Project Management view of Network and Information Security CAF Compliance Implementation in the Energy Sector

PROJECT MANAGEMENT VIEW

4 Step Approach to Managing CAF Project ..

1	2	3	4

Understand Regulatory Requirements

Identify applicable legal and regulatory frameworks (e.g., UK NIS Regulations for Operators of Essential Services).

Align CAF implementation with industry-specific security standards (e.g., ISO 27001, NIST CSF, IEC 62443 for industrial control systems).

STEP 1 | 2 | 3 | 4

Risk Assessment

Identify critical assets (e.g., SCADA systems, OT/IT infrastructure).

Map out threat vectors (e.g., ransomware, nation-state attacks, insider threats).

Perform a CAF-based self-assessment to gauge current cyber resilience levels.

What good looks like?

(a) Managing Security Risk

✓ security governance
✓ security policies
✓ supply chain security assessments.

(b) Protecting Against Cyber Attacks

✓ separating IT & OT networks
✓ MFA for critical systems
✓ patch & update ICS / Operational Technology OT

(c) Detecting Cyber Security Events

✓ SIEM solutions
✓ OT-specific intrusion detection systems (IDS)
✓ penetration testing and red teaming exercises

(d) Minimising the Impact of Incidents

✓ OT Cyber Incident Response Plan
✓ backup & disaster recovery plans
✓ incident response drills

Continuous Compliance & Improvement

✓ Regularly audit and assess cyber resilience against CAF guidelines.

✓ Engage with NCSC & industry cybersecurity forums for best practices.

✓ Foster a cyber-aware culture through employee training and simulations.

PROJECT MANAGEMENT

Initiating Project

- **Identify system or service**: Determine which systems and application are supporting Operational Assets / Critical Services
- **Key assets**: List critical assets like databases, IT assets, ERP, PLC, SCADA

Output:
Project Charter / PID
Stakeholder Register,
Scope Statement

Scoping

Identifying critical systems

Documenting critical system

Prioritising critical system

Sharing your scoping workbook with your independent assurer for feedback

Profile

Baseline or Enhanced?

- By default, the Baseline profile is most commonly applied.
- Enhanced profile applies to CNI systems and where there may be factors that make the system a higher threat target for attack.

Project Planning

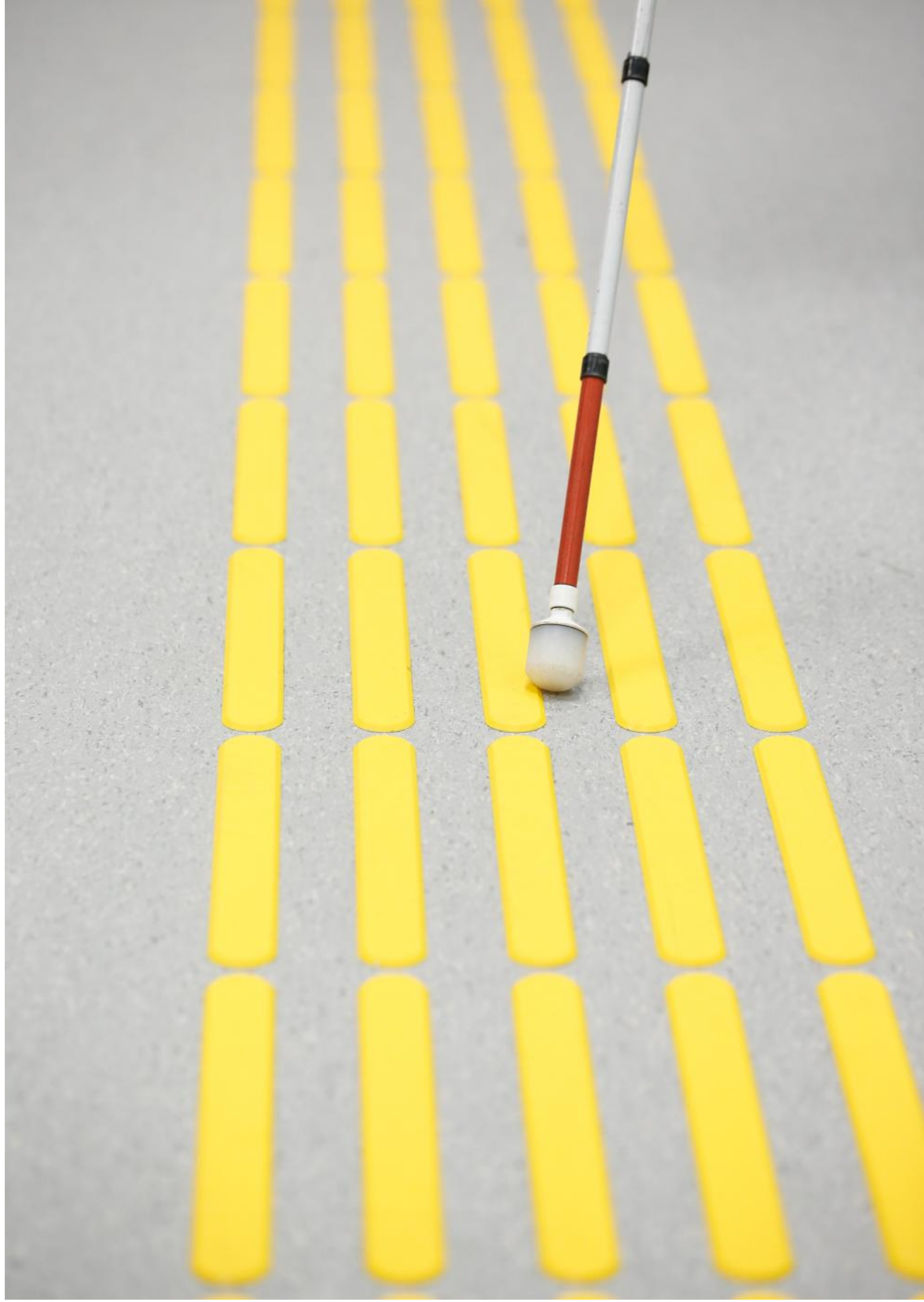
- **Scope**: Determine the systems, processes, and assets to be included in the assessment.
- **Stakeholders**: Identify key stakeholders and their roles in the assessment.
- **Resources**: Allocate necessary resources, tools, and personnel.
- **Timeline**: Develop a timeline with key milestones, deadlines, and deliverables.

Output:
Update PID
Risk Assessment Plan
Detailed Project Plan
Resource Plan
Communication Plan
Risk Management Plan (Project)
Change Management Plan

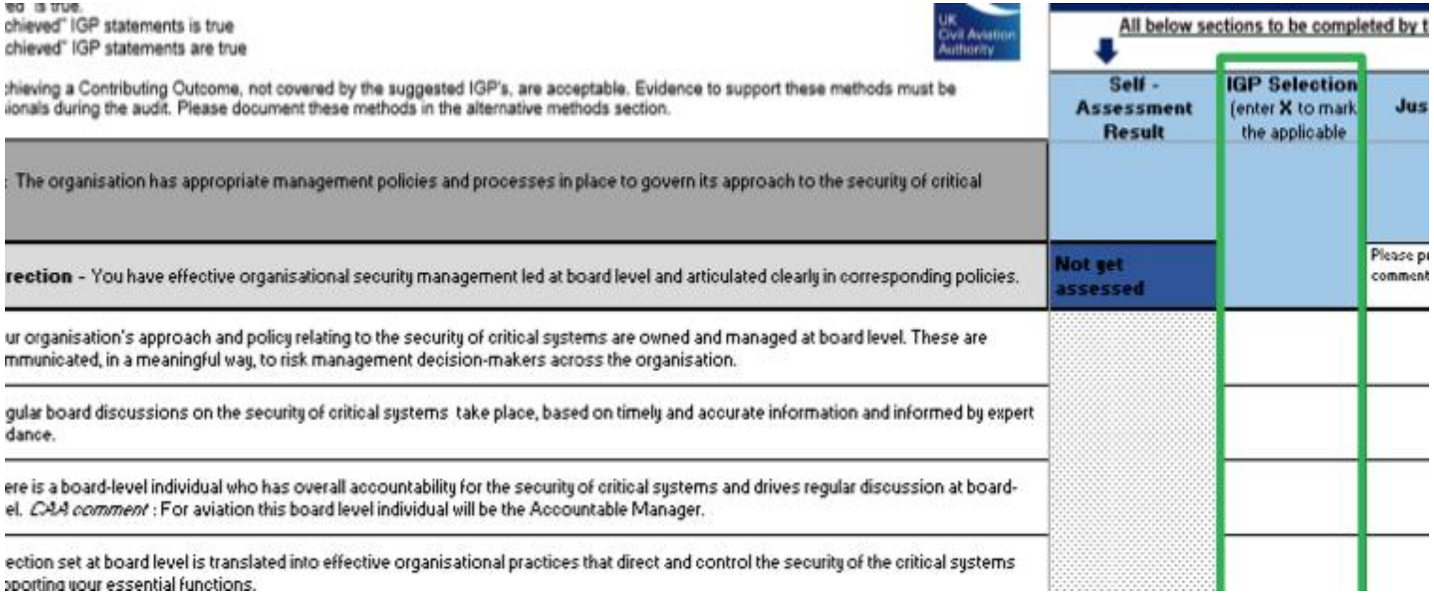
Indicators of Good Practice (IOGP)

Three categories of IGPs:

- **Achieved** – these show the typical characteristics of an organisation that has fully achieved an outcome
- **Partially achieved** – these show the typical characteristics of an organisation partially achieving an outcome
- **Not achieved** – these show the typical characteristics of an organisation that has not achieved an outcome



Risk Assessment Tools



ed" is true.
chieved" IGP statements is true
chieved" IGP statements are true

hieving a Contributing Outcome, not covered by the suggested IGP's, are acceptable. Evidence to support these methods must be
ionals during the audit. Please document these methods in the alternative methods section.

All below sections to be completed by t

	Self - Assessment Result	IGP Selection (enter **X** to mark the applicable	Jus
: The organisation has appropriate management policies and processes in place to govern its approach to the security of critical			
rection - You have effective organisational security management led at board level and articulated clearly in corresponding policies.	**Not yet assessed**		Please p comment
ur organisation's approach and policy relating to the security of critical systems are owned and managed at board level. These are mmunicated, in a meaningful way, to risk management decision-makers across the organisation.			
gular board discussions on the security of critical systems take place, based on timely and accurate information and informed by expert dance.			
ere is a board-level individual who has overall accountability for the security of critical systems and drives regular discussion at board-el. *CAA comment* : For aviation this board level individual will be the Accountable Manager.			
ection set at board level is translated into effective organisational practices that direct and control the security of the critical systems pporting your essential functions.			

Output:
Vulnerability Assessment
Data Protection Impact Assessments (DPIA)
Risk Assessment Report

Execution (Work Packages)

- Review the system or service to be assessed, focusing on critical assets, processes, and their security posture.
- Update IOGP
- Document the findings, including recommendations for mitigating identified risks.

Risk Assessor Site/WP 1

Risk Assessor Site/WP 2

Risk Assessor Site/WP 3

Site Manager

Principle Engineer

SCADA Operator

Physical Security

Telecoms

Output from Risk Assessment

Corrective Actions

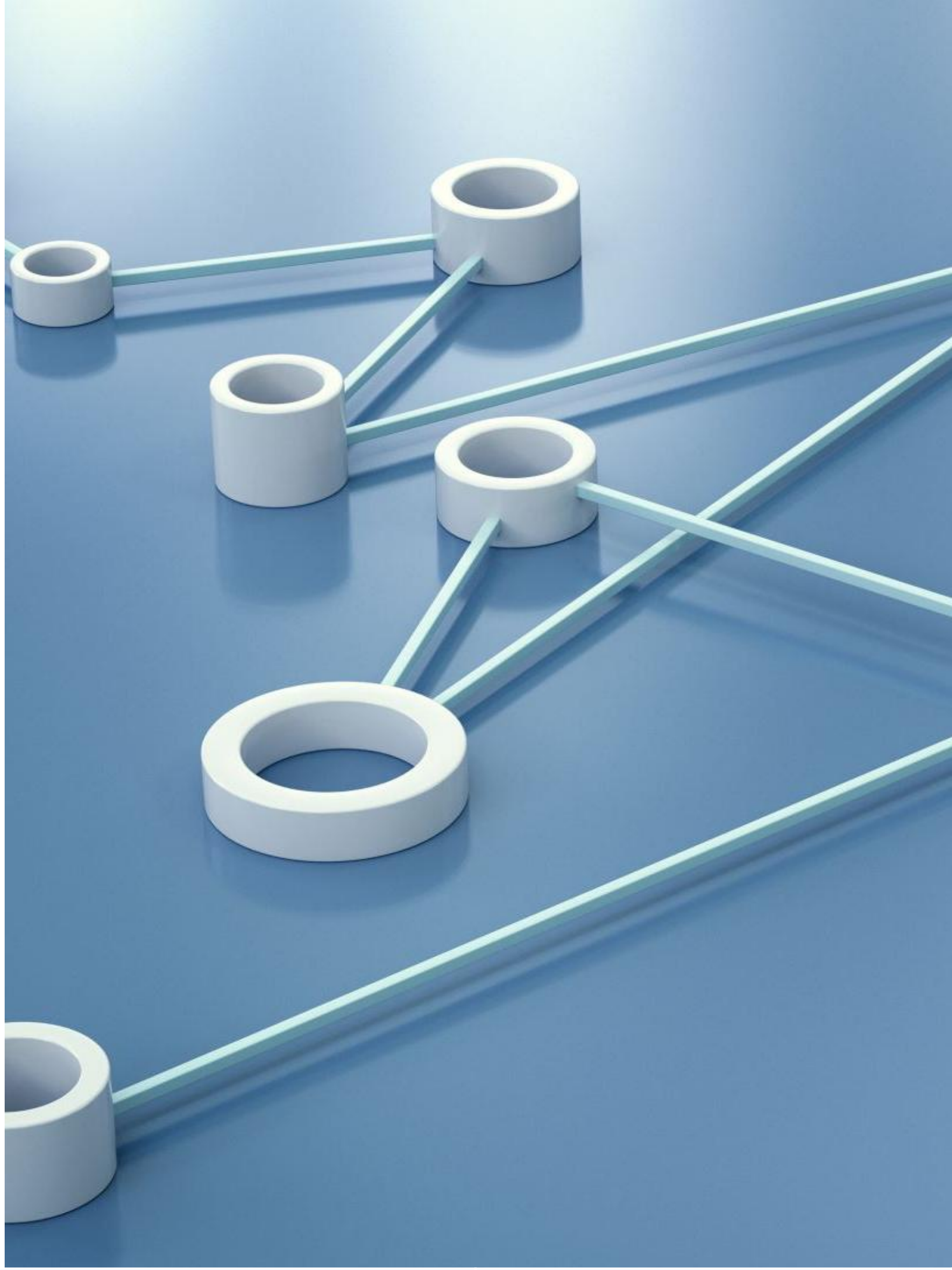
Build Processes, Standards

Build Policies

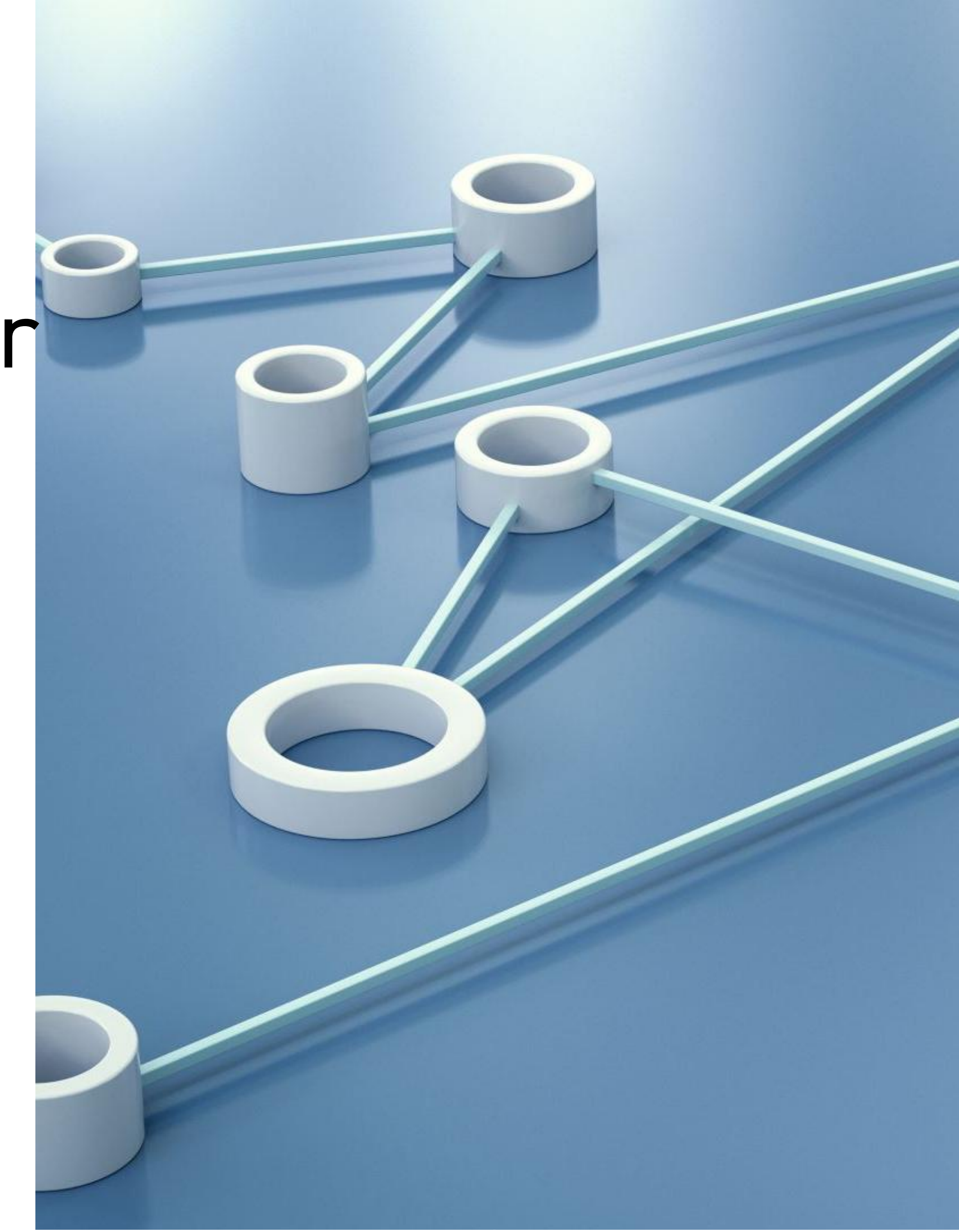
Supplier Evidence

New Responsibilities

New Projects!



Change Management Register



Change recommendation to meet IOGP – (Extract from Assessments)

- Convert each recommendation into a SMART objective (Specific, Measurable, Achievable, Relevant, Time-bound)
- Develop a Project Roadmap - Break down the initiative into phases (e.g., Assessment, Design, Implementation, Testing, Adoption)
- Identify executive sponsors and project leads
- Determine required skills and resources
- Establish key performance indicators (KPIs) to track compliance with IGPs
- Ensure Business Adoption & Continuous Improvement

Monitoring and Controlling

- Track Progress: Regularly monitor project milestones, timelines, and resources to ensure the assessment is on track.
- Identify and Address Issues: Proactively identify any risks or challenges and address them to prevent project delays.
- Adjust the Plan: Revise the assessment scope or resources if needed to stay aligned with objectives.
- Stakeholder Updates: Provide periodic updates to stakeholders on progress, findings, and adjustments.

- ✓ Progress Reports
- ✓ Key Performance Indicators (KPIs)
- ✓ Incident Response Records
- ✓ Management of Change

Closing Project

- ✓ Review the original project scope and ensure all deliverables (e.g., risk reports, mitigation plans, security assessments) have been completed.
- ✓ Ensure that mitigation actions have been successfully implemented and that any residual risks are documented and acknowledged by stakeholders.
- ✓ Obtain stakeholder sign-off on project deliverables and closure, ensuring they accept any residual risks.
- ✓ Document successes, challenges, and any issues that impacted the risk assessment and mitigation efforts.
- ✓ Mark the project as complete in the project management system (e.g., MS Project, Jira, etc.)
- ✓ Transition plan for handing over responsibilities, such as continuous risk monitoring, to the operational team.

Conclusion

Importance of Project Management

Effective project management is crucial for ensuring compliance with network and information security standards in the energy sector.

Protecting Sensitive Information

Protecting sensitive information is essential for maintaining trust and security within the energy sector's infrastructure.

Enhancing Cybersecurity Posture

Adopting best practices and addressing challenges helps organizations in the energy sector to enhance their cybersecurity posture.