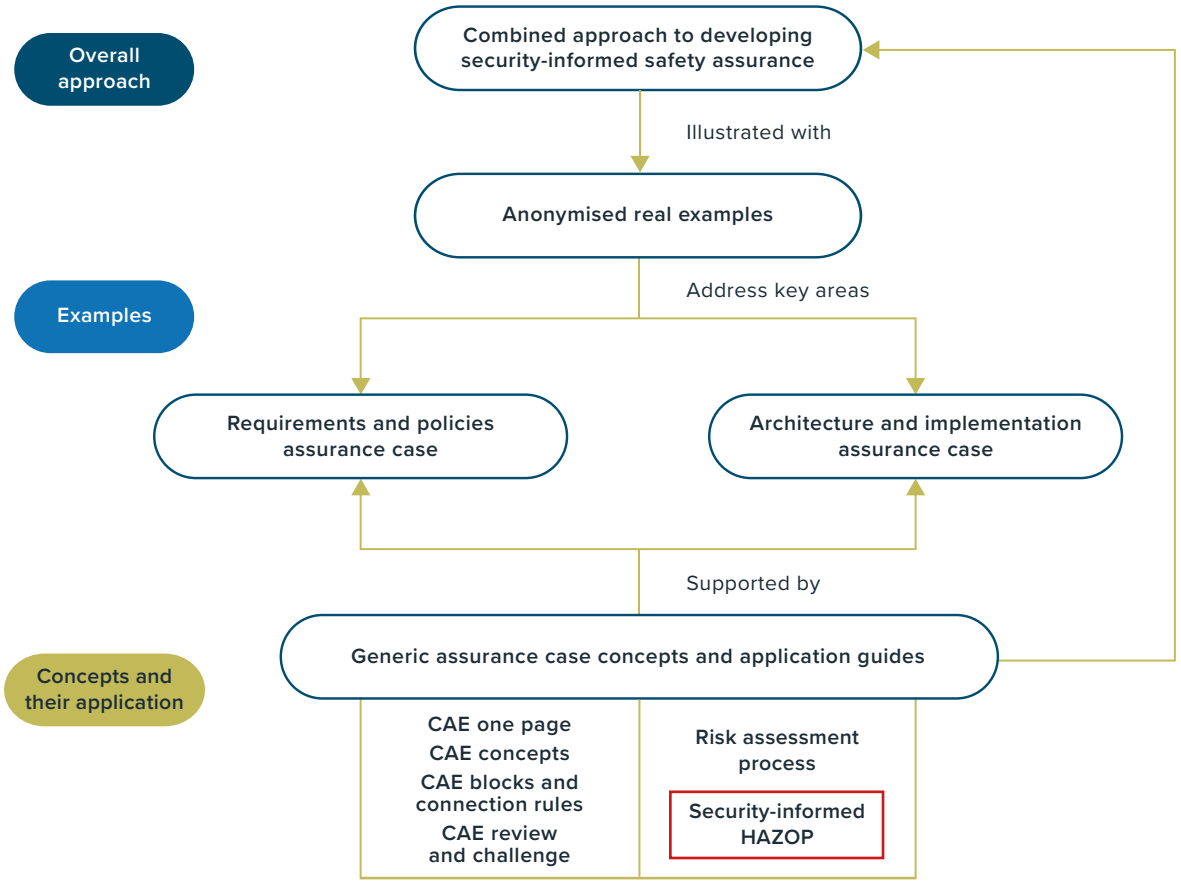

Figure 1: Location of this guide in the set of resources

[1] NCSC. Introducing component-driven and system-driven risk assessments, Version 1.0, December 2017

03. GUIDANCE

3.1 OVERVIEW

The cyber-security risk assessment methodology[2] set out in this document is a synthesis of the approaches used in conventional (non-malign) hazard analysis used in industry[3] (where the systems are generally composed of multiple elements) and those used in information assurance[4] (where consideration is given to malign actions instigated by threat sources). The methodology used in the standard information assurance approach has a defined series of steps which are set out Table 1 below.

Step 1 – Establish system context and scope of assessment	Step 8 – Report
Step 2 – Configure risk assessment	
Step 3 – Analyse policy interactions	
Step 4 – Preliminary risk analysis	
Step 5 – Identify specific attack scenarios	
Step 6 – Focused risk analysis	
Step 7 – Finalise risk assessment	

Table 1: Steps of the cyber-security risk assessment process

However, there are some significant differences between this approach and the one contained in this document, as summarised below.

- The approach to threat assessment (Step 2) is different. Without access to intelligence data, it is not possible to assess the actual threat, but it is still useful to identify potential threat scenarios in order to ensure that the risk assessment is focused on the kinds of threats that are of concern.
- Similarly, when it comes to prioritising risk (Step 6), it is not possible judge the likelihood of an attack from a particular threat source without access to intelligence data, but the capabilities and level of access to the system that a threat agent would need in order to launch a successful attack can be assessed. Thus, the attack scenarios can be ranked according to required capabilities and potential impact rather than likelihood and impact.
- In Step 4 an architecture-based approach is used (similar to a conventional hazard analysis[5] or failure modes and effects analysis[6]) where cyber attacks on individual subsystems and the impact of loss of integrity and availability of the subsystem on the overall service are considered.
- In Step 6, the resilience of the system to such service failures has to be taken into account when assessing the consequential impact.

The steps are summarised in Table 2.

[2] Adelard. Cyber Security Risk Assessment Methodology Comparison, Adelard, 2014
[3] HSE. Five steps to risk assessment, http://www.hse.gov.uk/risk/fivesteps.htm
[4] CESG. Information Assurance Standard No 1 and 2 Supplement, Technical Risk Assessment and Risk Treatment, Issue 1.0, April 2012, https://en.wikipedia.org/wiki/HMG_Infosec_Standard_No.1
[5] IEC61882:2002 Hazard and operability studies (HAZOP studies) - Application Guide, 2002
[6] ESA. Failure Modes, Effects and Criticality Analysis (FMECA). D. European Space Agency. ECSS–Q–30–02A, 1991

3.1 OVERVIEW (CONTINUED)

Step	Brief description
Step 1 – Establish system context and scope of assessment	Describe the system to be assessed and its relationship with other systems and the environment. Identify the services provided by the system and the system assets. Agree the scope of and motivation for the assessment and identify the stakeholders and their communication needs. Identify the type of decisions being supported by the assessment.
Step 2 – Configure risk assessment	Identify any existing analyses, e.g. safety cases, or business continuity assessments that provide details of the system, the impact of failure and the mitigations that are in place. Define the threat sources and identify potential threat scenarios. Refine generic capability and impact levels for the systems being assessed. Identify risk criteria. Characterise the maturity of the systems or project, the key uncertainties, and overall.
Step 3 – Refine and focus system models	Refine and focus system models in the light of the threat scenarios to ensure that they are at the right level of detail for an effective risk analysis.
Step 4 – Preliminary risk analysis	Undertake architecture-based risk analysis, identifying potential hazards and consequences and relevant vulnerabilities and causes, together with any intrinsic mitigations and controls. Consider doubts and uncertainties, data and evidence needs. Identify intrinsic and engineered defence in depth and resilience.
Step 5 – Identify specific attack scenarios	Refine preliminary risk analysis to identify specific attack scenarios. Focus on large consequence events and differences with respect to the existing system.
Step 6 – Focused risk analysis	Prioritise attack scenarios according to the capabilities required and the potential consequences of the attack. As with the previous step, the focus is on large consequence events and differences with respect to the existing system.
Step 7 – Finalise risk assessment	Finalise risk assessment by reviewing implications and options arising from focused risk analysis. Review defence in depth and undertake sensitivity and uncertainty analysis. Consider whether the design threat assumptions are appropriate. Identify additional mitigations and controls.
Step 8 – Report results	Report the results of the risk assessment to stakeholders at the appropriate level of detail.

Table 2: Cyber security assessment process summary

These steps are described in more detail in Section 3.5.

3.2 IMPACT ASSESSMENT

The impact of a successful attack on the transport system is assessed using the criticality scale shown in Table 3.

Criticality Scale	Loss of service	Loss of life
Cat 5 (Catastrophic)	Loss of or major disruption to transport system nationally (£10s of billions in economic impact)	Massive loss of life and/or casualties (1,000+ fatalities, 10,000s of casualties)
Cat 4 (Severe)	Loss of or major disruption to transport system regionally long-term (i.e. over a week) or nationally short-term (£billions in economic impact)	Severe loss of life and/or casualties (101-1,000 fatalities, 1,000s of casualties)
Cat 3 (Substantial)	Loss of or major disruption to transport system regionally short-term or sub-regionally long-term (£100s millions in economic impact)	Substantial loss of life and/or casualties (51-100 fatalities, 100s of casualties)
Cat 2 (Significant)	Loss of or major disruption to transport system sub-regionally short-term or localised long-term (£10s millions in economic impact)	Significant loss of life and/or casualties (10-50 fatalities, 10s of casualties)
Cat 1 (Moderate)	Short-term localised loss of transport system (£ millions in economic impact)	Moderate loss of life and/or casualties (<10 fatalities, <10 casualties)

Table 3: Impact levels for service failures

3.3 CAPABILITY OF THREAT SOURCES

The risk assessment should attempt to estimate the capabilities that an attacker would need in order to achieve a high impact failure. Without access to intelligence data, it is not possible to assess the actual threat, but it is still useful to identify potential threat scenarios in order to ensure that the risk assessment is focused on the kinds of threats that are of concern.

Critical National Infrastructure (CNI) could be subject to attack from a number of different sources. These threat sources can be categorised as follows:

- nation states, where the attacks might be part of a cyber war;
- terrorists, as an alternative to or in combination with conventional terror attacks;
- activists, who want to create disruption (but probably not death) to create publicity for their cause;
- hackers, who may simply be curious to know what they can compromise or control, or value exposing system vulnerabilities in order to seek system improvements and recognition for this expertise;
- criminals, who wish to gain financially (e.g. via blackmail threats to avoid attacks, or halting vehicles for robbery);
- disaffected employees, who may want to cause chaos but probably not death;
- malware authors, whose software could infect critical systems.

Threat sources who might only be interested in stealing information have been excluded as the focus of this guidance is on the integrity and safety of system and loss of confidentiality is only a major concern for some very specific attacks (e.g. in a transport system, attacks on high value passengers or hazardous and high-value cargoes).

The range of capability levels of potential threat sources has been adapted from HMG Information Assurance Standards 1 and 2 (see Table 4).

Capability Level	Description in IS1-2	Modification for CNI systems
E	Where the threat source is extremely capable and well-resourced, i.e. can: • devote several man years to penetrating the system or service • develop bespoke attacks • coordinate information about targeted systems or services from several sources • cultivate insiders for long-term attacks • deploy large amounts of equipment • co-ordinate attacks using several threat actors Typically a well-resourced foreign intelligence service.	Use tools specific to the domain including customisation of these for the attacks and to develop novel equipment and tools specific to the attack. Use publicly available and proprietary information on how system works and mitigations. Develop large testbeds and trials for the attack. Coordinate timing of several attacks. Influence expert insiders.

Table 4: Capability levels of potential threat sources

[7] CESG. HMG Information Assurance Standard No 1 and 2 Supplement, Technical Risk Assessment and Risk Treatment, Issue 1.0, April 2012, https://en.wikipedia.org/wiki/HMG_Infosec_Standard_No.1

3.3 CAPABILITY OF THREAT SOURCES (CONTINUED)

Capability level	Description in IS1-2	Modification for CNI systems
D	When the threat source is capable and has significant resources, i.e. can: • devote several man-weeks to penetrating a system or service • use all publicly available attack tools • influence insiders for specific attacks • deploy modest amounts of equipment Typically a moderately well-resourced foreign intelligence service or a well-organised terrorist or criminal group.	Use tools specific to the domain including customisation of these for the attacks. Have access to equipment for trials and attack development. Use publicly available and proprietary information on how system works and mitigations. Influence knowledgeable insiders. Have expertise in security engineering.
C	Where the threat source has modest capabilities and resources, i.e. can: • devote a few man-days to penetrating system or service • use well-known publicly available attack tools • deploy small amounts of equipment Typically smaller organised terrorist or criminal group, or competent individual hacker.	Use tools specific to the domain but without customisation. Use publicly available information on how system works and mitigations. Understanding of security engineering. Influence insiders (but at routine skill level).
B	Where the threat source has very modest capabilities and resources, i.e. can: • devote a few man-days to penetrating a system or service • deploy a very small amount of equipment Typically an average Internet user.	An engineer with possible access to equipment but no specific training or authority in how to use, i.e. plug maintenance console into equipment. Some physical access to system. A typical enterprise IT user.
A	Where the threat source has almost no capabilities or resources, i.e. can: • use simple 'plug and play' devices and removable media • devote a few man-hours to penetrating system or service Typically a computer or Internet novice.	Accidental participants, i.e. from compromised machines/devices. Could be co-opted into scaling denial of service-type attacks.

Table 4: Capability levels of potential threat sources

Evaluation of the likely attack frequencies and capabilities of specific threat sources are outside the assessment scope and should be undertaken by the intelligence services.

3.4 POLICY INTERACTIONS

A range of issues that concern the interaction of safety requirements and security policies that need to be addressed are set out in Table 5 below. Some of these can be resolved at an early stage in a project but others will set policies and constraints that shape the development of the case at the architecture and implementation levels.

Policy issue	Activities
Scope of system, safety case and safety-related functionality.	Assess whether system boundary is drawn sufficiently wide e.g. to include sources of attack, connected systems. Assess whether we need additional confidentiality claims, e.g. 'System does not leak information that leads to unacceptable increase in risk of successful attack' or 'System protects confidentiality of assets that have direct information value'. Assess the role of the system/service in enabling other systems to be secure – good cyber citizenship. Consider an explicit claim about resilience to emphasise the need for adaptation and recovery in an uncertain world. This will require interactions with the other system owners and their policy setters.
Risk, responsibility and regulation.	Add explicit threat models and scenarios to environment description. Define capability levels of attackers and design basis threats. Introduce policy on design basis threats, not just in operational environment but in development infrastructure, organisation and supply chain. Make risk and safety statement conditional on these assumptions, discuss with regulators and overall duty holders. Agree how to demonstrate that the risks are as low as reasonably practicable (ALARP) with respect to security-initiated events. This may be problematic. Recognise that a duty-holder cannot outsource risk to a cyber department or through SLAs (although specialist advice will be needed). The holder still has a responsibility to understand safety hazards and mitigations. Augment competency scheme. Augment handling of information policy. Map claims and evidence to the organisations responsible for them.
Dealing with events and incidents.	Extend the safety case argument to include security-related events. Include a claim about handling these events in both preventative and reactive manner (e.g. incident response). Review with respect to different time bands. Ensure the approach and environmental assumptions are documented in the system design basis document. Review impact of architecture, design and deployment. Asset management and identification of vulnerable components/systems.

Table 5: Policy issues to be addressed

Policy issue	Activities
Obsolescence, lifetime and refurbishment.	Obsolescence, lifetime and refurbishment policy in light of weakening security controls with age. Assess impact of obsolescence on architecture.
Defence in depth.	Address independence and diversity for the system configuration and related activities. Training policy needs to address security. Any constraints on L1 (design) and L2 (organisation) need to be identified.

Table 5: Policy issues to be addressed – continued

A range of design and implementation policies may to some extent be defined at a requirements stage (see Table 6) but will require detailing and implementing at later stages of the project.

Design and implementation policies
Policy on which sets of 'critical controls' should be considered or mandated.
Policy on application of Kerckhoff's principles and 20 controls. [8]
Policy on applicable standards and guidance.
Policy on interpreting defence in depth in architecture.
Policy on robustness design and testing.
Policy on supply chain assurance and impact on design and architecture.
Policy on identifying security vulnerabilities in code. May impact use of third-party software and supply chain relationships and need for access to source code.
Policy on built-in security.
Policy that cryptographic aspects need to be assessed by national experts, e.g. NCSC.
Information assurance policy that addresses trustworthy safety case evidence and any trade-offs between openness and confidentiality.

Table 6: Design and implementation policies

[8] Center for Internet Security. Critical Security Controls for Effective Cyber Defense,. v7.1, 2019

3.4 STEPS IN MORE DETAIL

3.5.1 Step 1 – Establish system context and scope of assessment

Step 1	Establish system context and scope of the assessment
Objectives	Describe the system to be assessed and its relationship with other systems and the environment. Identify the services provided by the system and system assets. Agree the scope of and motivation for the assessment and identify the stakeholders and their communication needs. Identify any existing analyses, e.g. safety cases.
Input	Requires input from stakeholders, for example: • system architecture • organisation and responsibility diagrams • any existing risk or safety assessments.
Output	• description of system architecture, relationships with other systems, initial set of system models, etc. • list of services and assets • agreed scope of assessment • safety cases and other existing analyses
Approach	Establish system and context: • What are the socio-tech systems and services? • What are the confidentiality, integrity, availability (CIA) requirements? • What level of assurance does the existing system have? • Identify initial interdependencies and assumptions based on assets, components, functionality, use, environment Scope of assessment: • Who are the customers for the risk assessment? • What are their expectations and motivations? • What format should the risk assessment take? • Are there any standards / guidelines that should be followed? • Is there any standard terminology that should be used?

3.5.2 Step 2 – Configure risk assessment

Identify any existing analyses, e.g. safety cases, business continuity assessments that provide details of the system, the impact of failure and the mitigations that are in place. Characterise the maturity of the systems or project and the key uncertainties.

Define the threat sources and identify potential threat scenarios. Refine generic capability and impact levels for the systems being assessed. Identify risk criteria.

Refine and focus system models in the light of the threat scenarios and existing analyses to ensure that they are at the right level of detail for an effective security-informed risk analysis.

3.5.2.1 Identify any existing analyses

Step 2.1	**Identify existing analyses**
Objectives	Define the threat sources and identify potential threat scenarios.
Input	Existing analyses, e.g. safety cases, business continuity assessments that provide details of the system, the impact of failure and the mitigations that are in place.
Output	Summary of available information and bibliography.
Approach	• identify existing analyses. • characterise the maturity of the systems or project and the key uncertainties.

3.5.2.2 Identify potential threats

Step 2.2	Identify potential threats
Objectives	Ensure that the risk assessment is focused on the kinds of threats that are of concern. Define possible threat sources and identify potential threat scenarios. Refine generic capability and impact levels for the systems being assessed. Identify risk criteria.
Input	Briefing from Government agencies to focus assessment. Use of: • catalogue of potential threat sources and taxonomies • guidewords for threat actor types, levels of system access, etc. • intelligence assessments (if available)
Output	Statement on focus of risk assessment in terms of threat sources and capabilities. Depending on criticality of system and the threat level, this may include a list of threat scenarios, consisting of threat sources, target / objective and threat level
Approach	• identify threat sources and potential targets (threat scenarios) • classify the threat sources according to their capabilities and priorities • classify the scenarios with respect to the level of threat and the perceived risk of attack

3.5.2.3 Refine and focus system models

Step 2.3	Refine and focus system models
Objectives	Refine and focus system models in the light of the threat scenarios to ensure that they are at the right level of detail for an effective risk analysis.
Input	• threat scenarios • initial set of system models – architecture diagrams, information flow and stakeholder roles • generic briefing note on Hazop – see ‘Security-informed Hazop’
Output	Refined set of system models. Specific briefing note for architecture analysis advised in ‘Security-informed Hazop’.
Approach	• define focuses of interest, architecture and environment models • abstract/refine architecture, combine/distinguish assets

3.5.3 Step 3 – Analyse policy interactions

Step 3	**Analyse policy interactions**
Objectives	Undertake an analysis of policy issues considering interactions between safety requirements and security policies. Resolve any conflicts, show that the trade-offs are satisfactory and document the decisions made.
Input	• the information obtained from Step 2 on the system the safety requirements and security policies and any supporting analyses • the policy interaction tables
Output	Report on analysis and trade-offs that are considered. Escalate to stakeholders as necessary.
Approach	Address the policy issues as described in the **Table 5** and consider: • scope of system, safety case and safety-related functionality • risk, responsibility and regulation • dealing with events and incidents • obsolescence, lifetime and refurbishment • defence in depth Identify design and implementation policies based on **Table 6**.

3.5.4 Preliminary risk analysis

Step 4	**Preliminary risk analysis**
Objectives	Undertake architecture-based risk analysis, identifying consequences and relevant vulnerabilities and causes together with any intrinsic mitigations and controls. Consider doubts and uncertainties, data and evidence needs. Identify intrinsic and engineered defence in depth and resilience.
Input	System model
Output	Preliminary risk analysis, identifying: • relevant potential vulnerabilities, and their consequences • initial means of compromising the system • intrinsic mitigations and controls

3.5.4 Preliminary risk analysis

Step 4	Preliminary risk analysis
Objectives	Undertake architecture-based risk analysis, identifying consequences and relevant vulnerabilities and causes together with any intrinsic mitigations and controls. Consider doubts and uncertainties, data and evidence needs. Identify intrinsic and engineered defence in depth and resilience.
Input	System model
Output	Preliminary risk analysis, identifying: • relevant potential vulnerabilities, and their consequences • initial means of compromising the system • intrinsic mitigations and controls
Approach	• Use architectural risk analysis to identify relevant vulnerabilities and their consequences (and any intrinsic mitigations and controls): ○ Modified interface Hazop, trust relations analysis and vulnerability analysis. ○ Assess vulnerability and initial compromise route of trust relationships between system components (and any intrinsic mitigations and controls). ○ Assess interdependencies (both for consequences, recovery and also causes). Consider asset aggregation and cascade failures or other multipliers. • Consider ambiguity analysis – are there any aspects of the system specification that are unclear or open to interpretation? • Consider choice of implementation technology – are there any implementation-defined choices that might affect the security of the system?

3.5.5 Step 5 – Identify specific attack

Step 5	Identify specific attack scenarios
Objectives	Refine preliminary risk analysis to identify specific attack scenarios. Focus on large consequence events and differences with respect to existing system.
Input	• preliminary risk analysis • system models • threat scenarios

3.5.5 Step 5 – Identify specific attack

Step 5	**Identify specific attack scenarios**
Output	List of attack scenarios, consisting of: • description of plausible compromise and consequence • step-by-step account of how compromise is achieved • analysis of potential mitigations • assessment of level of access required, technical difficulty etc

Approach	• Refine preliminary risk analysis to identify specific attack scenarios. Focus on large consequence events and differences to existing system
	• Start with the list of relevant vulnerabilities and initial compromise routes identified in Step 4
	• Work backwards from compromise to attack
	• Describe the attack in detail (who, what, how, where, when)
	• Identify the path from threat actor to compromise to consequence:
	  ○ What vulnerabilities does the attack exploit?
	  ○ What mitigations and controls need to be overcome?
	  ○ How could the attack be prevented?
	• Classify the scenario:
	  ○ Technical difficulty
	  ○ Level of access required
	  ○ Type of failure
	  ○ Scale and scalability
	  ○ Impact (including recovery, resilience)
	  ○ Mitigation strategies (costs?)

3.5.6 Step 6 – Focused risk analysis scenarios

Step 6	**Focused risk analysis**
Objectives	Prioritise attack scenarios according to the capabilities required and the potential consequences of the attack. As with Step 5, the focus is on large consequence events and differences with respect to existing system.

3.5.6 Step 6 – Focused risk analysis

Step 6	Focused risk analysis
Input	Attack scenarios.
Output	• prioritised list of risks • worst case credible consequences and associated threat actor capabilities
Approach	• focus on large consequence events and identify increased risks / threats relative to the existing system • assess worst-case credible threats using scenarios • undertake comparative risk assessments with respect to existing system (consider whole risk profile to see how changed) • assess impact of interdependencies, particularly in terms of consequence and recovery

3.5.7 Step 7 – Finalise risk assessment

Step 7	Finalise risk assessment
Objectives	Finalise risk assessment by reviewing implications and options arising from focused risk analysis. Review defence in depth and undertake sensitivity and uncertainty analysis. Consider whether the design threat assumptions are appropriate. Identify additional mitigations and controls.
Input	Prioritised list of risks
Output	Final risk assessment.
Approach	• undertake sensitivity and uncertainty analysis (to architecture, mitigations, assumptions, abstractions) • review defence in depth features for systemic risks • consider whether design basis threats are still appropriate in the light of the risk analysis • identify additional mitigations and controls • review implications of findings, trade-offs and overall messages

03. GUIDANCE

3.5.8 Step 8 – Report results

Step 8	Report results
Objectives	Report the results of the risk assessment to stakeholders at the appropriate level of detail for each stakeholder.
Input	• final risk assessment • stakeholder needs from Step 1
Output	A series of reports, presentations, executive summaries.
Approach	• structure reports and presentations according to the needs and expectations of stakeholders identified in Step 1 • use different levels of detail for different stakeholders as appropriate • use capability/impact diagrams to illustrate risks and inform stakeholders

04. ACKNOWLEDGEMENTS

This document is based on material developed in earlier projects partially funded by the UK Control and Instrumentation Nuclear Industry Forum (CINIF) and guidance from previous CPNI projects and published research by Adelard.

Disclaimer

This guide has been prepared by CPNI and is intended to support the implementation of security-informed safety assurance and the Claims, Arguments and Evidence (CAE) methodology. This document is provided on an information basis only, and whilst CPNI has used all reasonable care in producing it, CPNI provides no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, CPNI accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the [report]. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

No Endorsement

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

CPNI
Centre for the Protection of National Infrastructure