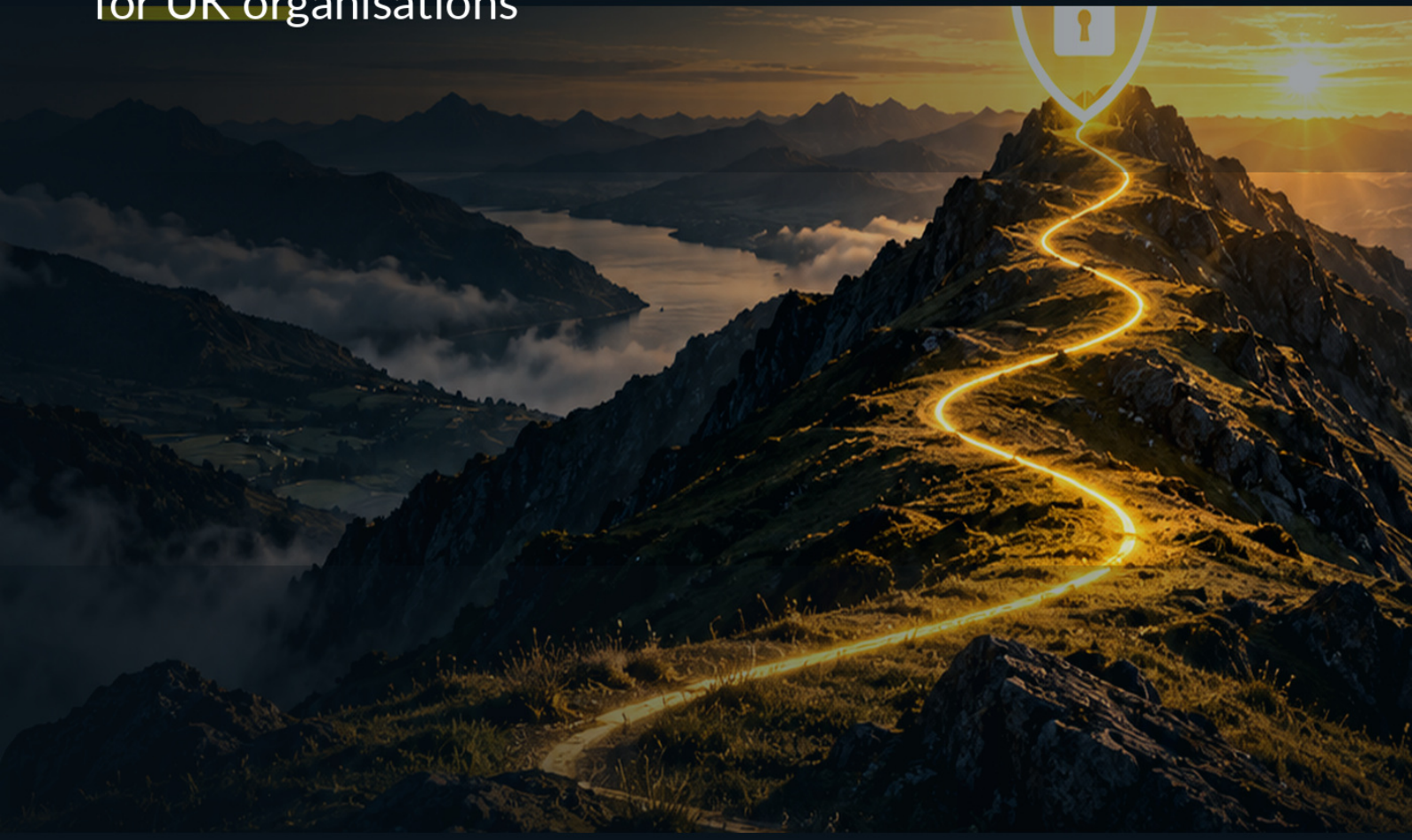
Cyber Karl Ltd

Helping you defend what matters.

NCSC CAF v4.0 IMPLEMENTATION GUIDE

A practical guide to cyber resilience for UK organisations



04	14	41	6D
Objectives	Principles	Outcomes	ProofGate™

Practical guidance. Real-world support. Lasting impact.

WELCOME / USING THE PACK

Resilience that stands up to scrutiny

Protect the services people depend on, demonstrate how cyber risks are managed and invest in the improvements that matter.

The NCSC Cyber Assessment Framework (CAF) is designed to help organisations assess and improve resilience of their **essential functions**. It is particularly relevant to critical national infrastructure, regulated essential services, public sector operations and other organisations with significant service dependencies.

> **Read this first**
> The CAF is **not** a general-purpose certification scheme, and there is no universal NCSC "pass score". Any sector-specific target CAF profile or regulatory interpretation must be confirmed with the relevant oversight body.

Inside this resource pack

- **Guide:** understand the four objectives, 14 principles and practical activities.
- **Assessment workbook:** review all 41 official CAF v4.0 contributing outcomes and record your judgement.
- **Evidence catalogue:** connect conclusions to documents, operational records and assurance results.
- **Improvement plan:** allocate accountable leads and priorities, and track progress.

What good looks like

Good resilience is not a folder full of policies. It is an organisation that knows which functions matter, understands what could disrupt them, implements the right safeguards, can spot adverse activity and can recover when things go wrong.

CONTENTS

Your route through the guide

PART	FOCUS
01	CAF explained: scope, profiles and assessment judgements
02	The four objectives and 14 principles
03	One-page implementation guidance for every principle
04	ProofGate™ 6D applied to CAF
05	Evidence and essential-function asset management
06	Running the assessment and using the workbook
07	A practical first-90-days plan
08	Customer checklists, worked example and references

Approach
Start by defining an **essential function** and its service boundary. A broad assessment of “all of IT” without considering service impact risks missing the most important systems and dependencies.

01 / ORIENTATION

Understanding CAF v4.0

The CAF expresses security and resilience as **outcomes**. It asks whether arrangements work in practice, not just whether a document or tool exists.

4 OBJECTIVES	14 PRINCIPLES	41 OUTCOMES
Manage risk / Protect / Detect / Respond	Outcomes grouped under A1–A4, B1–B6, C1–C2, D1–D2	Contributing outcomes assessed using NCSC Indicators of Good Practice

The hierarchy

- **Objective:** broad capability such as managing security risk.
- **Principle:** a more specific resilience goal, such as asset management.
- **Contributing outcome:** an assessable aspect of that principle, such as A3.a.
- **Indicators of Good Practice (IGPs):** examples that inform expert judgement. They are not an exhaustive mechanical checklist.

Assessment results

For each outcome, assess **Achieved**, **Partially Achieved** (where supported by the relevant official IGP table), or **Not Achieved**. A justified **Not Applicable** outcome may be appropriate within the agreed assessment scope or target profile. The workbook provides these statuses, but the assessor must refer to the official IGP table.

> **Avoid false precision**
> The workbook uses status counts to show review progress, not a numerical CAF certification score. Recording evidence and sound reasoning is more important than producing a percentage.

01 / SCOPE

Start with essential functions

Examples include delivering patient care, operating a transport service, maintaining water treatment or providing a critical public service. Scope is defined by the function, its unacceptable outcomes and the systems and people it depends on.

Five practical scoping questions

- Which services or activities are essential, and who depends on them?
- What disruption, data compromise or safety consequence would be unacceptable?
- Which business processes and IT/OT systems deliver these functions?
- Which people, suppliers, utilities, facilities and data are dependencies?
- Who is responsible for the function and who has authority to accept risk?

Outputs to agree

DELIVERABLE	WHAT TO RECORD
Essential-function register	Function, service lead, stakeholders, service boundary and impact.
Dependency map	People, applications, devices, OT, networks, facilities and suppliers.
Risk assumptions	Threat scenarios, failure modes, business impact and risk appetite.
Target profile	Applicable CAF outcomes and required target outcomes, as defined by the appropriate authority.

02 / OBJECTIVE A

Managing Security Risk

Understand and govern the risks to critical services.

PRINCIPLE	BUSINESS PURPOSE
A1 Governance	Clarify board accountability, decision-making and reporting for the security of essential functions.
A2 Risk Management	Understand how threats and weaknesses could interrupt important services; choose and assure proportionate treatments.
A3 Asset Management	Know the information, technology, people and dependencies needed to deliver essential functions.
A4 Supply Chain	Manage supplier dependencies and software assurance throughout the service lifecycle.

Management question
Can you demonstrate, using current operational evidence, that the relevant cyber risks to your essential functions are being managed?

02 / OBJECTIVE B

Protecting Against Cyber Attack

Put proportionate security controls into daily operations.

PRINCIPLE	BUSINESS PURPOSE
B1 Service Protection Policies, Processes and Procedures	Set understandable security rules and demonstrate that people actually follow them.
B2 Identity and Access Control	Verify identities, trust devices, restrict privileges and regularly review access.
B3 Data Security	Know important information and protect it in storage, transit, mobility and disposal.
B4 System Security	Build, configure, manage and maintain secure technology supporting essential functions.
B5 Resilient Networks and Systems	Plan recovery, design for failure and protect the backups needed to restore services.
B6 Staff Awareness and Training	Develop a culture in which people understand risk, report concerns and have the skills for their roles.

Management question
Can you demonstrate, using current operational evidence, that the relevant cyber risks to your essential functions are being managed?

02 / OBJECTIVE C

Detecting Cyber Security Events

Identify adverse activity early enough to act.

PRINCIPLE	BUSINESS PURPOSE
C1 Security Monitoring	Collect trustworthy logs, recognise attacks and respond to alerts effectively.
C2 Threat Hunting	Proactively look for adverse activity missed by routine controls and detection rules.

Management question
Can you demonstrate, using current operational evidence, that the relevant cyber risks to your essential functions are being managed?

02 / OBJECTIVE D

Minimising the Impact of Cyber Security Incidents

Respond, recover and improve after disruption.

PRINCIPLE	BUSINESS PURPOSE
D1 Response and Recovery Planning	Plan, resource, test and operate a response that protects or restores essential functions.
D2 Lessons Learned	Investigate causes of incidents, then make and verify improvements.

Management question
Can you demonstrate, using current operational evidence, that the relevant cyber risks to your essential functions are being managed?

03 / PRINCIPLE A1

A1 Governance

Clarify board accountability, decision-making and reporting for the security of essential functions.

What leaders should be able to demonstrate

A named executive sponsor, agreed responsibilities and reporting that helps leaders make risk decisions.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
A1.a **Board Direction**	Is security of essential functions directed and challenged at board level?	Board minutes, accountable executive, decision log, reports
A1.b **Roles and Responsibilities**	Are security roles agreed, resourced and understood?	RACI, role descriptions, appointment records, escalation chart
A1.c **Decision-making**	Are cyber risk decisions made by authorised people within agreed appetite?	Risk appetite, delegated authorities, acceptance records

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE A2

A2 Risk Management

Understand how threats and weaknesses could interrupt important services; choose and assure proportionate treatments.

What leaders should be able to demonstrate

Evidence of active risk decisions that take account of changing threats and operational impact.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
A2.a **Risk Management Process**	Are risks to essential functions regularly assessed and treated?	Risk method, service risk register, treatment decisions
A2.b **Understanding Threat**	Are relevant actors, techniques and plausible attacks understood?	Threat scenarios, intelligence sources, threat modelling
A2.c **Assurance**	Is control effectiveness tested and weaknesses resolved?	Assurance schedule, test reports, remediation evidence

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE A3

A3 Asset Management

Know the information, technology, people and dependencies needed to deliver essential functions.

What leaders should be able to demonstrate

A trustworthy inventory and dependencies, including OT, cloud and infrastructure services where relevant.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
A3.a **Asset Management**	Are essential assets, dependencies and owners known and maintained?	Asset and dependency inventory, review trail, data map

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE A4

A4 Supply Chain

Manage supplier dependencies and software assurance throughout the service lifecycle.

What leaders should be able to demonstrate

Critical supplier visibility, contractual duties and ongoing review of important dependencies.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
A4.a **Supply Chain**	Are critical suppliers and downstream dependencies appropriately assured?	Supplier register, risk tiering, contract and review evidence
A4.b **Secure Software Development and Support**	Is developed or purchased software supported and securely maintained?	Supplier SSDLC assurance, SBOM where appropriate, support terms

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE B1

B1 Service Protection Policies, Processes and Procedures

Set understandable security rules and demonstrate that people actually follow them.

What leaders should be able to demonstrate

Approved, communicated policies backed by actual operating records.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
B1.a **Policy, Process and Procedure Development**	Are practical security policies and procedures maintained?	Policy library, approvals, exception and revision records
B1.b **Policy, Process and Procedure Implementation**	Can the organisation demonstrate that procedures operate effectively?	Operational sampling, attestation, non-compliance actions

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE B2

B2 Identity and Access Control

Verify identities, trust devices, restrict privileges and regularly review access.

What leaders should be able to demonstrate

Access records that match genuine business need, including service accounts and contractors.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
B2.a **Identity Verification, Authentication and Authorisation**	Are users and systems appropriately verified and granted access?	Identity procedures, MFA configuration, access requests
B2.b **Device Management**	Are connecting devices known, trusted and appropriately controlled?	MDM inventory, compliance reports, third-party device rules
B2.c **Privileged User Management**	Are elevated rights limited, separated, monitored and reviewed?	PAM logs, admin inventory, privileged-access reviews
B2.d **Identity and Access Management (IdAM)**	Are joiners, movers, leavers and access rights governed?	JML tickets, access recertification, revoke evidence

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE B3

B3 Data Security

Know important information and protect it in storage, transit, mobility and disposal.

What leaders should be able to demonstrate

Data ownership, flow maps, technical protection and safe disposal records.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
B3.a **Understanding Data**	Are critical data, owners, flows and impact understood?	Data inventory, criticality classification, flow diagrams
B3.b **Data in Transit**	Are critical data transfers appropriately controlled and protected?	Network flows, TLS/VPN settings, transfer agreements
B3.c **Stored Data**	Are critical data and backups suitably protected against loss and change?	Encryption records, backup tests, access restrictions
B3.d **Mobile Data**	Is critical data controlled and protected on mobile devices?	Mobile policy, endpoint inventory, encryption and wipe tests
B3.e **Media / Equipment Sanitisation**	Are assets reliably sanitised prior to reuse or disposal?	Disposal certificates, erasure logs, chain of custody

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE B4

B4 System Security

Build, configure, manage and maintain secure technology supporting essential functions.

What leaders should be able to demonstrate

Secure system designs, configuration baselines, technical administration and vulnerability remediation.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
B4.a **Secure by Design**	Is security designed into systems and does one weakness avoid causing disproportionate impact?	Design reviews, segmentation and threat models
B4.b **Secure Configuration**	Are hardened configurations documented and checked?	Baselines, configuration monitoring, exceptions
B4.c **Secure Management**	Are systems administered and supported in a controlled manner?	Admin access records, platform diagrams, malware monitoring
B4.d **Vulnerability Management**	Are vulnerabilities discovered, prioritised and resolved with assurance?	Scan coverage, remediation SLAs, validation reports

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE B5

B5 Resilient Networks and Systems

Plan recovery, design for failure and protect the backups needed to restore services.

What leaders should be able to demonstrate

Recovery dependencies, resilient design decisions and tested restoration evidence.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
B5.a **Resilience Preparation**	Can necessary systems and dependencies be recovered in the right order?	Business impact analysis, recovery plans, exercise results
B5.b **Design for Resilience**	Are single points of failure and resource limits appropriately mitigated?	Resilience diagrams, redundancy tests, dependency review
B5.c **Backups**	Are backups secure, current, usable and regularly tested?	Restore logs, backup coverage and immutable copy evidence

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE B6

B6 Staff Awareness and Training

Develop a culture in which people understand risk, report concerns and have the skills for their roles.

What leaders should be able to demonstrate

Role-based awareness, training, exercise and culture improvement evidence.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
B6.a **Cyber Security Culture**	Can staff raise concerns and contribute to security without blame?	Culture surveys, campaigns, staff feedback, reporting trends
B6.b **Cyber Security Training**	Do staff and specialists receive relevant training?	Role-based plan, training records, skills assessments

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE C1

C1 Security Monitoring

Collect trustworthy logs, recognise attacks and respond to alerts effectively.

What leaders should be able to demonstrate

Relevant log coverage, monitored detection rules, triage, staff capability and threat-informed tuning.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
C1.a **Sources and Tools for Logging and Monitoring**	Do monitoring inputs cover important systems and attacks?	Logging catalogue, source coverage, SIEM use cases
C1.b **Securing Logs**	Are monitoring records protected and retained appropriately?	Log access controls, immutability, retention settings
C1.c **Generating Alerts**	Do monitoring rules detect relevant suspicious activity reliably?	Detection rule library, alert test and tuning evidence
C1.d **Triage of Security Alerts**	Are alerts investigated promptly using service and threat context?	Alert queue, runbooks, case sampling, escalation records
C1.e **Personnel Skills for Monitoring and Detection**	Do internal or outsourced analysts have the needed expertise?	SOC role matrix, skill records, supplier assurance
C1.f **Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)**	Are behaviour patterns and intelligence used to strengthen detection?	Threat-intelligence feeds, behaviour baselines, detection reviews

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?

- What risks or overdue actions require a management decision?

03 / PRINCIPLE C2

C2 Threat Hunting

Proactively look for adverse activity missed by routine controls and detection rules.

What leaders should be able to demonstrate

Structured hunts, hypotheses, results, learning and coverage improvements.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
C2.a **Threat Hunting**	Are proactive hunts planned, conducted, recorded and improved?	Hunt backlog, hypotheses, reports, improvement actions

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE D1

D1 Response and Recovery Planning

Plan, resource, test and operate a response that protects or restores essential functions.

What leaders should be able to demonstrate

Actionable response plans, decision authorities, communications and exercise results.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
D1.a **Response Plan**	Is an up-to-date incident response plan tied to essential functions?	Approved response plan, contacts, scenarios, decision triggers
D1.b **Response and Recovery Capability**	Can teams execute plans and sustain critical operations during incidents?	Call-out records, exercises, specialist support, recovery tests
D1.c **Testing and Exercising**	Are realistic incidents regularly rehearsed and lessons recorded?	Tabletop schedule, exercise reports, actions

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

03 / PRINCIPLE D2

D2 Lessons Learned

Investigate causes of incidents, then make and verify improvements.

What leaders should be able to demonstrate

Blameless analysis, tracked remediation and evidence that changes worked.

Contributing outcomes and practical evidence

CAF REF / OUTCOME	ASSESSMENT FOCUS	EXAMPLE EVIDENCE
D2.a **Post Incident Analysis**	Are root causes and contributing factors investigated thoroughly?	Post-incident review, timeline, root cause analysis
D2.b **Using Incidents to Drive Improvements**	Are lessons turned into completed, verified improvements?	Improvement log, owner sign-off, retest evidence

Practical first step
Ask the service owner and relevant technical leads to walk through how this works in practice. Check one recent decision, example transaction, test or incident record rather than relying on policy statements.

Management review prompts

- What would a failure of this area mean for an essential function?
- Who leads and who provides independent challenge?
- Which evidence demonstrates operation and effectiveness?
- What risks or overdue actions require a management decision?

04 / CYBERKARL METHOD

ProofGate™ 6D applied to CAF

Our six-stage delivery method makes the assessment actionable. The CAF outcomes and relevant regulator profile remain the assessment basis; ProofGate™ is CyberKarl's implementation approach.

STAGE	PRACTICAL CUSTOMER OUTPUT
Discover	Confirm essential functions, service owners, dependencies, relevant CAF profile and evidence already available.
Define	Agree risk appetite, assessment scope, target outcomes, control leads and a proportionate improvement plan.
Design	Design necessary governance, technical controls, detection, resilience and assurance activities.
Deliver	Implement changes, collect operating evidence, train teams and carry out the baseline assessment.
Defend	Monitor performance, retest effectiveness, exercise incidents and periodically reassess outcomes.
Decommission	Securely retire systems, suppliers and access no longer needed; retain required records and update dependencies.

The relationship
ProofGate™ 6D is the **delivery method**. CAF v4.0 is the **assessment framework**. Your target profile and any binding obligations are determined by the appropriate oversight body, not by CyberKarl.

05 / EVIDENCE

Evidence that stands up to scrutiny

Evidence should be relevant, current, attributable and sufficient to support the assessment judgement. A policy without operational proof rarely tells the whole story.

A four-part evidence test

- **Ownership:** who approves, operates and reviews the relevant activity?
- **Operation:** when did it last happen, and what does a real sample show?
- **Effectiveness:** how do you know the activity reduces risk to the essential function?
- **Improvement:** what happens when a weakness or change is identified?

Suggested evidence categories

CATEGORY	ILLUSTRATIVE RECORDS
Direction and risk	Board reporting, risk appetite, risk register, decisions
Asset and suppliers	Service dependency maps, supplier assurance, contractual obligations
Protective measures	Access approvals, secure baselines, vulnerability remediation, recovery tests
Detection and response	Logging coverage, investigation casework, incident exercises
Learning	Post-incident reviews, verified remediation and management review

Handling sensitive evidence

An assessment register should point to secure evidence, not duplicate sensitive network designs, passwords or incident details inside a widely distributed spreadsheet. Record a link or reference and apply appropriate access restrictions.

06 / USING THE WORKBOOK

Run a defensible 41-outcome assessment

- **1. Define the assessment:** confirm scope, function(s), applicable profile and assessment lead.
- **2. Assign leads:** identify the responsible technical or business lead for each outcome.
- **3. Review official IGPs:** consult the relevant NCSC CAF v4.0 table, noting partial-achievement applicability.
- **4. Capture evidence:** record evidence IDs and links plus what they demonstrate.
- **5. Record a justified judgement:** select one of the four tracking statuses and record rationale or scope justification.
- **6. Act on gaps:** create prioritised actions and identify independent assurance or regulator review where needed.

Status meanings
Achieved = supporting evidence meets the outcome; **Partially Achieved** = meaningful benefits are evidenced and the official table allows that result; **Not Achieved** = relevant outcome is not adequately met; **Not Applicable** = permitted and justified by the assessment scope/profile. Leave **Not assessed** until reviewed.

What the dashboard shows

The workbook dashboard displays how many outcomes have been assessed, results by status and outstanding improvement actions. These are internal management indicators, not the NCSC's certification or regulatory result.

07 / ACTION PLAN

Your first 90 days

A realistic starting programme assumes that scope and leadership need to be agreed before detailed technical work begins. Adapt the pace to service complexity, operational technology constraints and regulator requirements.

PERIOD	ACTIVITY	OUTPUT
Days 1–15	Confirm essential functions, sponsors, dependencies and baseline risks.	Signed scope, owners, assumptions
Days 16–30	Review the 41 outcomes against official NCSC IGPs and gather evidence.	Evidence-backed baseline
Days 31–60	Prioritise high-consequence gaps; design controls and assign accountable leads.	Risk-approved delivery plan
Days 61–90	Deliver priority improvements; exercise critical processes and report progress.	Tested changes, management pack

Prioritise based on consequence

- Impact to essential functions and recovery ability.
- Plausibility and capability of threats and exploit paths.
- Dependencies, single points of failure and existing safeguards.
- Regulatory targets, contractual expectations and feasibility.

First meeting agenda
Agree the essential function; name the accountable sponsor; choose a function owner and control leads; confirm the external oversight position; authorise a 30-day baseline assessment.

08 / WORKED EXAMPLE

From a finding to a decision

Illustrative scenario: a transport operator relies on a cloud scheduling platform and a specialist communications provider. A service outage could significantly affect passengers.

STEP	EXAMPLE
Essential function	Passenger service coordination
Risk identified	Loss of scheduling platform or supplier connectivity
CAF outcomes	A3.a (assets), A4.a (supply chain), B5.b (resilience), D1.b (response capability)
Evidence reviewed	Service dependency map; supplier SLA; failover test; response exercise
Finding	Supplier dependency recorded, but alternate communications arrangement not exercised
Assessment outcome	Expert assessor judges relevant outcomes against official IGPs; supporting rationale is recorded
Improvement	Exercise the alternate process with supplier, owner and dispatch leads; record result and remediate gaps

What this teaches
A purchased technical solution does not prove resilience. Test that the right people can keep the service operating when a real dependency fails.

08 / PRE-ASSESSMENT

CAF readiness questions

Use these questions to prepare interviews. They are CyberKarl prompts, not official NCSC IGPs.

- Can senior management identify the essential functions and unacceptable consequences?
- Are the supporting assets, data, people, facilities and suppliers mapped?
- Do risk reviews consider realistic adversaries, weaknesses and operational dependencies?
- Can owners show evidence that protective controls operate as intended?
- Do monitoring arrangements cover critical systems and lead to investigated alerts?
- Are threat hunting and detection improvements proportionate to the threat?
- Have response teams rehearsed credible service disruption scenarios?
- Can you show closed and verified actions from incidents, tests or assurance?
- Does each CAF outcome have a justified result, owner and accessible evidence reference?
- Has the relevant regulator or oversight body set a required target profile?

REFERENCES / ATTRIBUTION

Sources and publication notes

Primary source: NCSC Cyber Assessment Framework v4.0, published 4 August 2025, maintained by the UK National Cyber Security Centre.

Official CAF v4.0 document
NCSC CAF collection and implementation guidance

The outcome identifiers and titles are drawn from CAF v4.0. Plain-English questions, indicative evidence and implementation steps in this publication are original CyberKarl explanatory material and **must not** be treated as substitutes for the NCSC IGP tables or regulatory instructions.

Attribution: Contains public sector information derived from NCSC CAF v4.0, © Crown copyright 2025, licensed under the Open Government Licence v3.0. NCSC imagery has not been reproduced.

Document control: CK-RES-GDE-003 | Version 1.0 | Published October 2026 | Review due October 2027, or earlier if CAF or sector requirements change.

Independent publication
This is a CyberKarl Ltd guidance resource. It is not authored, sponsored, assured or endorsed by the NCSC, and its use does not demonstrate regulatory compliance or confer certification.

NEXT STEPS

Helping you defend what matters.

CyberKarl Ltd helps organisations turn cyber security frameworks into proportionate, usable governance and evidence. We can support scoped CAF baselines, risk and control design, evidence reviews, management reporting and practical improvements.

Website: cyberkarl.co.uk