AI Generated

Security & Resilience challenges of Operators of Essential Services

Applying Health & Safety Success to Essential Services



CYBER · PHYSICAL · IT · OT

VIBERT

No mentions of Stuxnet, AI or Quantum !



Assurance and Compliance – it's really Best Practice

"All you ever wanted to know about achieving compliance…

but were too busy to ask….."



VIBERT

Cevn Vibert
Vibert Ltd.



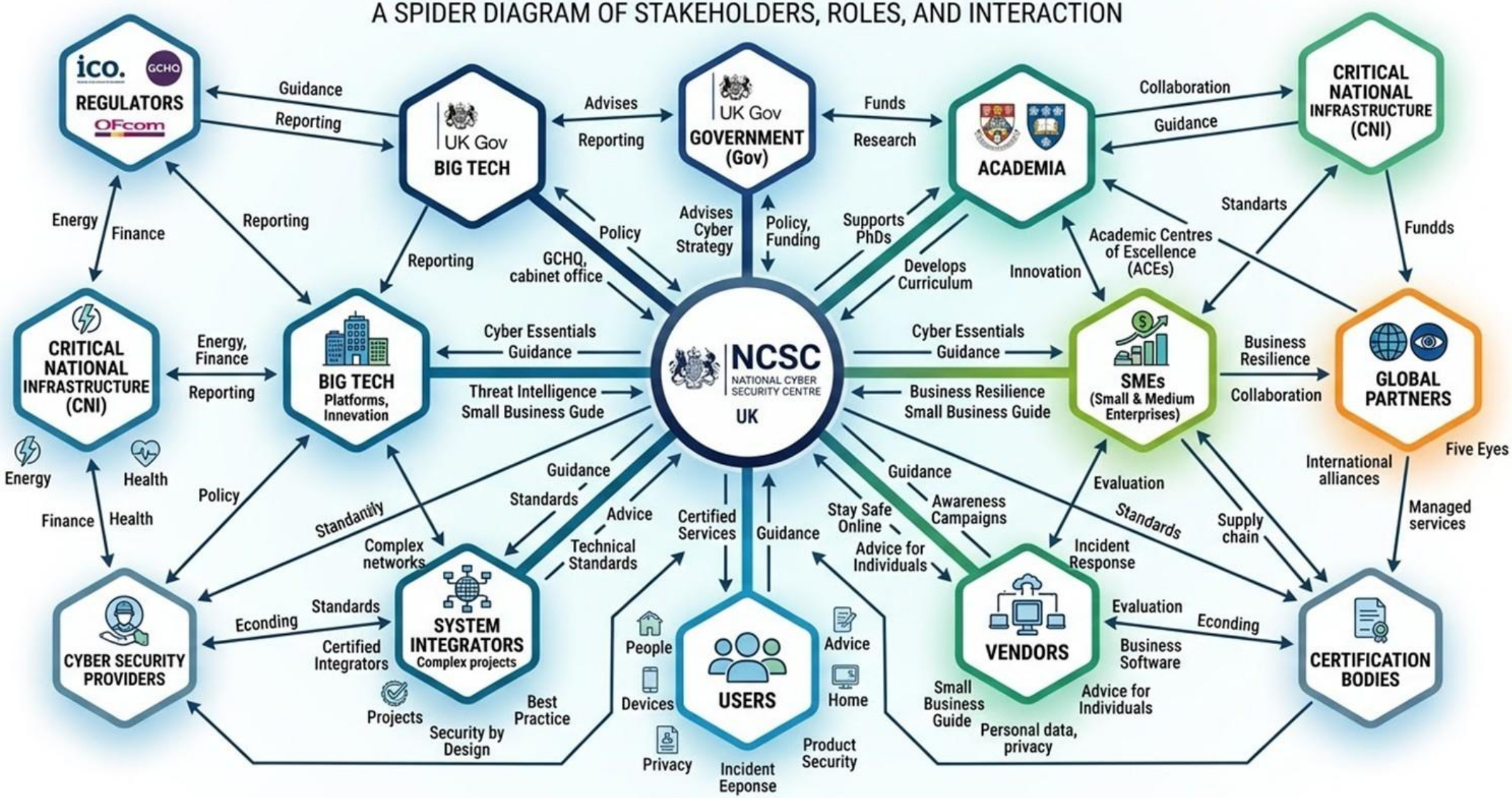
- NIS/NIS2/NIST Compliance Advisor.
- Ex-Principal Assurance at OFGEM NIS Competent Authority.
- Ex-Thales UK CNI Security SME and Design Authority.
- Founding Chair of the InstMC Cyber SIG.
- Cyber Alliance founding member, formed UK Cyber Security Council.
- OT Cyber Consultant.
- Chartered Cyber Professional. ChCSP
- Chartered IT Professional. CITP
- Chartered Engineer. CEng
- Fellow of the BCS, IET, and InstMC.
- Member of NCSC COI.
- Student Mentor.

Welcome connections on **LinkedIn**. 30k followers. Easy to Google!

VIBERT

THE UK CYBER SECURITY ECOSYSTEM & NCSC LINKS

A SPIDER DIAGRAM OF STAKEHOLDERS, ROLES, AND INTERACTION



AI Generated

Example Experiences



Nuclear



The ISS. SPACE!

Ocular Contact Lenses





P&G



English China Clay Proteus GTG



Piccadilly Lights



CBRN



Colombian Oil Pipeline Coupler





FPSO Radio Coupler

Cross-Thames Link

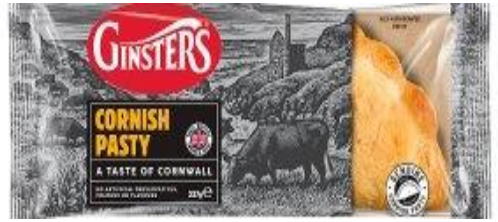




Sibur Jaroslavl Tyre Factory



Maidenhead, Basingstoke, Guildford, Hereford, Chertsey,..... Water Industry.



Career sector and Industry experiences *(since 1985!)*

Energy, Water, Waste, Defence, Steel, Tyres, Cement, Pharmaceuticals, Ceramics, Packaging, Medical Devices, Oil and Gas, Renewables, Nuclear Energy, Mining, Nuclear Reprocessing, Ink, Radio Systems, Media Systems, Space, Food, FMCG, Rail, Road, Metro, Chemicals, Demo Facilities, Micro-Electronics, ...

Prime System Providers, Systems Integrators, Global Supplier, Global Reseller, Independent Consultant, Industry Volunteering, Industry Chairing, Conference Chair and Speaker, Government Competent Authority, ...

LinkedIn Groups owner/manager for around 120,000 members in total.

30,000 followers. 30,000 connections

I need to get out more! ☺

VIBERT

Compliance findings in my career



Many organisations typically have : -

- False/relaxed compliance reports – hiding it under the carpet.
- Compliance reported with low skills and experience – irrelevant evidence.
- Compliance based on IT only, and not OT nor Physical nor Resilience.
- Risks unmanaged and undocumented – “Joe knows what he’s doing, we talked it over”
- Poor resources – people, tech, social, education, PR, 3rd party,…
- No holistic integrated security and resilience – departments, panels, ..
- No risk appetite – what is acceptable? Is the C-Suite aware?
- No network flow diagrams – who knows what comms should be going & where?
- No resilience practiced…….
- Supply Chain choices managed by finance/purchasing dept.
- Complex compliance confusion NIS(UK), NIS2(EU), CAF(UK NCSC), new CS&R Bill, NIST(global), ISA 62443(OT), …

VIBERT

Organisational security failings observed



- Insufficient SQEP throughout the Roles and Responsibilities. No RACIs or equiv.
- No mapping of projects/activities back to Governance/Policies.
- Insufficient Technical and Operational Risk Assessments.
- No ‘full-circle’ Risk Management linked to Governance/Policies.
- Poor Holistic Asset Management and unidentified criticalities.
- Poor or no Incident Management and Resilience (DR/BC) exercising, tabletop or real.
- Lack of Secure Holistic Configuration/ Development.
- Lack of holistic Physical, IT, OT, and Operational Security.
- Weak or non-existent Supply Chain Security.
- Internal audits, if they exist, lack evidence and are not BAU.
- Weak understanding of OT <> IT <> Physical Security Networks, flows and protocols.
- Poor or disconnected JML Joiners/Movers/Leavers.
- Inadequate, if it exists, holistic Security and Resilience Training and Culture.

VIBERT

Excuses… Excuses…!?



Dog ate my homework!

- Lack of awareness at all levels vertically and horizontally (“That’s Cyber”)
- Poor communication of relevant and non-relevant teams (“We never talk”)
- Over-cooking the responsibilities to individuals. (“I left in the end”)
- Over-loading individuals (“I also have a day-job”)
- Mis-matched RACI with skills and experience. (“They never trained me”)
- Poor Governance of Security - shop-floor to C-Suite. (Beyond me!”)
- Little or no involvement from other departments (“It’s all cyber!”)
- Legacy tasking and poor documentation. (“Before my time!”)
- Poor control on base outcomes (“Purchasing buy the cheapest provider”)
- “We have no budget – not enough people – jobs too big – no management - ..”

VIBERT

Typical Assurance Findings
Missing Risk Management Framework
Incomplete Asset Inventory
Weak Governance & Accountability
Poor Incident Detection & Response
Delayed Incident Reporting
Insecure System Development Practices
Inadequate Authentication Controls
Patch & Vulnerability Management Gaps
Unencrypted Sensitive Data
Missing Compliance Evidence Documentation

How can we all help the UK (and beyond) to improve its Resilience?

CSRB is the “directive”.

How can we all help?

VIBERT

Guidance 1: Use “Best Practices”



- Determine your aims and build a **continuous review** process
- Obtain **SENIOR buy-in** now, and collaborate always.
- Adapt your own applicable framework.
- Risk assess, but ask why, and keep asking why, related to the business need and policies.
- Consider a RACI chart to ensure who is who **and** develop a skills matrix alongside the RACI. Do they match?
- Who **don’t** you train Cyber Security **and** Resilience?
- Are you working alone or as a team with 3rd parties, technical authorities, and others?
- Is this a Project, a Programme, or BAU?
- When did you last practice resilience? DR (Disaster Recovery) or BC (Business Continuity)
- Socialise: Use the successful H&S “marketing vehicle” and add Cyber Security, Physical Security and Resilience to the machine.

Make “Compliance” into BAU and not a pain point, as it makes business sense.

VIBERT

Guidance 2: Run Workshops (It's how we help)



- More organisations are running internal and external workshops.
  - Building relationships across departments.
  - Innovating
  - Assist in clarifying the RACIs for each role.
  - Finding gaps in technical, operational and processes.
  - Involving 3rd parties and supply-chain.
  - Implementing holistic security and resilience as **BAU.**
  - Sharing information such as incidents, threats, risks, ..
  - Gamification to strengthen understanding and exercising.
  - Understanding what the Compliance Inspectors will ask for.

Evidence Continual Improvements !

VIBERT

Guidance 3: Include Physical Security – not just “Cyber stuff” but also Safety Related

AI Generated





Know your critical assets, know your resilience processes, safety first, strive for zero harm, use the Health and Safety “bandwagon” that is now common practice.

VIBERT

Objective	Objective		Principle		Contributing Outcome
A	Managing Security Risk	A1	Governance	A1.a	Board Direction
		A1	Governance	A1.b	Roles and Responsibilities
		A1	Governance	A1.c	Decision-Making
		A2	Risk Management	A2.a	Risk Management Process
		A2	Risk Management	A2.b	Understanding Threat (New in v4.0)
		A2	Risk Management	A2.c	Assessment and Management of Risk
		A3	Asset Management	A3.a	Asset Identification and Ownership
		A3	Asset Management	A3.b	Asset Classification and Handling
		A4	Supply Chain	A4.a	Supply Chain Risk Management
		A4	Supply Chain	A4.b	Secure Software Development and Support (New/Expanded in v4.0)
B	Protecting Against Cyber Attacks	B1	Service protection policies, processes and procedures	B1.a	Policy and Process Development
		B1	Service protection policies, processes and procedures	B1.b	Policy and Process Validation & Implementation
		B2	Identity and Access Control	B2.a	Identity Verification and Authentication
		B2	Identity and Access Control	B2.b	Access Control and Privilege Management
		B2	Identity and Access Control	B2.c	Identity and Access Management Governance
		B3	Data Security	B3.a	Data in Transit Security
		B3	Data Security	B3.b	Data at Rest Security
		B3	Data Security	B3.c	Data Sanitisation and Media Handling
		B3	Data Security	B3.d	Mobile and Remote Working Data Protection
		B4	System Security	B4.a	Secure Configuration and Vulnerability Management
		B4	System Security	B4.b	Secure Architecture and Boundary Protection
		B4	System Security	B4.c	Secure System Administration
		B4	System Security	B4.d	Malware Protection and Software Security
		B5	Resilient networks and systems	B5.a	Segregation and Network Architecture
		B5	Resilient networks and systems	B5.b	Resilience and Redundancy Design
		B5	Resilient networks and systems	B5.c	Physical Security
		B6	Staff awareness and training	B6.a	Cyber Security Training and Awareness Culture
		B6	Staff awareness and training	B6.b	Staff Vetting and Ongoing Capability Assessment
C	Detecting Cyber Security Events	C1	Security Monitoring	C1.a	Monitoring Coverage and Scope
		C1	Security Monitoring	C1.b	Log Generation and Collection
		C1	Security Monitoring	C1.c	Log Retention and Protection
		C1	Security Monitoring	C1.d	Security Analytics and Correlation
		C1	Security Monitoring	C1.e	Monitoring Capability and Operations
		C1	Security Monitoring	C1.f	Understanding User and System Behaviour, and Threat Intelligence (New in v4.0)
		C2	Threat Hunting	C2.a	Proactive Incident and Anomaly Discovery
		C2	Threat Hunting	C2.b	Threat Hunting Capability and Methodologies (Updated in v4.0)
D	Minimising the Impact of Cyber Security Incidents	D1	Response and Recovery Planning	D1.a	Incident Response Plan Development
		D1	Response and Recovery Planning	D1.b	Incident Response Capabilities and Resources
		D1	Response and Recovery Planning	D1.c	Incident Testing and Exercises
		D2	Lessons Learned	D2.a	Post-Incident Review and Analysis
		D2	Lessons Learned	D2.b	Continuous Improvement Implementation
E?					

AI Generated

NCSC CAF

Cyber Assessment Framework.

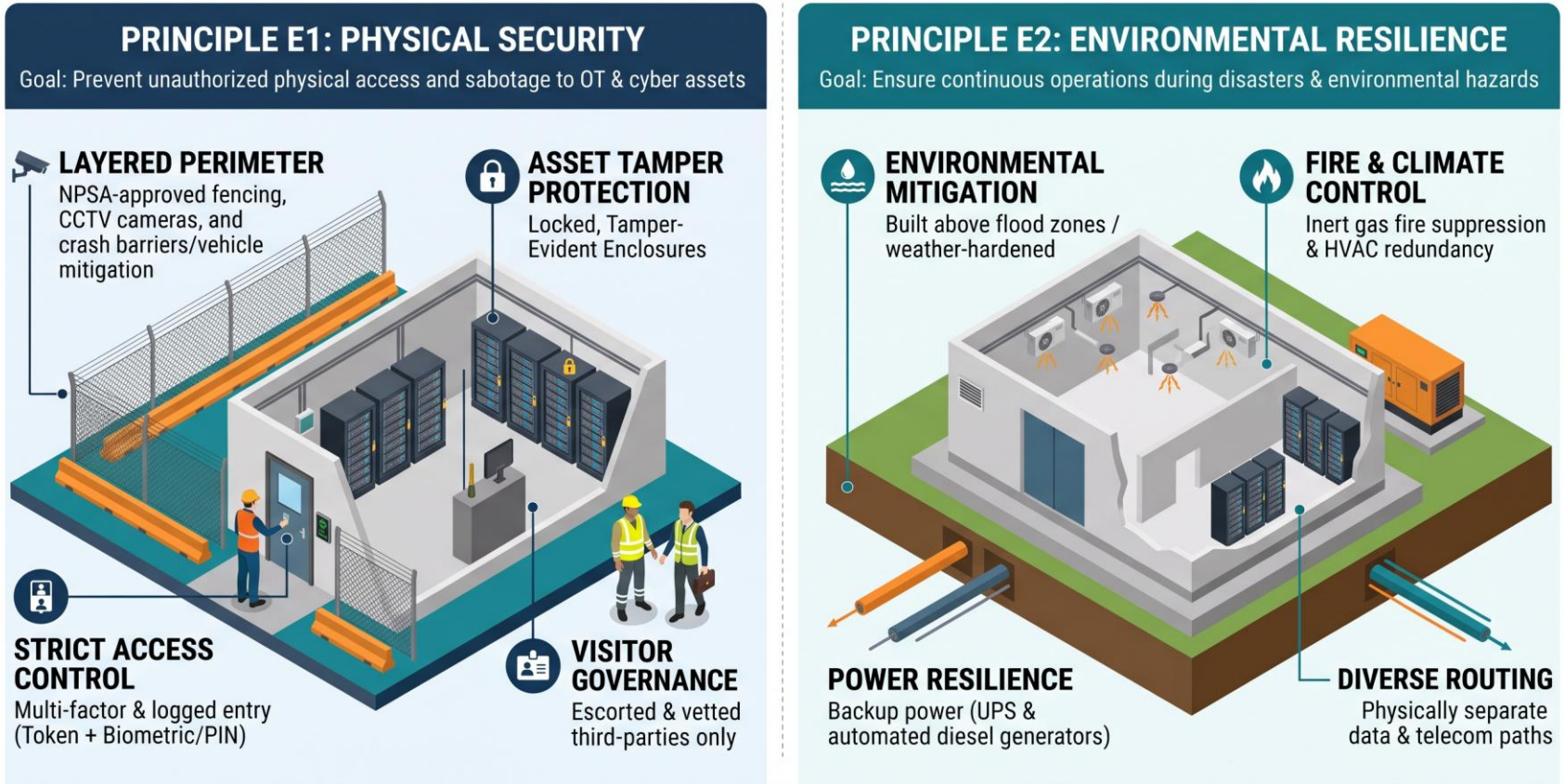
NIS Compliance “yardstick”.

V4

This is not NIS2

VIBERT

Ofgem CAF Compliance: Physical & Environmental Security



AI Generated

CAF Objective E: Protecting against non-cyber risks..

NIS security duties include taking non-cyber measures to manage the risk of 'physical events that might have an adverse effect on networks and information systems'

Objective E relates only to the physical security of the **components of the network and information systems** on which the essential function relies.

Principle E1 relates to the risks presented by malicious threat actors gaining physical access to the components of network and information systems.

Principle E2 relates to non-malicious risks such as those caused by environmental hazards and accidents.

VIBERT

E1. Physical Access Security.
Example Indicators of good practice

- **Perimeter and Layered Defence:** Facilities housing critical systems must use a "defence-in-depth" model (e.g., NPSA-approved perimeter fencing, CCTV monitoring, and hostile vehicle mitigation).

- **Strict Access Control:** Physical entry points to server rooms and OT control cabinets must require multi-factor authentication (e.g., physical token + biometric or PIN). All entries must be continuously logged and automatically audited.

- **Asset Tamper Protection:** Localized network switches, cabling, and engineering workstations must be housed inside locked, tamper-evident enclosures.

- **Visitor and Supply Chain Governance:** Unescorted physical access is restricted entirely to vetted personnel. Third-party contractors must be monitored continuously while in proximity to critical systems.

VIBERT

E2. Environmental Resilience. Example Indicators of good practice

- **Environmental Mitigation:** Server rooms and critical infrastructure facilities must be built out of historical flood zones or appropriately hardened against severe weather, extreme temperatures, and seismic risks.

- **Fire Suppression and Climate Control:** Automated, non-destructive fire suppression systems (e.g., inert gas) and industrial-grade HVAC redundancy must be actively maintained.

- **Power and Utility Resilience:** Critical systems must possess immediate backup power capabilities (uninterruptible power supplies (UPS) coupled with automated-start diesel generators) tested regularly under load.

- **Diverse Routing:** Critical communication links, backup data pathways, and telecommunications feeds must enter the facility via physically separate geographic paths to avoid a single point of failure (e.g., a single stray excavator cutting all lines).

VIBERT

Guidance 4: Build a Security & Resilience Compliance Culture

Health and Safety posters are everywhere,

and well understood …

Why not **Security**?

Why not **Resilience**?

Develop Integrated Holistic Security



AI Generated

VIBERT

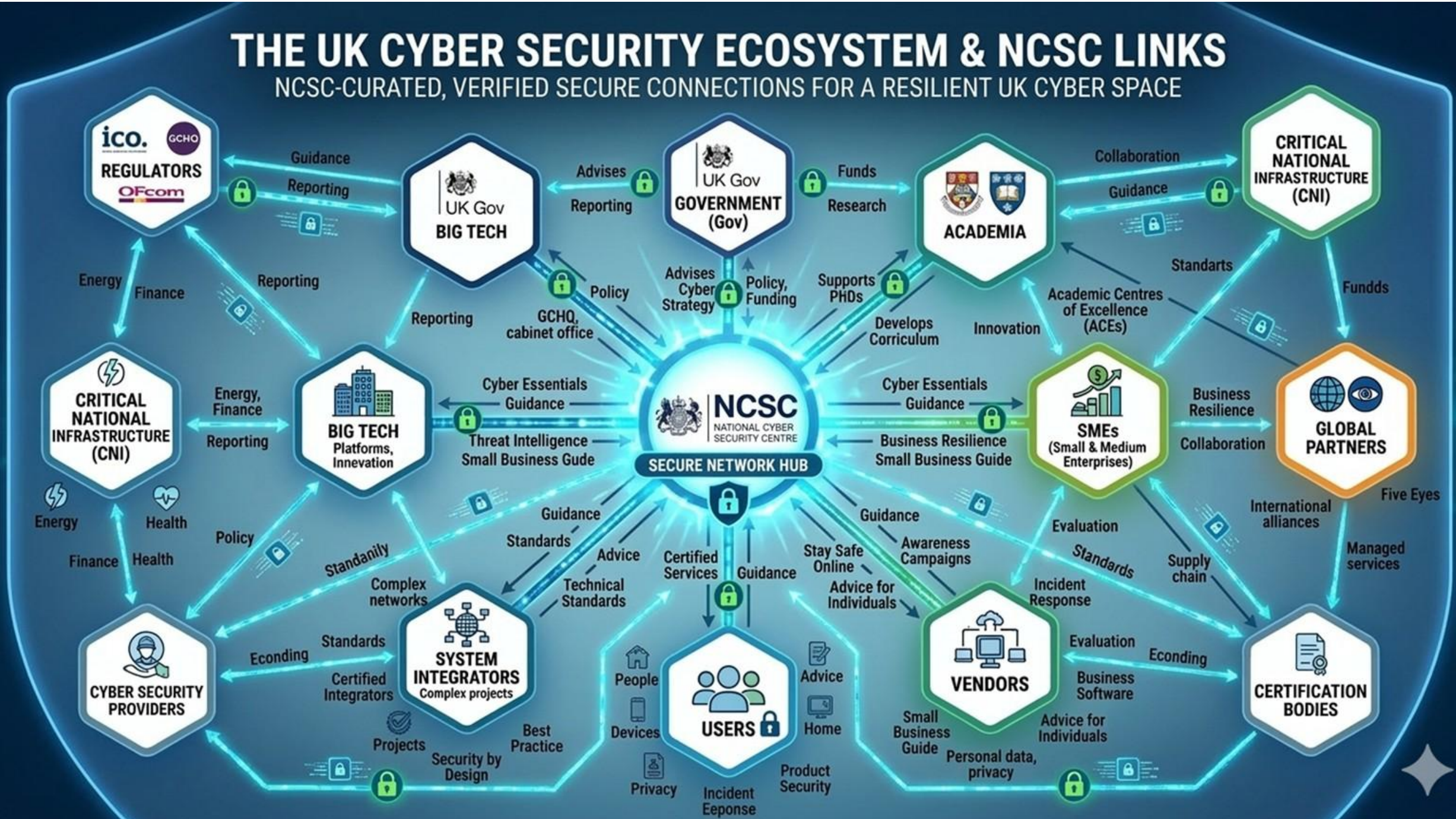
Guidance 5: Cev's Dreams.



1. Build Leader-Level Resilience engagement in the C-Suite.
2. Improve Budgets for Security and Resilience nationally.
3. Build a SQEP Factory (suitably qualified & experienced people).
4. Build training programmes with useful experiencial hands-on.
5. Legislate supply-chains to the NIS(UK) & NIS2(EU) regs.
6. Fund National Resilience busses – Security goes on tour!.
7. Fund a National Programme of Cyber interconnection of Labs.
8. Connect up the NCSC, Academia, Vendors, Users and System Integrators.
9. Fund a proctored/managed 'secure test network' for all to use.



VIBERT


THE UK CYBER SECURITY ECOSYSTEM & NCSC LINKS
NCSC-CURATED, VERIFIED SECURE CONNECTIONS FOR A RESILIENT UK CYBER SPACE
ico.
GCHQ
REGULATORS
OFcom
Guidance
Reporting
UK Gov
BIG TECH
Advises
Reporting
UK Gov
GOVERNMENT (Gov)
Funds
Research
ACADEMIA
Collaboration
Guidance
CRITICAL NATIONAL INFRASTRUCTURE (CNI)
Energy
Finance
Reporting
Reporting
Policy
GCHQ, cabinet office
Advises Cyber Strategy
Policy, Funding
Supports PHDs
Develops Corriculum
Innovation
Academic Centres of Excellence (ACEs)
Standarts
Fundds
CRITICAL NATIONAL INFRASTRUCTURE (CNI)
Energy, Finance
Reporting
BIG TECH
Platforms, Innevation
Cyber Essentials
Guidance
Threat Intelligence
Small Business Gude
NCSC
NATIONAL CYBER SECURITY CENTRE
SECURE NETWORK HUB
Cyber Essentials
Guidance
Business Resilience
Small Business Guide
SMEs
(Small & Medium Enterprises)
Business Resilience
Collaboration
GLOBAL PARTNERS
Five Eyes
Energy
Health
Finance
Health
Policy
Standanily
Guidance
Standards
Advice
Technical Standards
Certified Services
Guidance
Stay Safe Online
Advice for Individuals
Guidance
Awareness Campaigns
Evaluation
Standards
Supply chain
International alliances
Managed services
Complex networks
CYBER SECURITY PROVIDERS
Econding
Standards
Certified Integrators
SYSTEM INTEGRATORS
Complex projects
Projects
Best Practice
Security by Design
People
Devices
Privacy
USERS
Advice
Home
Incident Eeponse
Product Security
Incident Response
VENDORS
Small Business Guide
Personal data, privacy
Advice for Individuals
Evaluation
Econding
Business Software
CERTIFICATION BODIES

CYBER TOUR BUS: EDUCATING THE UK

BUS FITTED MATERIALS (Inside View)



- Interactive Threat Simulators
- Secure Device Demos
- Cyber Essentials Guidance Kiosks
- Privacy Workshops Workshops
- Cyber Act Inharances
- Privacy Workshops

TOUR HIGHLIGHTS

- Workshops
- Talks
- Resilience Workshop
- Hands-on activities
- Attentions
- Hands-on activities

Academia & Innovation Hub

Academia & Innovation Hub
Smal Business & Enterpies

3 BELFAST

UK Gov GOVERNMENT (Gov)

4 MANCHESTER

CRITICAL NATIONAL INFRASTRUCTURE (CNI)

BIG TECH
Platforms, Innevation

NCSC
NATIONAL CYBER SECURITY CENTRE
UK

SMEs BIRMINGHAM

GLOBAL PARTNERS

2 CARDIFF

USERS

7 BRISTOL

1 LONDON
- Start at NCSC, Whitehall

Advises
Reporting
Funds
Research
Collaboration
Guidance
Policy
Advises Cyber Strategy
Policy, Funding
Supports PhDs
Standarts
Fundds
Reporting
GCHQ, cabinet office
Develops Curriculum
Innovation
Academic Centres of Escellence (ACEs)
Cyber Essentials Guidance
Cyber Essentials Guidance
Business Resilience
Collaboration
Threat Intelligence Small Business Gude
Business Resilience Small Business Guide
Five Eyes
International alliances
Managed services
Guidance
Standards
Advice
Technical Standards
Certified Services
Guidance
Stay Safe Online
Advice for individuals
Guidance
Awareness Campaigns
Evaluation
Standards
Supply chain
Incident Response
Standardly
Complex networks
Standards
Certified Integrators
Projects
Security by Design
Best Practice
People
Devices
Privacy
Incident Eeponse
Advice
Home
Product Security
Small Business Guide
Personal data, privacy
Business Software
Advice for Individuals
CYBER TOUR BUS

AI Generated

Compliance as BAU

Industry Standard Operating Practices

Governance & Leadership

1. Executive Security & Resilience Board
2. CAF Ownership Matrix (RACI + Skills Framework)
3. Board-approved Risk Appetite Statements
4. Continuous Compliance Programme

Risk & Assurance

5. Threat-Informed Risk Management
6. Evidence-Driven Internal Audit Programme
7. Integrated Security KPIs & Reporting

People & Culture

8. Security & Resilience Culture Programme
9. SQEP Development and Competency Management
10. Security Champions Across Departments

Technology & Operations

11. Enterprise Asset & Dependency Management
12. Identity Governance and Access Certification
13. Security Monitoring Across IT, OT & Physical Domains
14. Secure-by-Design Project Governance

Resilience & Supply Chain

15. Resilience Exercising and Supply Chain Assurance

VIBERT

National Guidance:

2025 UK Cyber Security & Resilience Priorities for CNI

Key Messages from NCSC, NPSA, DSIT & Government

✅ **Cyber Security & Resilience Bill CSRB (Not NIS2)**
Expands scope beyond traditional NIS sectors.
Stronger incident reporting requirements.
Greater focus on supply chain assurance.
Increased regulatory oversight and resilience outcomes.
Focus on resilience not just compliance.

✅ **Board-Level Accountability**
New Cyber Governance Code requires Boards to own cyber risk.
Focus areas: Risk, Strategy, People, Incident Response, Assurance.
Cyber governance now expected alongside financial governance.

✅ **CAF v4.0 (August 2025)**
Updated NCSC Cyber Assessment Framework.
Greater emphasis on threat-informed defence.
Increased focus on evidence of effectiveness and resilience.

✅ **NPSA: Protective Security & Sabotage**
Growing concern over hostile-state sabotage. Protect critical assets from physical, personnel and cyber threats. Review response, recovery and crisis-management plans. Strengthen security culture and insider-risk awareness.

✅ **Resilience at Scale**
NCSC identifies protection of UK CNI as a national priority.
Focus on operational resilience, crisis preparedness, detection and response.
Integration of cyber, physical and personnel security.

✅ **Supply Chain Security**
Critical suppliers and MSPs under increasing scrutiny.
NCSC continues to promote its 12 Supply Chain Security Principles.
Cyber resilience is only as strong as the weakest supplier.

Organisations must move beyond compliance and demonstrate measurable cyber resilience, strong governance, secure supply chains, tested recovery capabilities, and continuous assurance.
Organisations must prepare for crisis.

NCSC says secure your systems. NPSA says secure your people and sites. DSIT says prove both.
Sector specific Competent Authorities Ofgem/Ofwat/CAA/HSE/etc. give sector relevant advice.

NCSC Cyber Governance Code: https://www.ncsc.gov.uk/cyber-governance-for-boards/code-of-practice
DSIT Cyber Security & Resilience Bill: https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement
NCSC CAF: https://www.ncsc.gov.uk/collection/cyber-assessment-framework
NCSC Supply Chain Security: https://www.ncsc.gov.uk/collection/supply-chain-security
NPSA portal: https://www.npsa.gov.uk/

VIBERT

Questions?

Experiences?

Successes?

Challenges?

Help Needed?



Cevn Vibert
Vibert Ltd

Advisory, Consulting and Training –
IT/OT/Physical, Compliance Prep, NIS, NIS2, CAF, OT, GRC, ...

LinkedIn CevnVibert

cevn@vibert.ltd.uk

www.vibert.ltd.uk

+44 7909 992786

VIBERT