Science and
Technology
Facilities Council

Scientific Computing

GridPP
UK Computing for Particle Physics

Security in GridPP7

David Crooks (he/him)
david.crooks@stfc.ac.uk

GridPP 51, March 2024, Sheffield

Outline

- Landscape for GridPP7
- Review of framework approach
- GridPP Security Strategy
- Potential strategic objectives
- DRI Cybersecurity update
- Immediate next steps

Science and Technology Facilities Council

Scientific Computing

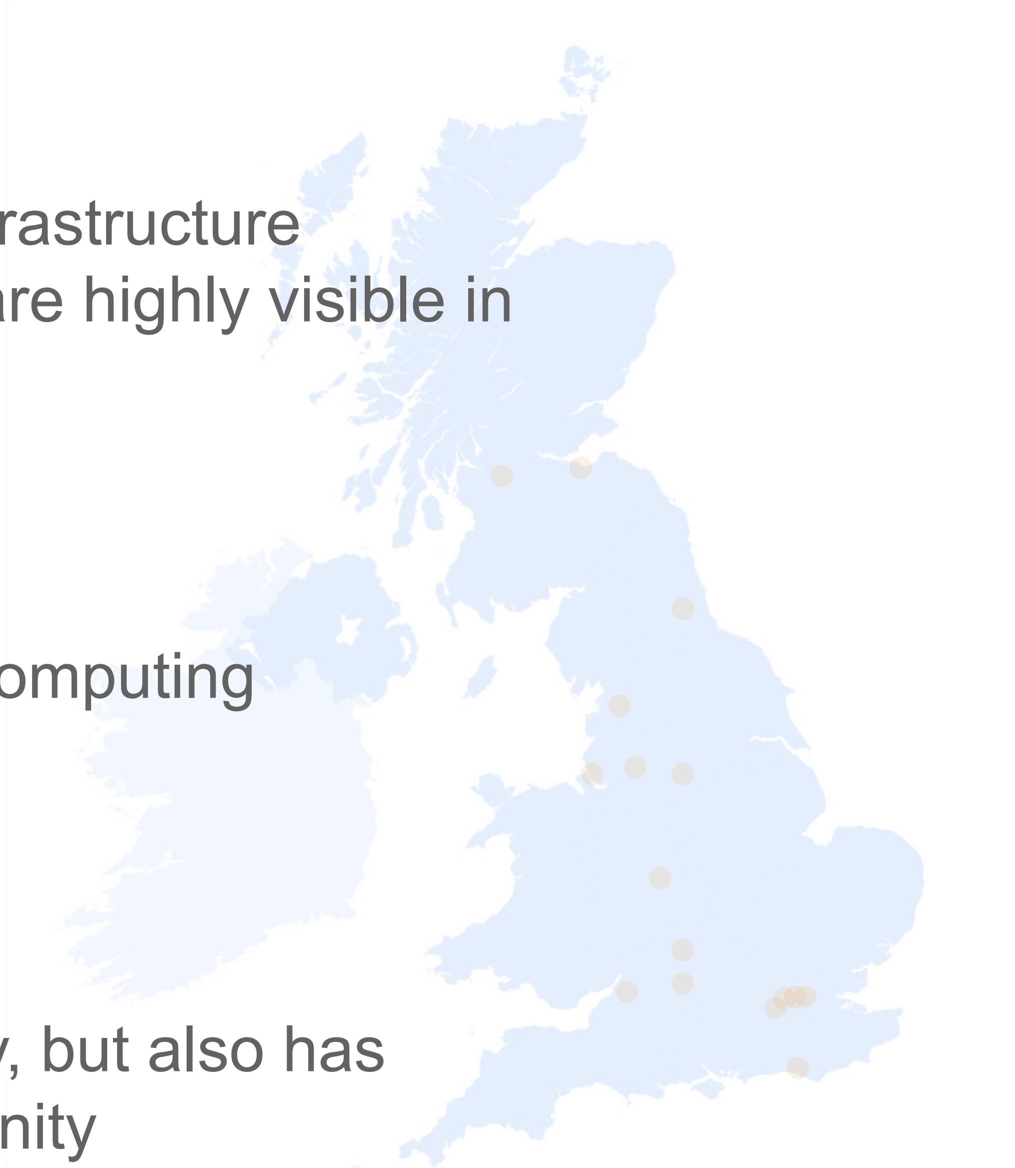
GridPP UK Computing for Particle Physics

Landscape

- The cybersecurity risk faced by GridPP as an infrastructure remains high due to the range of attacks which are highly visible in our sector
  - See recent example of the British Library

- We operate in an environment with very active computing infrastructure development
  - Future of Compute/exascale/…

- GridPP needs to ensure it works in a secure way, but also has experience it can share with the broader community

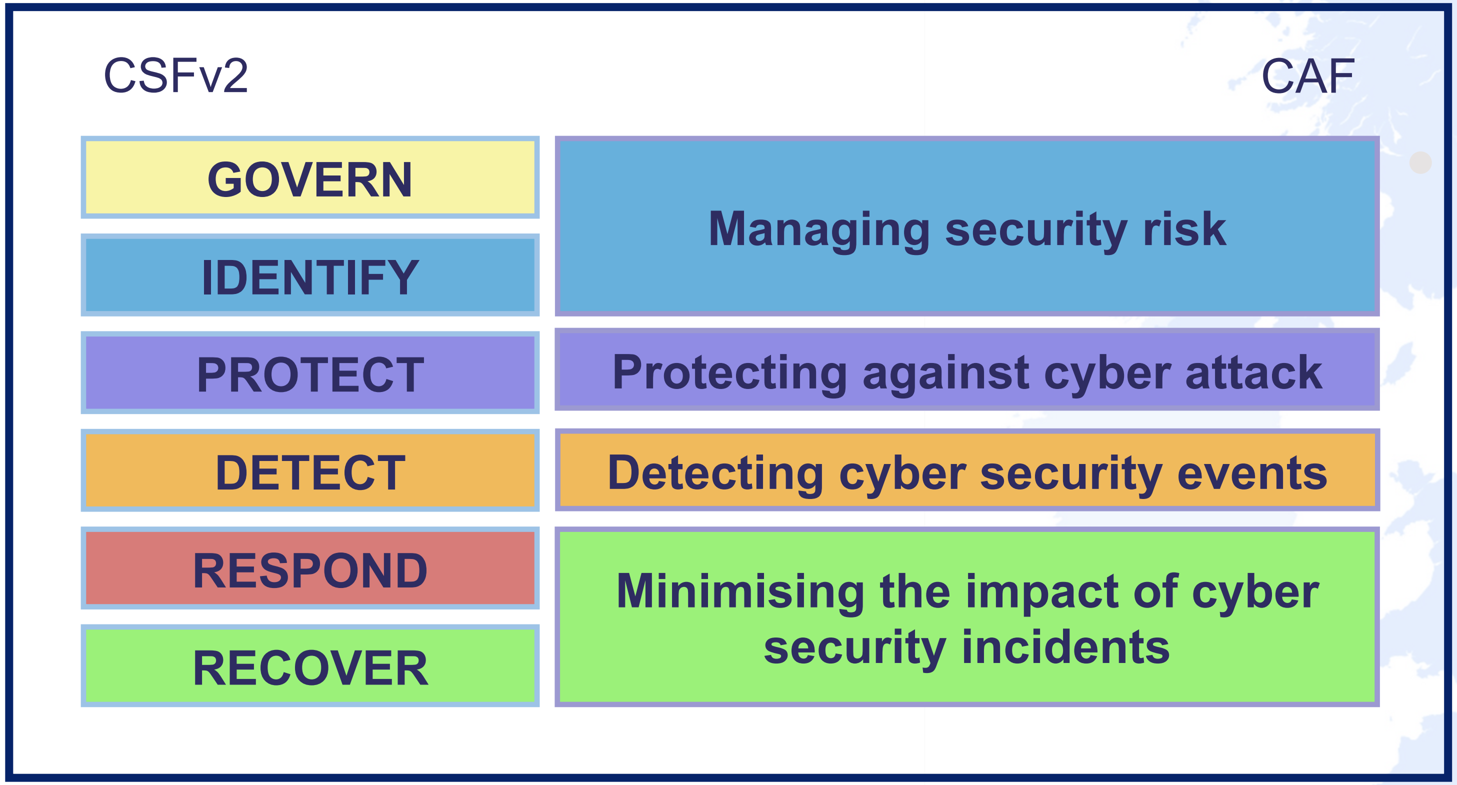


Cybersecurity Framework Approach

- As discussed in previous talks, understanding our approach in the context of existing cybersecurity frameworks is important
  - Tool to help structure strategy roadmap
  - Align with possible future compliance requirements

NIST Cybersecurity Framework v2/CAF

- NIST recently released v2 of their Cybersecurity Framework

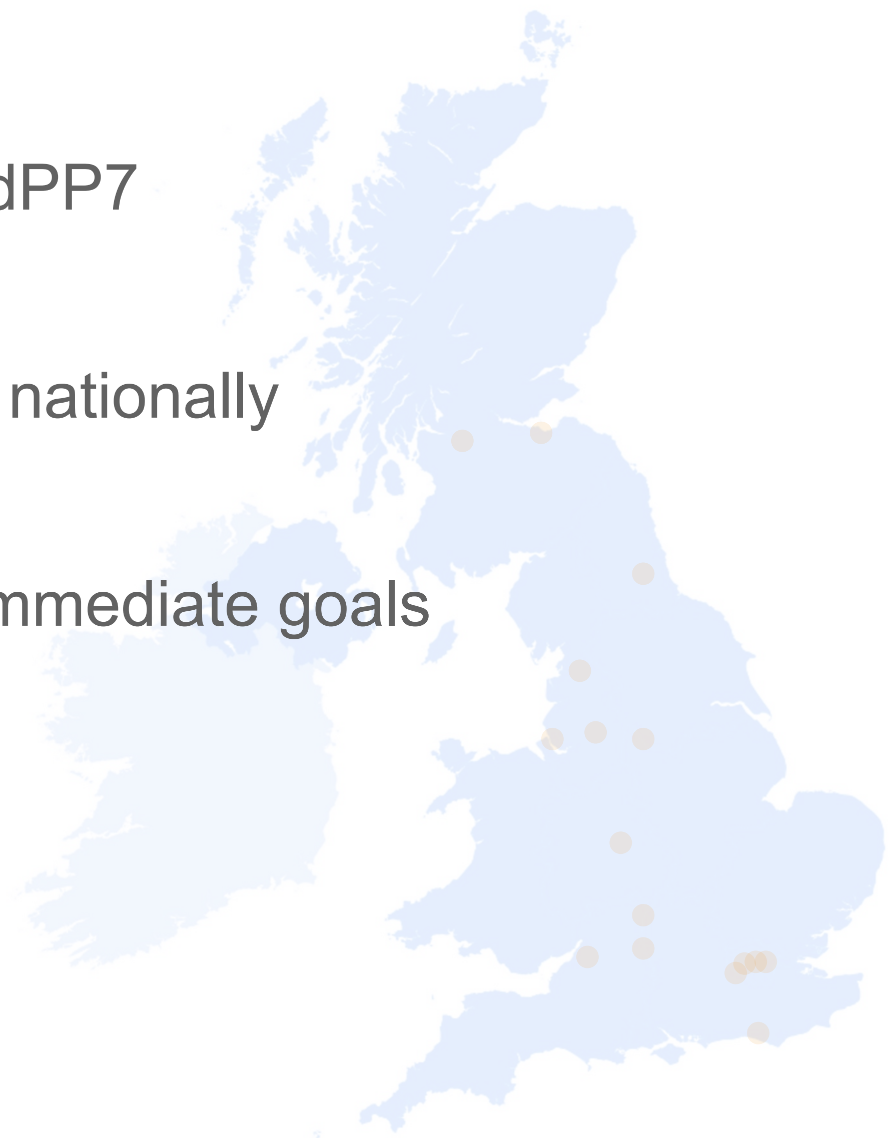


CSFv2	CAF
GOVERN	Managing security risk
IDENTIFY	
PROTECT	Protecting against cyber attack
DETECT	Detecting cyber security events
RESPOND	Minimising the impact of cyber security incidents
RECOVER	

GridPP Security Strategy

- Need to plan our approach over the course of GridPP7
- Make sure that we're achieving what we need
- Align and participate in broader work taking place nationally

- Identify goals for the duration of the project, and immediate goals
  - Mindful of individual site considerations



Science and Technology Facilities Council

Scientific Computing

GridPP UK Computing for Particle Physics

Inputs + parallel work

- What are the external inputs to such a strategy?

- The threat landscape we’ve already discussed
- Compliance environment
- Other (inter)national infrastructure developments
  - Including IRIS (referring back to Jon’s talk)

- Parallel work
  - We’re also looking at strategy work for STFC and DRI

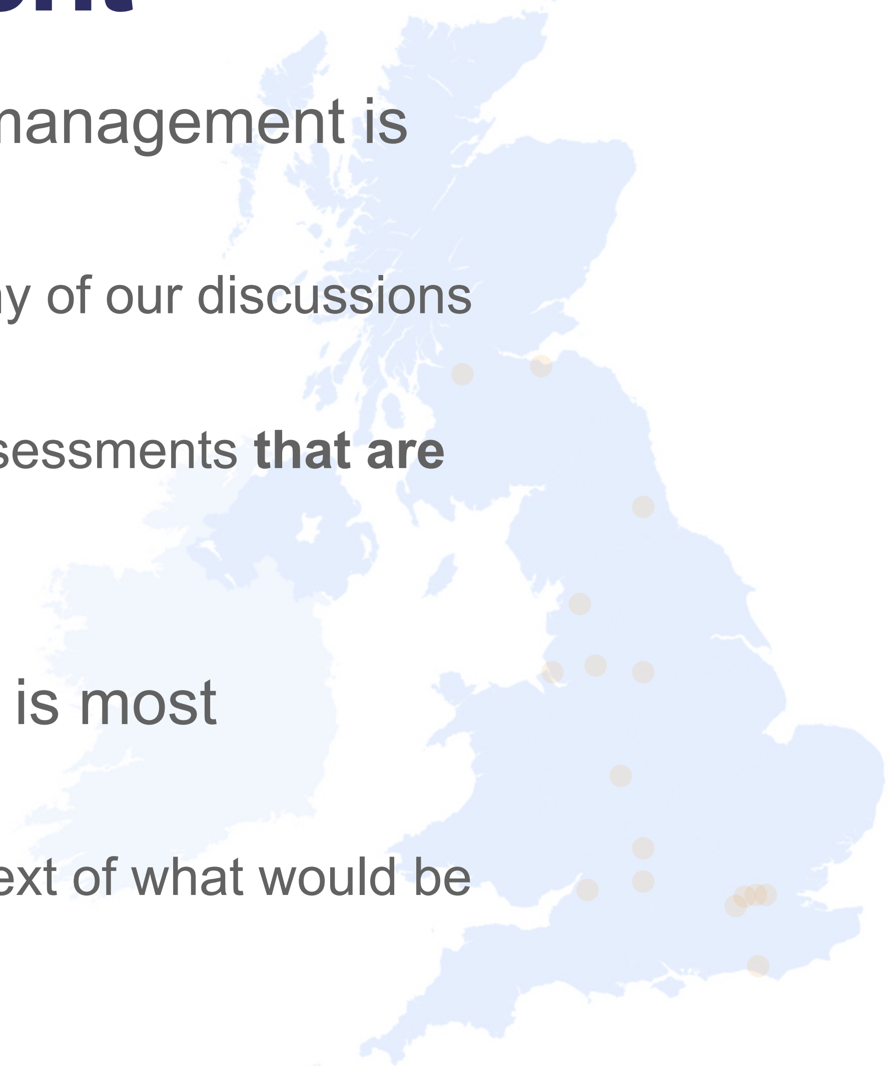
Potential strategic objectives

GOVERN

IDENTIFY

Managing security risk

Governance/Risk management



- It is clear from many recent discussions that risk management is essential
  - Notable that at recent EGI CSIRT F2F, the result of many of our discussions was “we need a risk assessment”
  - And: from previous project experience, we need risk assessments **that are acted upon**
- What cybersecurity risk assessment methodology is most appropriate for GridPP?
  - Both in the context of the overall project and in the context of what would be effective for sites

Protect

- Protection covers a broad range of topics

Policy	Dave K discussed at ISGC the need for revised WLCG policies
Security architecture and hardening	Identify best practice as part of broader (inter)national activity; indicate which is most appropriate for GridPP
Vulnerability risk assessment	Understanding the risk posed by different vulnerabilities is critical; examine how best to approach this work in the new DRI context
Skills and training	Identifying users, operations and cybersecurity staff as groups requiring training; examine what role GridPP can/should play

Science and Technology Facilities Council

Scientific Computing

GridPP UK Computing for Particle Physics

Detection

- Discussed the development of SOC reference designs for many years
  - And now the SOC WG is officially expanding its scope to cover people and processes as well as technology
- Must identify and plan what activity is needed for GridPP
  - As part of broader work in IRIS/DRI
- In particular, need to consider how to approach this from a people and process perspective
  - How can GridPP/IRIS support sites with distributed processes and analysis
- In this area in particular need concrete planning this quarter

DETECT

Detecting cyber security events

Detection

- What would be most impactful as a testbed activity
  - How to identify the best approach for the Tier1 vs Tier2s
    - Full-scale SOCs require significant sustained effort: will necessitate collaboration with central security teams

- Technical aside: host-based monitoring, Endpoint Detection and Response (EDR: Crowdstrike/Carbon Black/etc) is a very important tool
  - What is the performance impact of using these areas?
  - Already have some broader interest in working on this
  - Propose a CHEP abstract

RESPOND

RECOVER

Minimising the impact of cyber security incidents

Respond and Recover

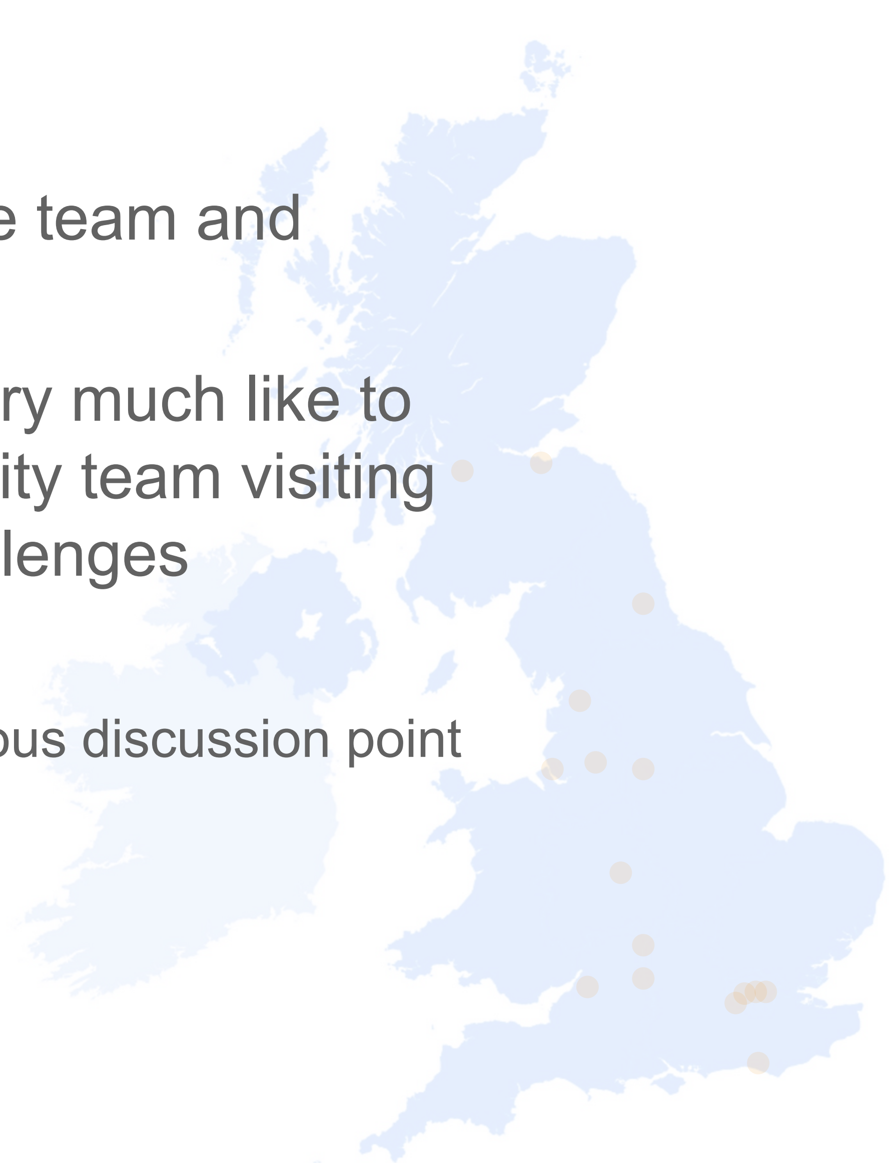
- Combined GridPP/IRIS security team well established
- Make concrete plans – in conjunction with IRIS – for how to continue the development of this team
- As noted in previous discussions, establish the roles and capabilities we want to have in the team
  - Incident response
  - Relationships with other security teams
  - Role in supporting other areas of work

DRI Cybersecurity Update

- In April we will hold the first DRI Cybersecurity Strategy Workshop
- Bring together research infrastructures, trusted research environments, University and NREN (Jisc) perspectives
- Over two days, finalising 3 primary outcomes
  - Overview of landscapes and challenges (short term, 2-3 year)
    - Intend to write a position paper as a result
  - Initial form of long-term strategy (3-5 year)
  - Initial set of short-term goals (FY24)
    - Including identifying testbed work to which GridPP could contribute

Next steps

- In coming weeks build the overall strategy with the team and others
- Consult with sites: with start of GridPP7, would very much like to arrange a Security Tour with a subset of the security team visiting individual sites to talk about their context and challenges
  - Could meet individually or in groups
  - Relationship with corporate/central IT would be an obvious discussion point
- Build action plan for this FY
  - Including work as part of broader IRIS/DRI activities



Science and Technology Facilities Council

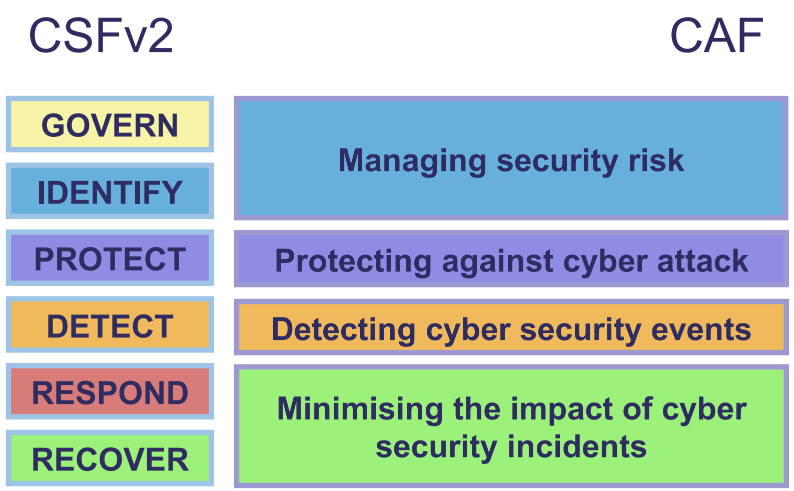
Scientific Computing

GridPP

UK Computing for Particle Physics

Questions?

Reference colour blocks: small



CSFv2

GOVERN

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

CAF

Managing security risk

Protecting against cyber attack

Detecting cyber security events

Minimising the impact of cyber security incidents