Cyber Security Governance: Updates from the Front Line

Templar Executives

Cyber Security Resilience For Business

Cyber Security Supplier to Government:

HM Government

Courses Accredited and Certified by:

Certified Training in association with National Cyber Security Centre

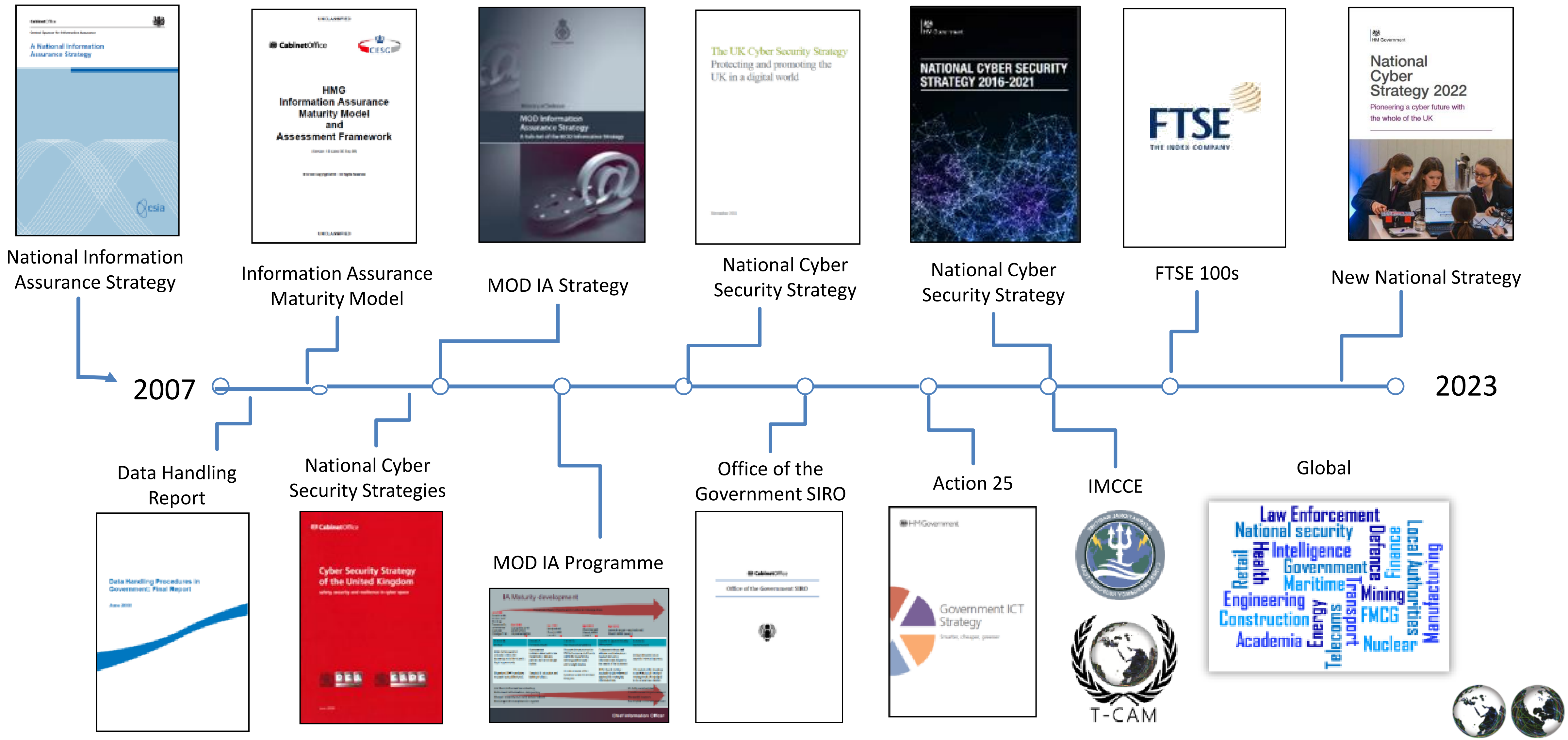
APMG International

Chartered Institute of Information Security

CYBER ESSENTIALS PLUS

The contents are confidential and may not be reproduced in whole or part without the prior written consent of Templar Executives.

World Class Track Record – Advising Government & Industry



2007

National Information Assurance Strategy

Data Handling Report

Information Assurance Maturity Model

National Cyber Security Strategies

MOD IA Strategy

MOD IA Programme

National Cyber Security Strategy

Office of the Government SIRO

Action 25

National Cyber Security Strategy

IMCCE

FTSE 100s

Global

New National Strategy

2023

A National Information Assurance Strategy
csia
HMG Information Assurance Maturity Model and Assessment Framework
Cabinet Office
CESG
MOD Information Assurance Strategy
The UK Cyber Security Strategy
Protecting and promoting the UK in a digital world
NATIONAL CYBER SECURITY STRATEGY 2016-2021
FTSE
THE INDEX COMPANY
National Cyber Strategy 2022
Pioneering a cyber future with the whole of the UK
Data Handling Procedures in Government: Final Report
Cyber Security Strategy of the United Kingdom
IA Maturity development
Office of the Government SIRO
Government ICT Strategy
T-CAM
Law Enforcement
National security
Intelligence
Government
Maritime
Engineering
Construction
Academia
Retail
Health
Defence
Finance
Local Authorities
Mining
FMCG
Nuclear
Manufacturing
Transport
Telecoms
Energy
Utilities

Templar Executives
Cyber Security Resilience For Business

Templar Executives - Services & Solutions

Business Consultancy

Cyber Academy

Cyber-as-a-Service

Cyber Physical Security

Global Services: MCERT

Business Continuity & Crisis Management

Our introductory video: https://www.youtube.com/watch?v=p_7LX-eRNAo

Cyber Security Consultancy

Assure & Advise; Board-level engagement, Cyber Security Risk Assessments, Governance & Strategy

Templar Cyber Academy

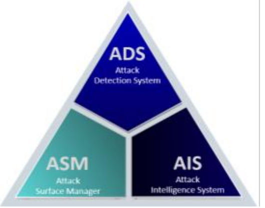
World-class education and training; market-leading portfolio of NCSC Certified courses

Templar BLADE

TEMPLAR BLADE
Cutting-Edge Cyber Intelligence For Business

A unique Threat Intelligence and monitoring service

Deception Technologies

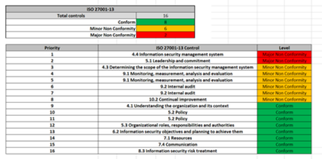


Active Defence to create a hostile environment for attackers

The Templar

A 'data center in a box' for contingency, backups, segregated environments

The CMAD



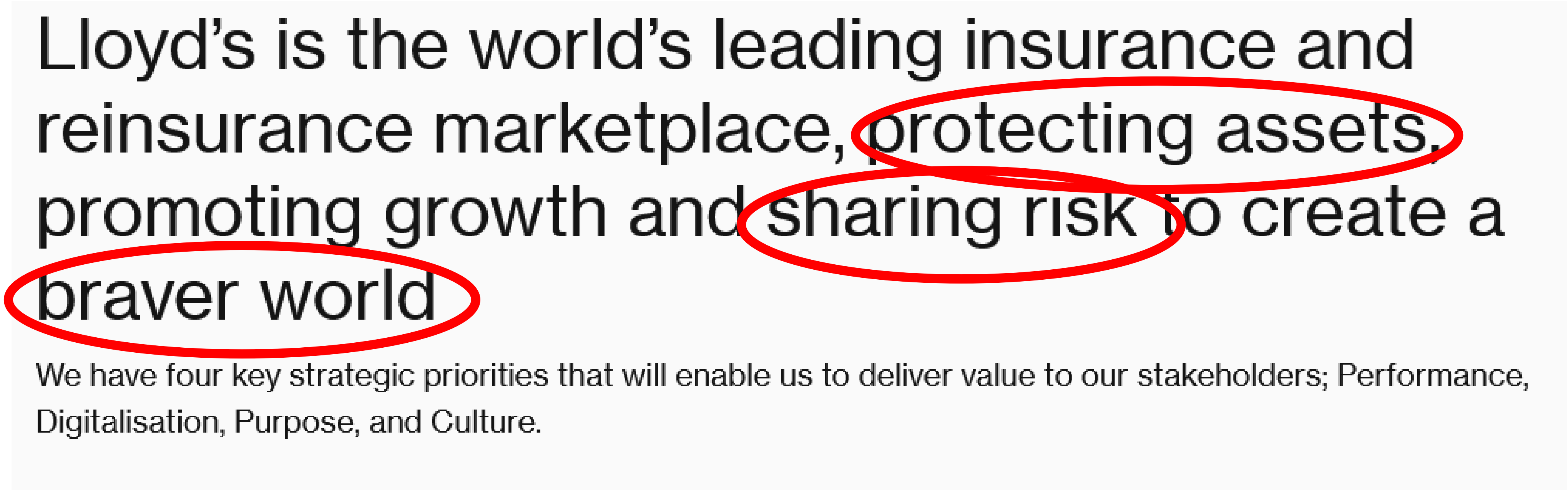
ISO 27001-13	
Total controls	16
Conform	8
Minor Non Conformity	6
Major Non Conformity	2

Priority	ISO 27001-13 Control	Level
1	4.4 Information security management system	Major Non Conformity
2	5.1 Leadership and commitment	Major Non Conformity
3	4.3 Determining the scope of the information security management system	Minor Non Conformity
4	9.1 Monitoring, measurement, analysis and evaluation	Minor Non Conformity
5	9.1 Monitoring, measurement, analysis and evaluation	Minor Non Conformity
6	9.2 Internal audit	Minor Non Conformity
7	9.2 Internal audit	Minor Non Conformity
8	10.2 Continual improvement	Minor Non Conformity
9	4.1 Understanding the organization and its context	Conform
10	5.2 Policy	Conform
11	5.2 Policy	Conform
12	5.3 Organizational roles, responsibilities and authorities	Conform
13	6.2 Information security objectives and planning to achieve them	Conform
14	7.1 Resources	Conform
15	7.4 Communication	Conform
16	8.3 Information security risk treatment	Conform

A tiered, comprehensive and output driven Cyber assessment

Templar Executives
Cyber Security Resilience For Business

Cyber Security – a Shared Endeavour



Lloyd's is the world's leading insurance and reinsurance marketplace, protecting assets, promoting growth and sharing risk to create a braver world

We have four key strategic priorities that will enable us to deliver value to our stakeholders; Performance, Digitalisation, Purpose, and Culture.

Governance: Why?

Templar Executives
Cyber Security Resilience For Business

Governing What: Information Assets

An Information asset is a body of information defined and managed so it can be understood, shared , protected and exploited effectively.

An information asset has a recognisable value, associated risk, content and lifecycle.

Common types of information assets:

- Personal/Sensitive Personal Data
- Business Critical Systems
- Commercial
- Intellectual Property
- Supplier Information

Templar Executives
Cyber Security Resilience For Business

‘Cyber’ – more than this

The Human Factor

95%*

Of data breaches in 2020 were caused by human error

IBM, Dec 2022

58%

Of organisations report that employees ignore cyber security guidelines

Compitech, 2022

Templar Executives
Cyber Security Resilience For Business

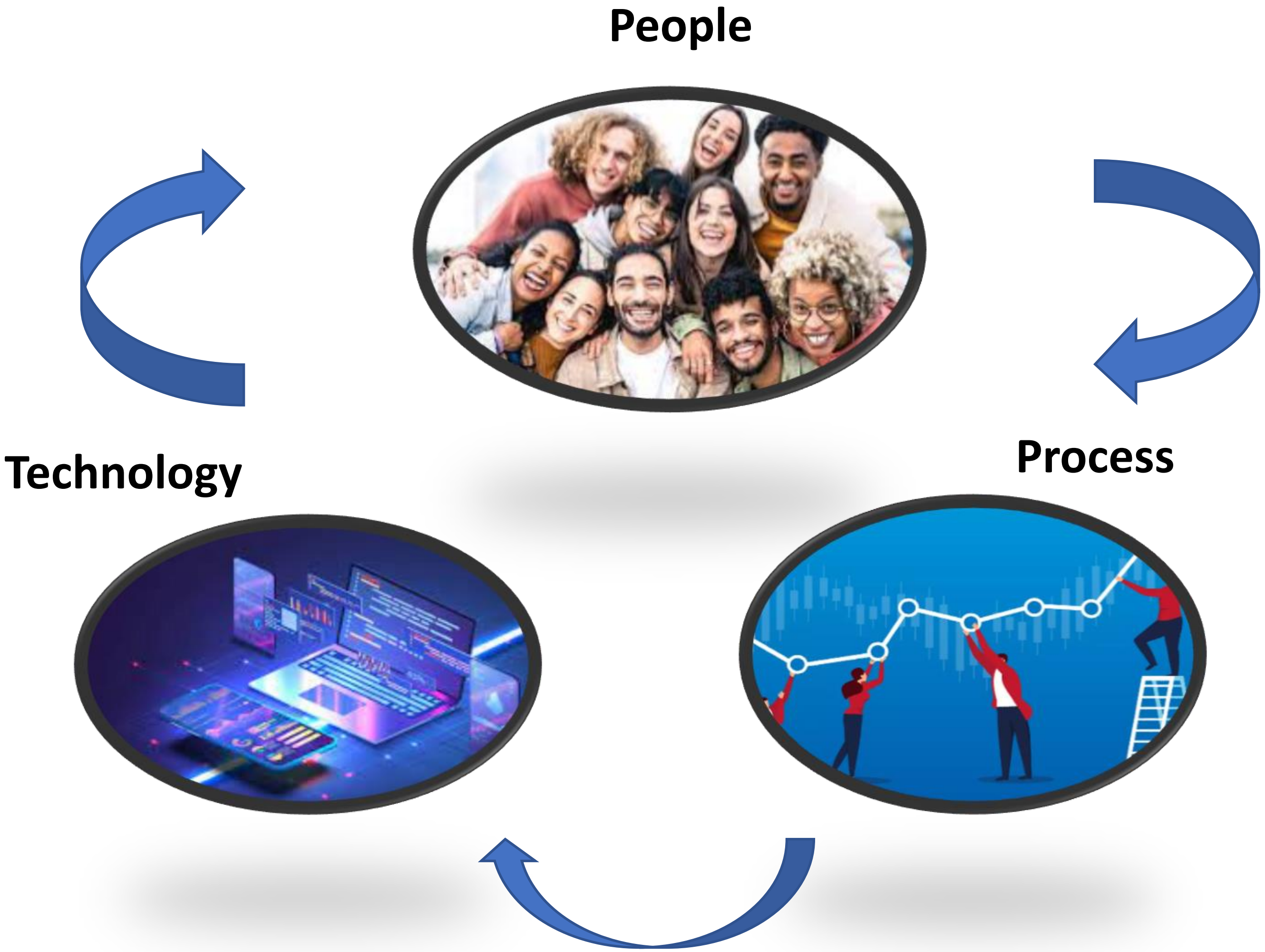
Governing How: Key Considerations

Ownership

Accountability

Engagement

Holistic Cyber Security: the Winning Combination



People

Process

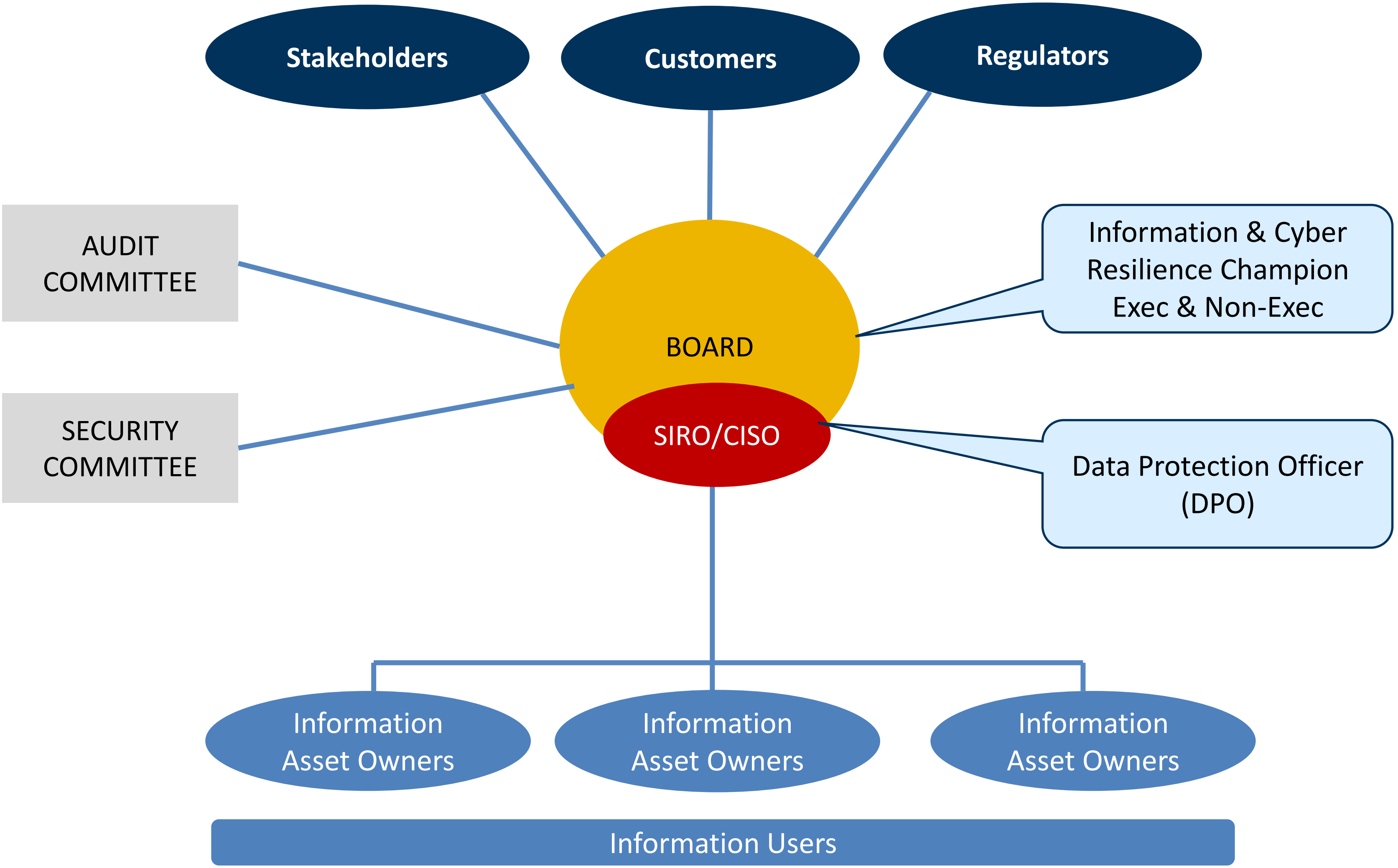
Technology

Accountability – the Big Ask

Cyber Security Means…

Templar Executives
Cyber Security Resilience For Business

Accountability – Governance Structure



Templar Executives
Cyber Security Resilience For Business

Ownership: The Senior Information Risk Owner (SIRO)

Own the overall information risk policy and risk assessment process, test its outcome, and ensure it is used.

Lead and foster a culture that values, protects and uses information for corporate good.

Advise on the information risk/set Risk Appetite aspects of business delivery within the organisation and throughout the supply chain.

Ownership: The Information Asset Owner

Risk and compliance

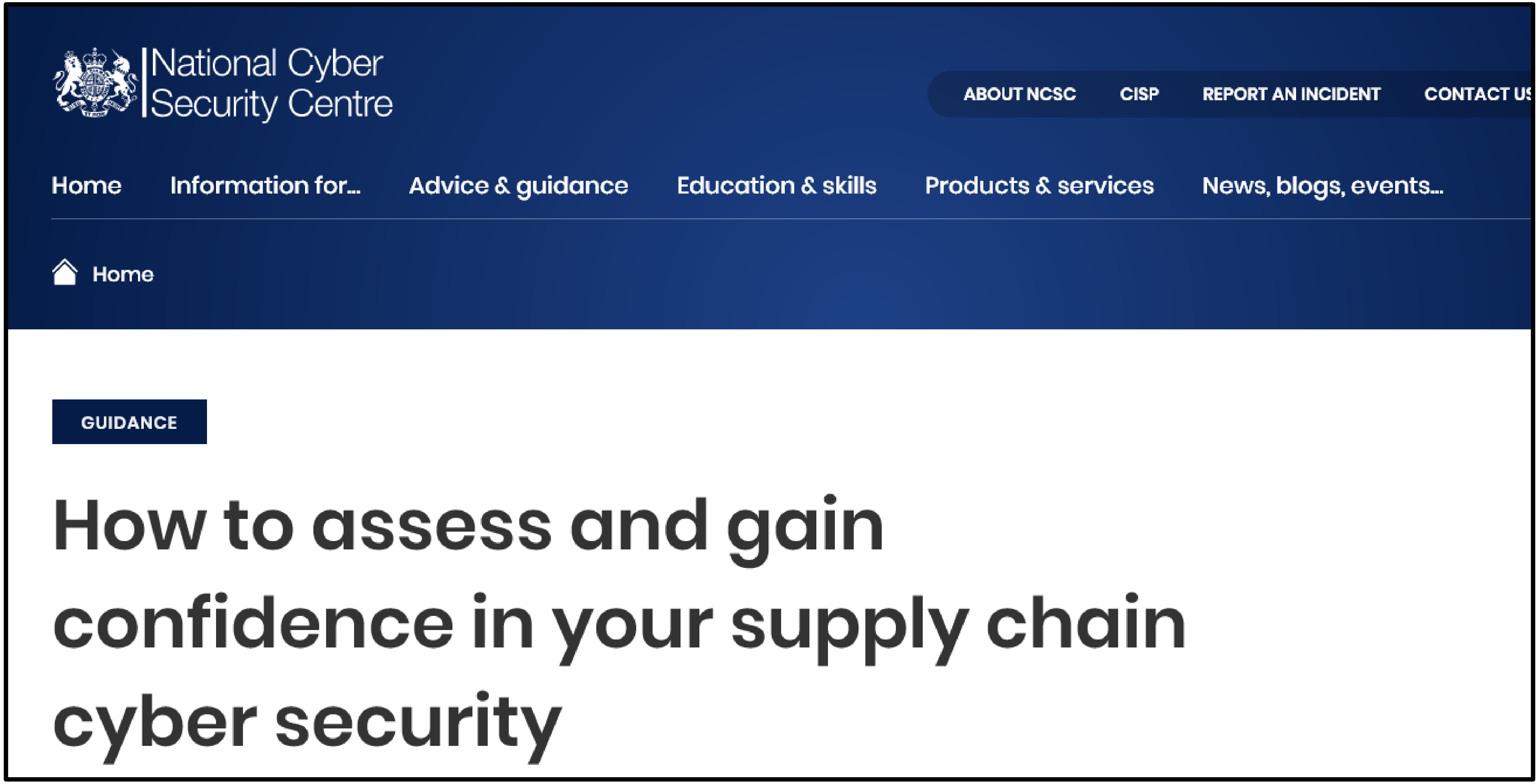
Access

Information Asset Owner

Skills and knowledge

Culture

Governance: Third Party Suppliers



GUIDANCE

How to assess and gain confidence in your supply chain cyber security

Accountability and Assurance: Standards Versus Maturity

Hard on the outside, soft on the inside: Favours a Standards Approach

Layered security: Favours a Maturity Approach

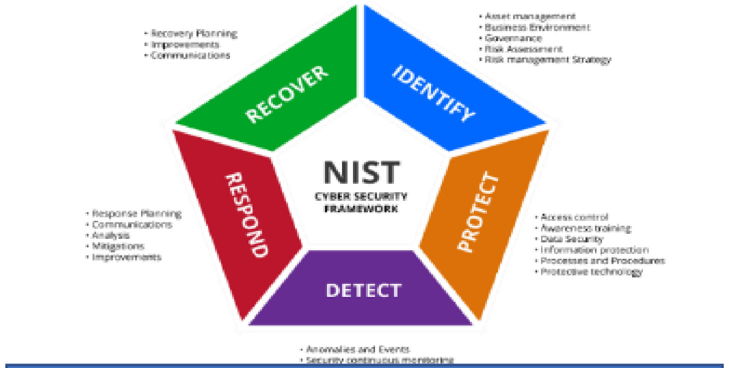
Assessment Tools

Key principles

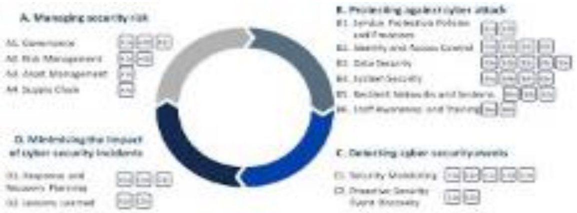
- Independent assessment preferable to self assessment
- Maturity based models identify baseline, gap and ambition
- Assessment should be against holistic criteria, not just technology based. Include:
  - Leadership and Governance
  - Enterprise Systems and Processes
  - Technology
  - People
  - Supply Chain
- Repeat to assess progress and inform strategy/plan

Assessment models

NIST

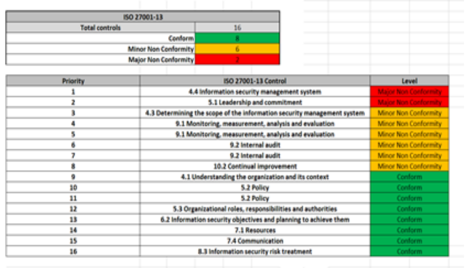


NCSC CAF 3



A. Managing security risk
A1. Governance
A2. Risk Management
A3. Asset Management
A4. Supply Chain
B. Protecting against cyber attack
B1. Service Protection Policies and Processes
B2. Identity and Access Control
B3. Data Security
B4. System Security
B5. Resilient Networks and Systems
B6. Staff Awareness and Training
C. Detecting cyber security events
C1. Security Monitoring
C2. Proactive Security Event Discovery
D. Minimising the impact of cyber security incidents
D1. Response and Recovery Planning
D2. Lessons Learned

Templar Executives CMAD



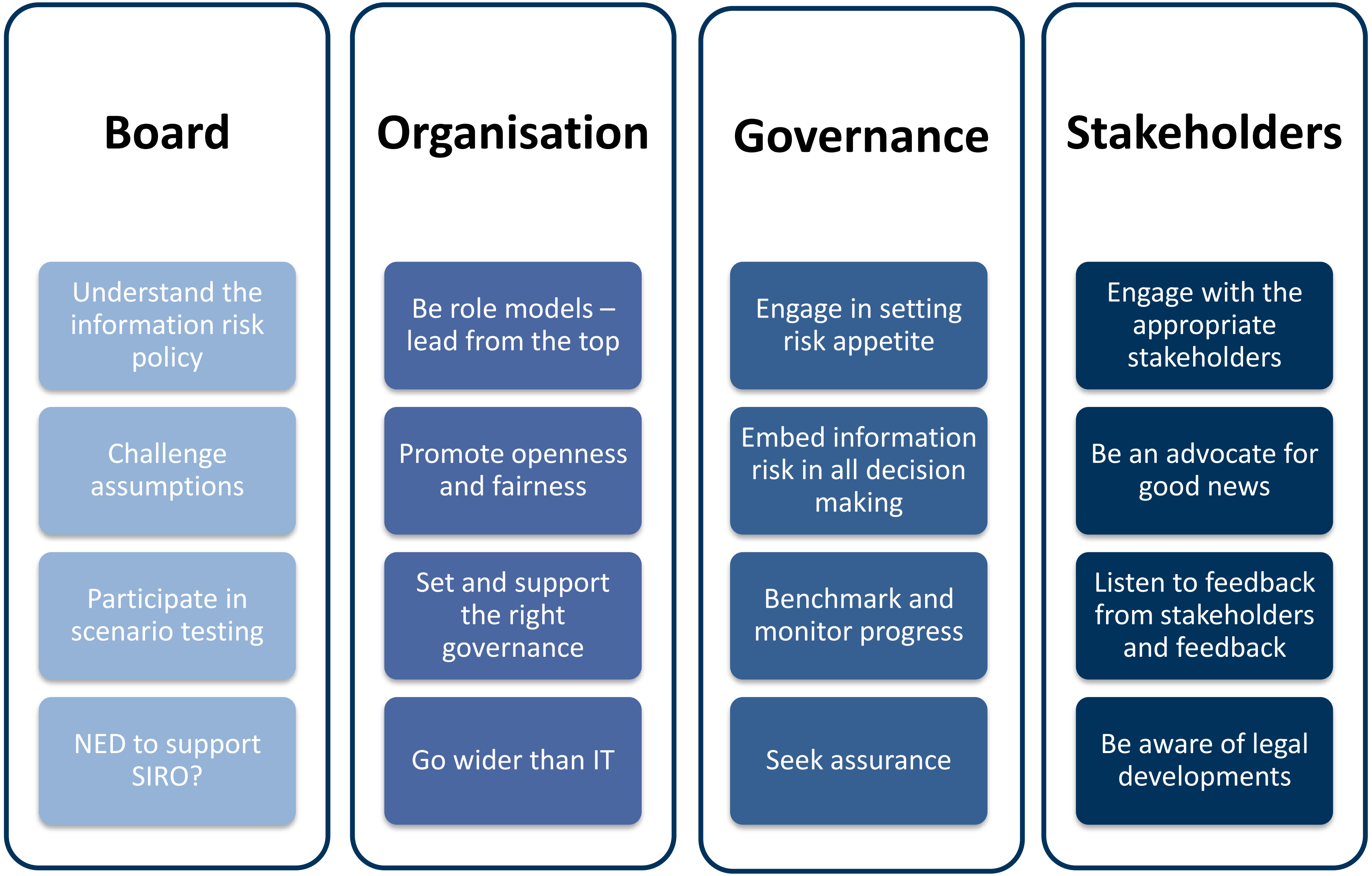
ISO 27001-13	
Total controls	16
Conform	8
Minor Non Conformity	6
Major Non Conformity	2

Priority	ISO 27001-13 Control	Level
1	4.4 Information security management system	Major Non Conformity
2	5.1 Leadership and commitment	Major Non Conformity
3	4.3 Determining the scope of the information security management system	Minor Non Conformity
4	9.1 Monitoring, measurement, analysis and evaluation	Minor Non Conformity
5	9.1 Monitoring, measurement, analysis and evaluation	Minor Non Conformity
6	9.2 Internal audit	Minor Non Conformity
7	9.2 Internal audit	Minor Non Conformity
8	10.2 Continual improvement	Minor Non Conformity
9	4.1 Understanding the organization and its context	Conform
10	5.2 Policy	Conform
11	5.2 Policy	Conform
12	5.3 Organizational roles, responsibilities and authorities	Conform
13	6.2 Information security objectives and planning to achieve them	Conform
14	7.1 Resources	Conform
15	7.4 Communication	Conform
16	8.3 Information security risk treatment	Conform

Templar Executives
Cyber Security Resilience For Business

Engagement

Engagement: How the Board can Support the SIRO

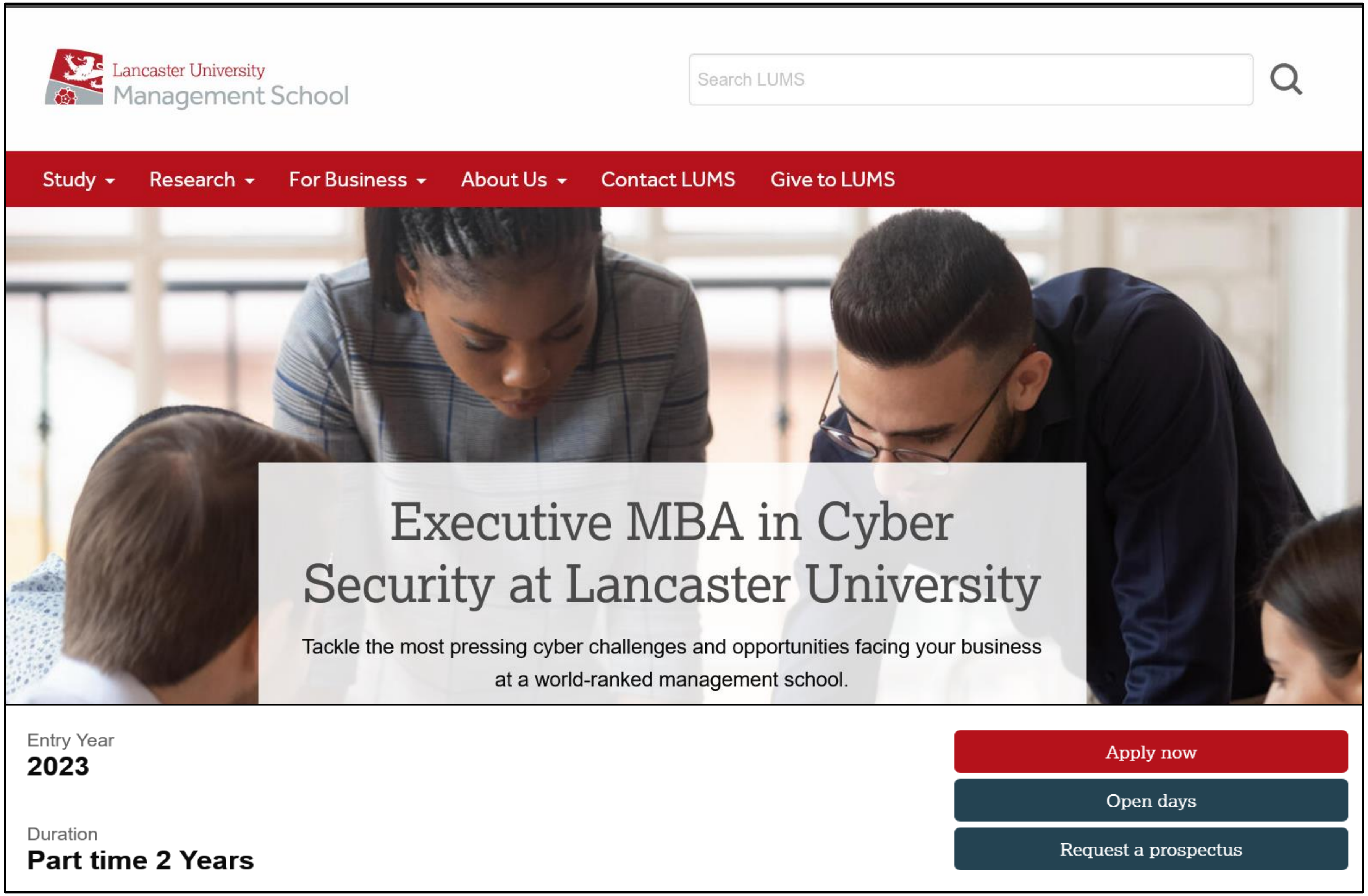


Board	Organisation	Governance	Stakeholders
Understand the information risk policy	Be role models – lead from the top	Engage in setting risk appetite	Engage with the appropriate stakeholders
Challenge assumptions	Promote openness and fairness	Embed information risk in all decision making	Be an advocate for good news
Participate in scenario testing	Set and support the right governance	Benchmark and monitor progress	Listen to feedback from stakeholders and feedback
NED to support SIRO?	Go wider than IT	Seek assurance	Be aware of legal developments

How Engaged are your IT People?

Templar Executives
Cyber Security Resilience For Business

For Your Own Front Line



Lancaster University Management School

Search LUMS

Executive MBA in Cyber Security at Lancaster University

Tackle the most pressing cyber challenges and opportunities facing your business at a world-ranked management school.

Entry Year
2023

Duration
Part time 2 Years

Further Resources

ico.
Information Commissioner's Office

National Cyber Security Centre
Search
Guidance | Threats | Incident Management | Marketplace | Education & Research | Insight | Press & Media

The National Cyber Security Centre

Helping to make the UK the safest place to live and do business online

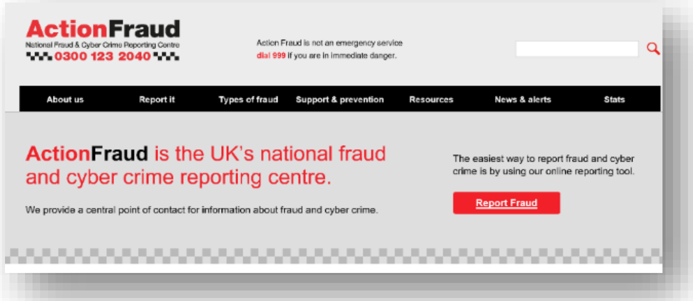
National Cyber Security Centre
a part of GCHQ

NCSC CAF guidance

The Cyber Assessment Framework (CAF) provides guidance for organisations responsible for vitally important services and activities.

cro forum

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY



Action Fraud is not an emergency service
dial 999 if you are in immediate danger.

ActionFraud is the UK's national fraud and cyber crime reporting centre.

We provide a central point of contact for information about fraud and cyber crime.

The easiest way to report fraud and cyber crime is by using our online reporting tool.

CYBER ESSENTIALS

Templar Executives: Further Support, including…

Leadership and Governance

- Board Training
- Support to develop/refresh Cyber Security Strategy
- Executive mentoring
- Review of Board level policies
- NCSC Certified SIRO Training
- SIRO mentoring and support
- NCSC Certified IAO workshop
- NCSC Certified IAO elearning
- Cyber Awareness for Procurement teams and Contract Managers
- IG Suite of elearning e.g. GDPR/DPA 2018, DPIAs, SARs, FOI, Records Management

Operational / Technical

- Cyber Security Awareness training e.g. NCSC Cyber Security and Hybrid Working
- Cyber Essentials Plus Guidance
- Review/Support: processes and technology for sharing information; network segregation; secure configuration; patch management; logging solutions; Enterprise Architecture; Technical Design Authority
- Cyber Security training for roles/transformation programmes; Cyber Security elearning for IT, HR, Finance, Procurement, Comms
- Incident Management, Business Continuity and Crisis Exercises

Templar Executives
Cyber Security Resilience For Business

Thank You

Templar Executives
Cyber Security Resilience For Business

enquiries@templarexecs.com

Tel: 020 3542 9075
83, Victoria Street, London, SW1H 0HW

http://www.templarexecs.com

@templarexecs