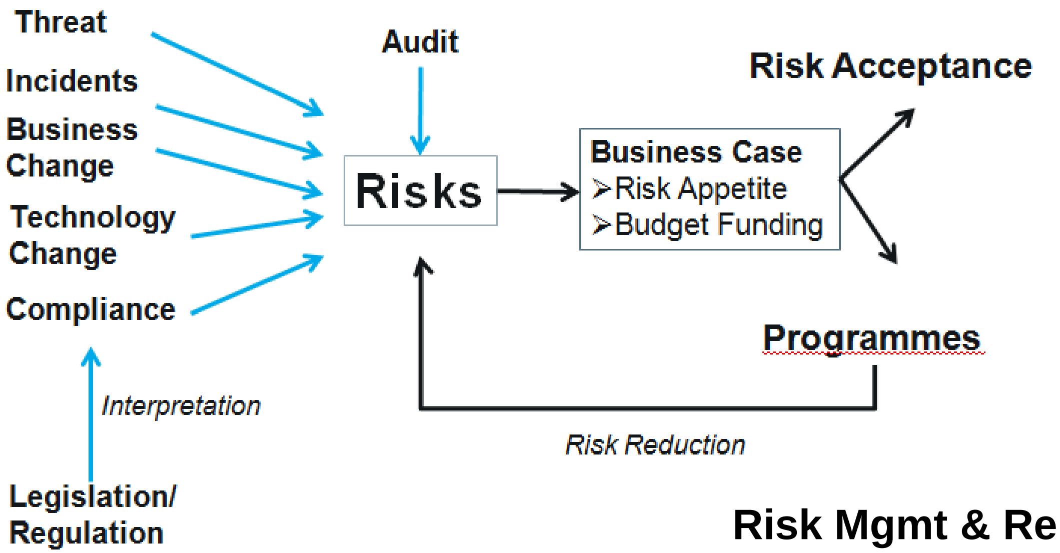
nationalgrid

THE POWER OF ACTION

Enterprise Security Governance

Robert Coles – Chief Information Security Officer and Global Head of Digital Risk & Security

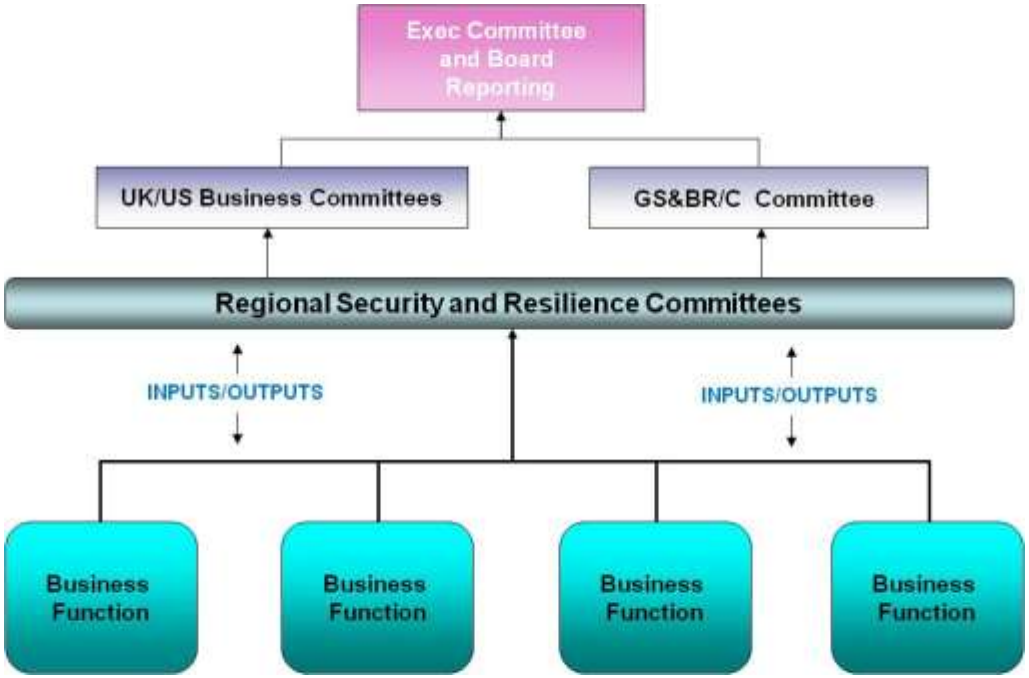
Governance and Organisational Model



Digital Risk & Security Team

- Governance
- Strategy, Architecture, Policy & PMO
- Inv & Threat Mgmt
- Business Info Risk Mgmt
- Consulting
- Global Privacy

Risk Mgmt & Reporting

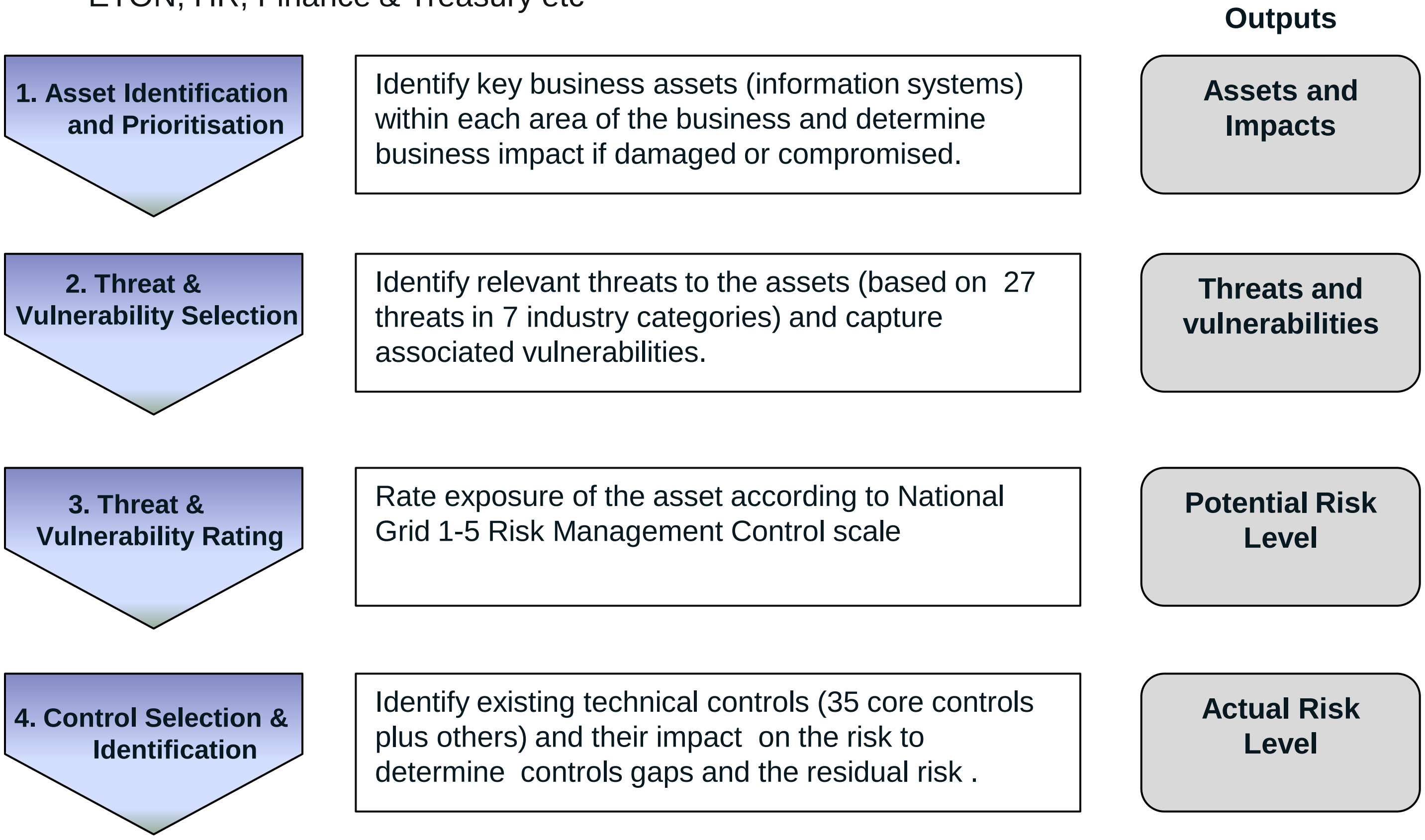


Threat & Control Assessment

Approach

33 Workshops, 47 Information Assets/Asset Types

Across UK & US: Business Units, Trading Systems, CNI/Network Operations/Field Devices – Gas & Electricity, Field Management, LNG, Metering, Generation, IT Infrastructure – email, desktops mobiles, etc', IT Applications – SAP, Billing, Payments, ETON, HR, Finance & Treasury etc



		Outputs
1. Asset Identification and Prioritisation	Identify key business assets (information systems) within each area of the business and determine business impact if damaged or compromised.	**Assets and Impacts**
2. Threat & Vulnerability Selection	Identify relevant threats to the assets (based on 27 threats in 7 industry categories) and capture associated vulnerabilities.	**Threats and vulnerabilities**
3. Threat & Vulnerability Rating	Rate exposure of the asset according to National Grid 1-5 Risk Management Control scale	**Potential Risk Level**
4. Control Selection & Identification	Identify existing technical controls (35 core controls plus others) and their impact on the risk to determine controls gaps and the residual risk .	**Actual Risk Level**

Key Threats

A) Insider Attack / Error
A threat to National Grid Systems / Data from a trusted source within the National Grid security perimeter

B) System Availability / Malfunction
A threat to National Grid Systems / Data availability due to System Malfunction

C) Malware / Virus Attack
A threat to National Grid Systems / Data from an indirect attack via Malware or Virus infestation

D) Data Leakage / Corruption / Availability
A threat to National Grid Data confidentiality, integrity or availability

E) External Attack
A threat to National Grid Facilities, Personnel, Systems / Data via a directed attack by an outside party from outside the security perimeter with the intent of causing damage or destruction

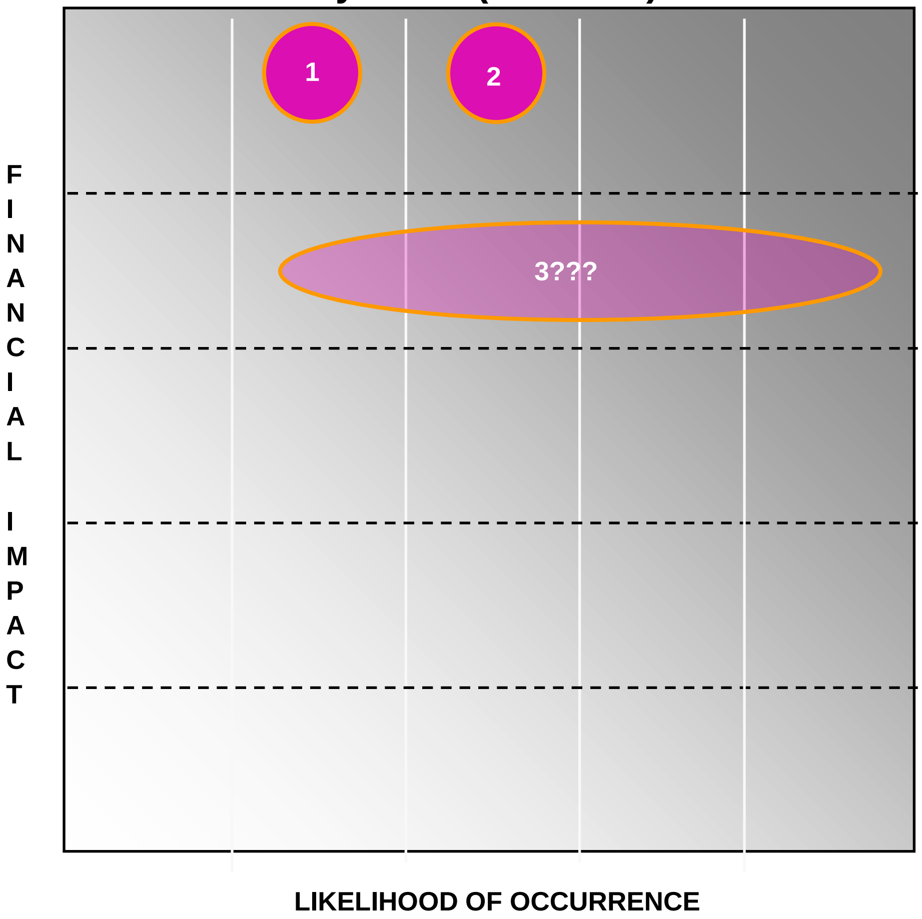
F) Unauthorized Access
A threat to National Grid Facilities, Personnel, Systems / Data due to unauthorized access

G) Criminal Victimization of Employees
A threat to National Grid personnel from criminals, disgruntled customers, or members of the pubic.

H) Regulatory Non-Compliance
A threat of fine or sanction resulting in monetary loss or negative reputational impact

I) Commercial/state sponsored espionage
A threat by foreign actors to achieve economic or technical advantage at the expense of National Grid

Key Risks (GLOBES)



1 Catastrophic cyber security breach of CNI systems
2 Major cyber security breach of business systems/data
3 IT embedded in Operational Technology

Threat and control assessment (cont)

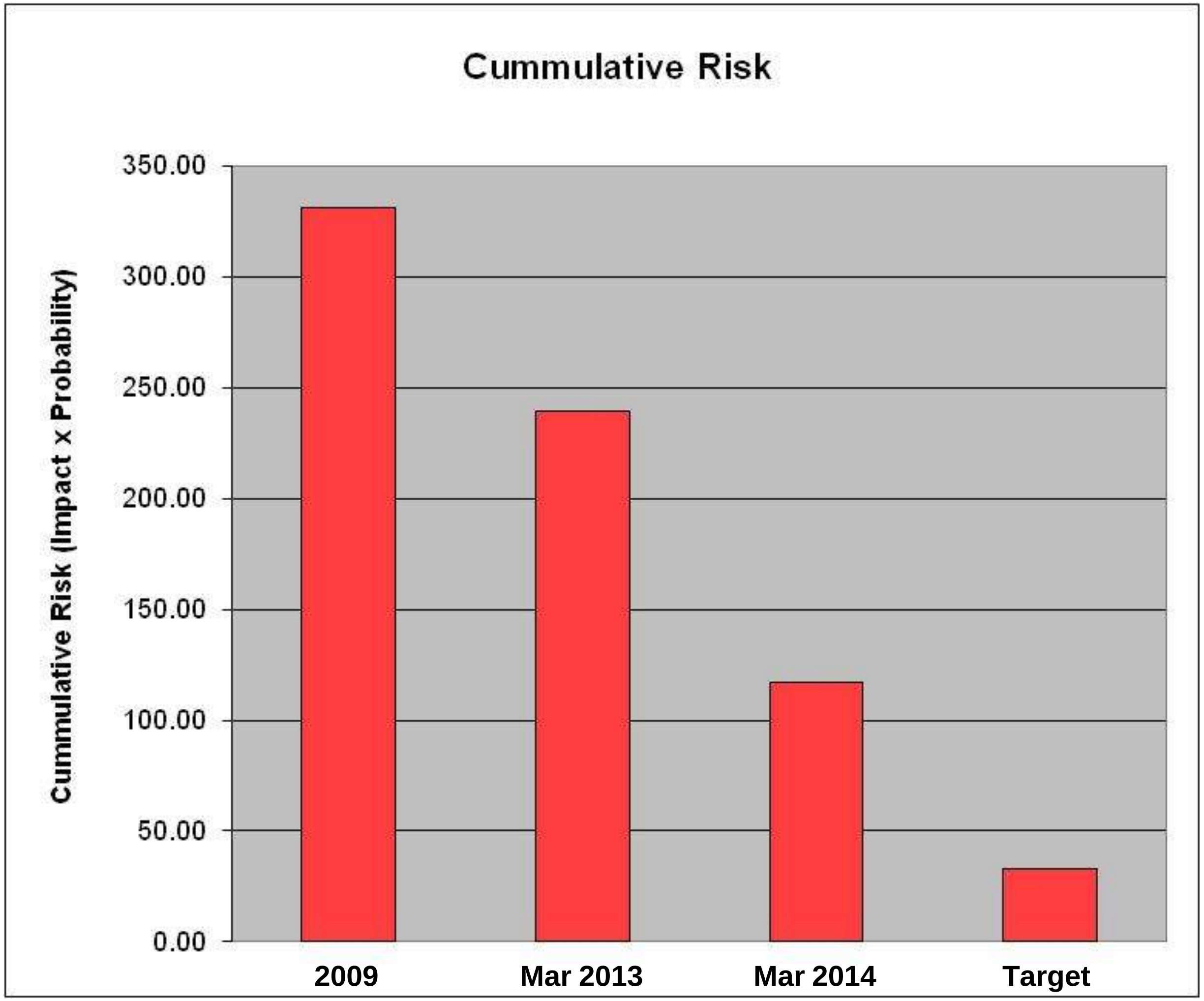
Key investment areas

1. **Endpoint Security** – security of end user computing and information
2. **Shared Information** – security and access to stored sensitive information
3. **Network Security** – network access control, configuration and zoning
4. **Access Control** – user access provisioning and management
5. **Critical National Infrastructure** – specific improvements

Program

1. **Foundational** – definition of underlying policies & standards and more detailed analysis and remediation planning across several specific areas
2. **Tactical** – short to medium term remediation activities
3. **Strategic** – long term remediation activities focused on enhancing and implementing new security technologies and capabilities

Digital Risk & Security Programme Update



Energy threat landscape is changing

nationalgrid

THE POWER OF ACTION

We need:

- Better intelligence and co-ordination from intelligence communities
- Disruptive response capabilities from federal agencies and co-ordination across state and national borders
- A regulatory environment to allow investment in security infrastructure to address changing risks
- Facilitated co-ordination of incident response across government and business

We don’t need:

- Forced disclosure of incidents that could increase our vulnerability
- Standards/audits/compliance based rules
- Sanctions for infringements of the national rules