Science and Technology Facilities Council

IRIS Security

IRIS Collaboration meeting, Durham, July 1st 2025

David Crooks
david.crooks@stfc.ac.uk
On behalf of the IRIS Security Team

iris

Landscape

- Broad status the same: high, persistent risk
- Considerable focus on compliance → Risk
  - Organisational focus

IRIS Security Team

- From last time:

- Focus on “professionalisation” of IRIS Security Team towards IRIS CSIRT
  - RFC 2350 + SIM3
  - Expectations for Computer Security Incident Response

- Work is ongoing, focused on RFC 2350
  - Structural elements of a CSIRT

Science and Technology Facilities Council

iris

Security Handbooks

- More recent work focuses on underpinning “security checklist” for sites, stemming from work for GridPP
  - Partly following longstanding appetite for “security baseline” from sites
  - Focus on using existing work and materials but identify key elements for our environment
  - Propose to extend this to IRIS
  - “Living document”, mature over time
  - Linked to local policies and procedures

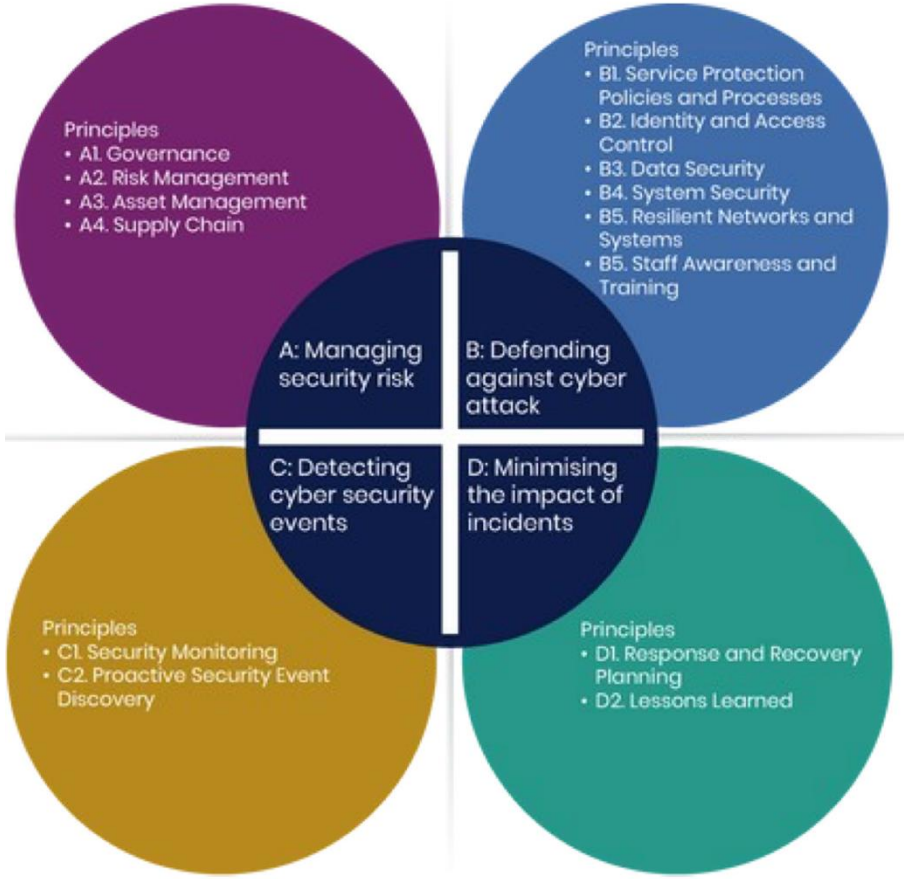
- Also an RFC for security handbooks!
  - RFC2196
  - Some obvious technology anachronisms, but useful basis

Science and Technology Facilities Council

iris

Cybersecurity reviews

- Potential for many organisations to be undergoing cybersecurity reviews at this time
- In DRI context, drive to focus on NCSC Cyber Assessment Framework (CAF) as “lingua franca”
- Which sites are undergoing such activity?

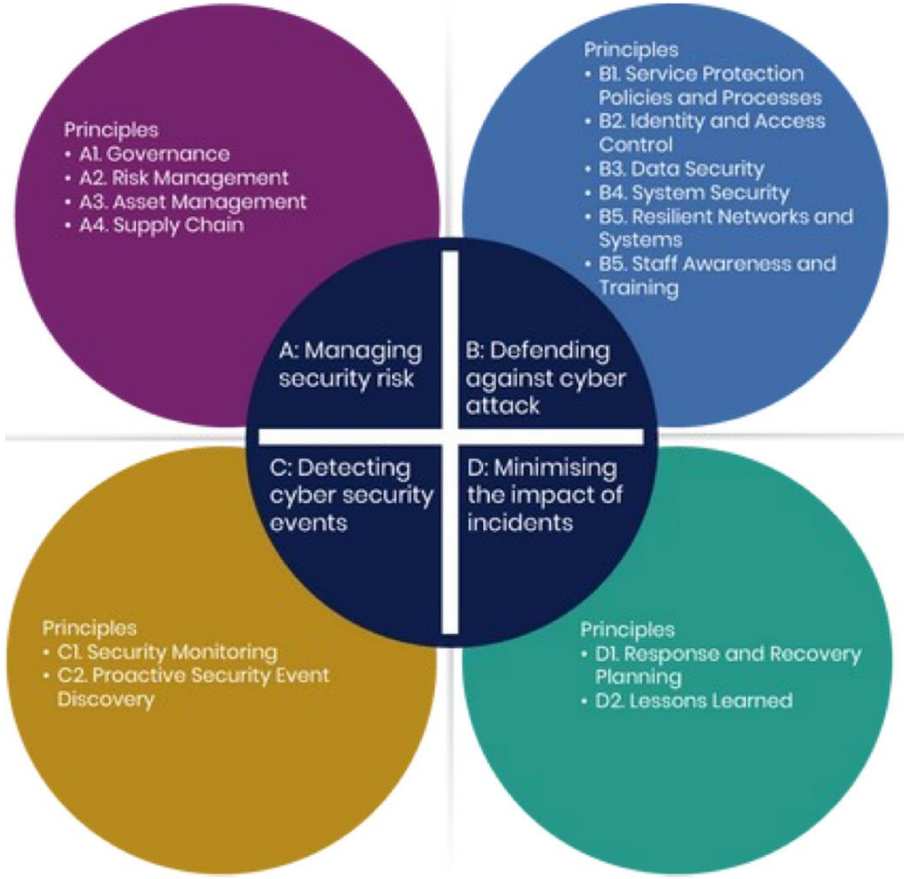


Science and Technology Facilities Council

iris

Tier1 CAF outcomes [1]

- Tier1 CAF assessment now complete, including both internal and external assessments
- One conclusion: a full assessment, with over 200 indicators of good practice, is a heavyweight process: up to months of 20%-50% FTE for assessment team

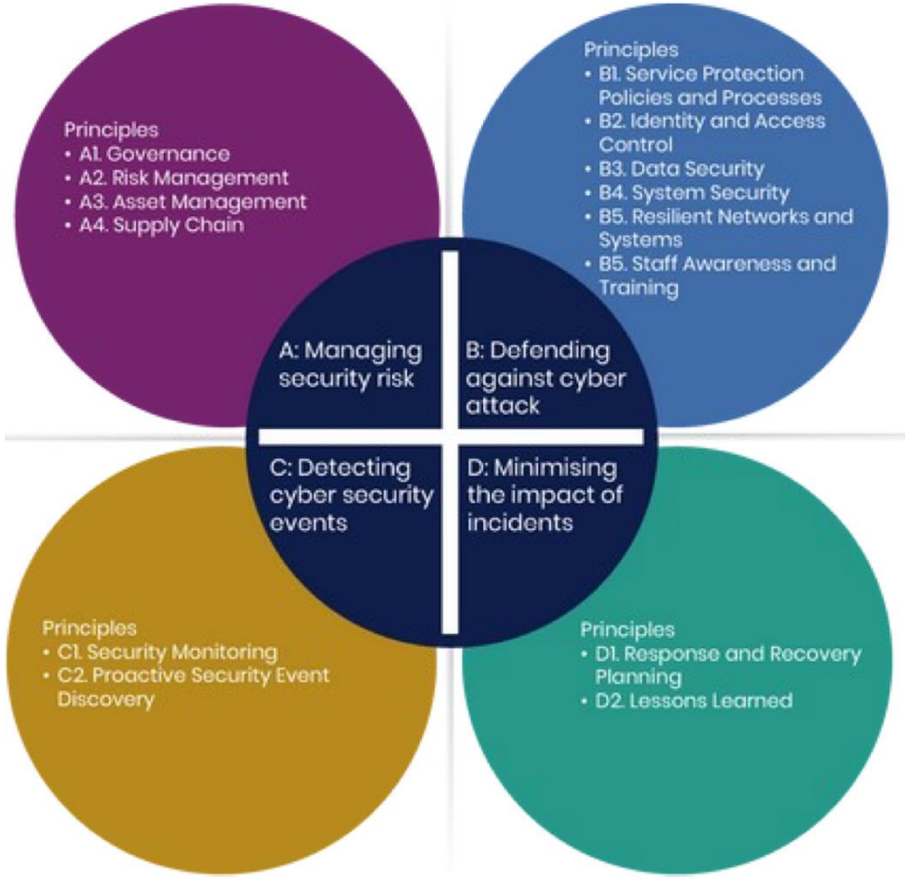


Science and Technology Facilities Council

iris

Tier1 CAF outcomes [2]

- Broad outcomes from external assessors fall into
  - Topics which may be specific to research environment
  - Specific work for Tier1
  - Work best focused at higher level



Science and Technology Facilities Council

iris

Cybersecurity Governance

- Focus on higher level
- Processes for governance, risk management and assurance
- Likely to be common thread
- Ongoing process to identify most effective approach

Cybersecurity Governance for Infrastructures

- What does this look like at an infrastructure level?
- Focus of work this summer under the aegis of DRI Cybersecurity
- Invitation for infrastructures/participating organisations to perform lightweight CAF assessment (contributing outcome level, **not** full assessment)
- Followed by in-depth workshops to dig into Objective A: Governance and Risk Management

UKRI Science and Technology Facilities Council

iris

CAF Objective A

- Governance
- Risk Management
- Asset Management + Supply Chain

- Focus on this area as everything else follows from this

- Intended outcomes from this work:
  - Understand current posture
  - Identify steps to improve
  - Continued understanding of needs in research computing context

Science and Technology Facilities Council

iris

DRI Cybersecurity Workshop

- Next DRI Cybersecurity Workshop: 17/18 July, hosted in Bristol
  - Registrations now open

  - Focus on governance, risk and policy
  - Kick-off workshop for CAF A work

- Overall DRI Cybersecurity focus on Governance, risk, and skills and training

- Build long-term planning to improve overall posture

UKRI Science and Technology Facilities Council

iris

Skills and Training

- Alongside governance and risk, for me one of the most important activities with long-term impact

- Recent experiences: Thematic CERN School on Computing (Security)
  - First run in 2022
  - Third iteration this year, April 6-12
  - Hosted by STFC at Cosener's House

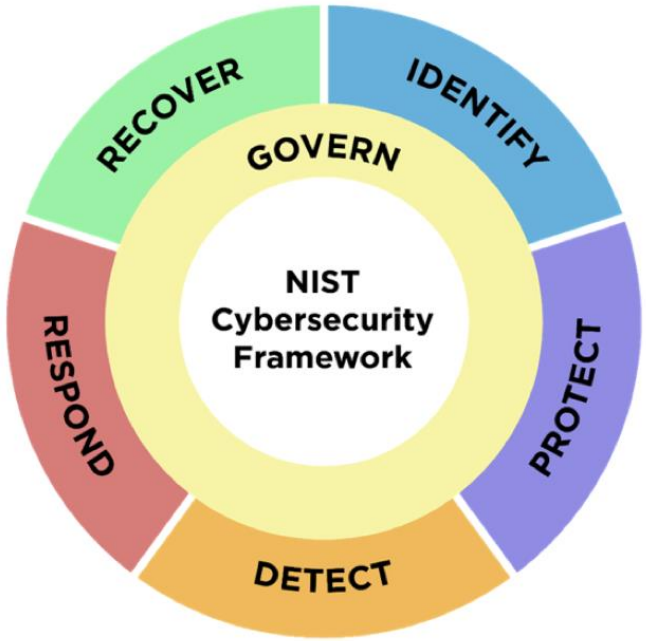
- Same structure as other thematic schools
  - 5 days, mix of lectures and exercises
  - Tutors from EGI CSIRT, CERN and STFC

CERN School on Security

- Aimed at system managers expected to work with security in their day-to-day role
  - As opposed to cybersecurity professionals – but typically have a small number of these as well
  - Cover security lifecycle of a service

Risk management
Security architecture
AAI
Logging and Traceability
Virtualisation + cloud security
Container security
Vulnerability management
Application security

Security Operations Centres
Security operations
Incident response management
Forensics
Incident response exercise



Science and Technology Facilities Council

iris

Types of training: IRIS

- In person training very effective in delivering broad curriculum
  - And team building within cohort

- Impossible to scale this
  - How do we approach this for IRIS?
  - Approaches + Identify key topics
  - Continue discussion tomorrow

- Identify additional external training

Science and Technology Facilities Council

iris

Upcoming topics: policy

- Setting a flag for the future: IRIS does have a current set of security policies: www.iris.ac.uk/security
- Clear from earlier discussions that not everyone is aware of these – but also we're approaching the point at which a review would make sense
  - See also contemporaneous work in EGI/WLCG scope + AARC TREE
- More on this soon

Science and Technology Facilities Council

iris

Upcoming topics: operational security

- Focus on monitoring across IRIS
  - Site/organisation level
  - Part of IRIS CSIRT work: what would benefit from coordinated activity
- Next SOC Hackathon: Bucharest, 15-17 September
  - Remote attendance possible
  - Identify where we could encourage additional IRIS/GridPP/DiRAC work in this area
  - Potential focus this time on growing toolset
  - Talk to David afterwards
- Software vulnerability risk assessments
  - EGI Software Vulnerability group looking at future developments
  - Very important for IRIS/DRI scopes to best understand how to contribute to this work

Summary

- In a continued high risk environment, security governance and risk management are key areas for development
- Understand impact for IRIS: engage with broader DRI activities

- Skills and training vital additional strand

UKRI Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council @STFC_Matters Science and Technology Facilities Council

Science and
Technology
Facilities Council

Questions?