Building an Information Security Strategy

Darren Kewley
Technical Director & Head of Security Services

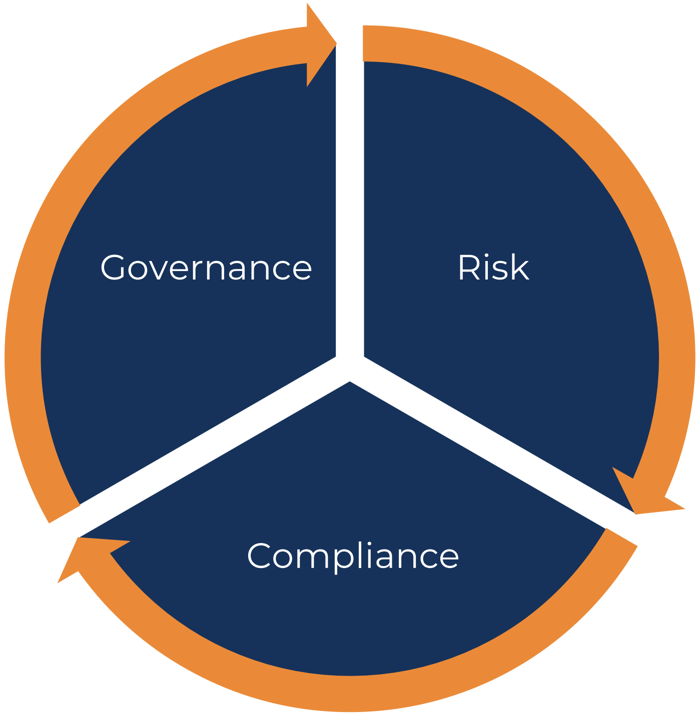
protos NETWORKS

Agenda

- GRC
- InfoSec Governance
- Managing Risk
- Compliance & Frameworks
- Organisational and Technical Controls
- When Things Go Wrong

Governance, Risk & Compliance

- GRC is not just a framework for IT or Information Security.
- It helps boards and leaders manage their organisations.
- Ensures that they take reasonable care in areas including finance, legal, health and safety, data protection and information security.
- **Governance**: making and enforcing decisions in an organisation.
- **Risk**: understanding current and future risks.
- **Compliance**: structures to ensure the organisation conforms to internal controls and external rules and regulations.
- Let's look at this in an information security context...



Governance

Business Alignment

- Security strategy aligns with business strategy and needs
- Stakeholders understand the importance of security information
- Everybody works together to achieve goals

Roles & Responsibilities

- Board-level accountability
- Day-to-day management of security
- Committees, groups, etc.
- Dispute resolution
- Employee responsibilities

Policies

- What are our policies (BYOD, access control, etc.)?
- Policy review and approval
- Policy realisation
- Dealing with breaches of security policies

Risk Appetite

- Who sets risk appetite?
- What are our security priorities?
- What risks should be minimised?
- What risks are acceptable?

Planning

- Security objectives
- Budgetary planning
- Monitoring and auditing compliance

Data Protection

- Does this fall within InfoSec GRC?
- What is our exposure to Data Protection risks?
- Do we need a DPO?

Managing Risk

Asset Management

Risk Assessments

Threat Modelling

Supply Chain Risks

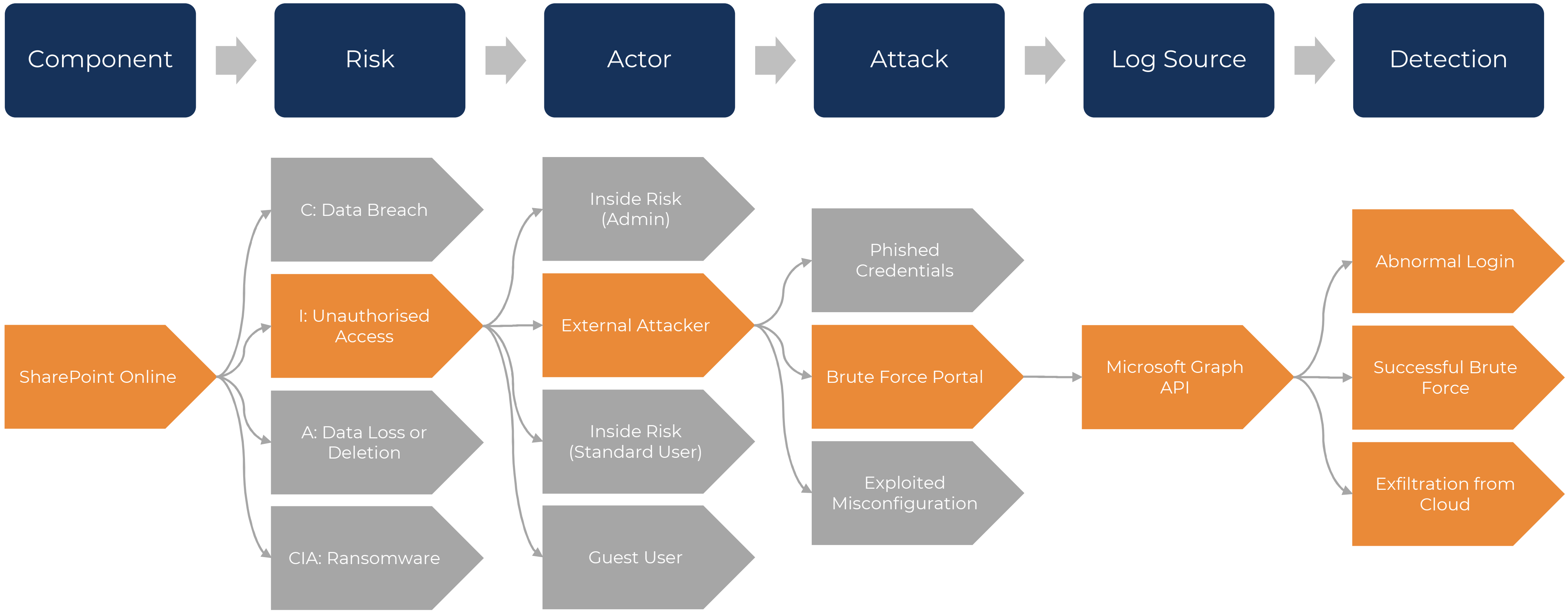
Assessing Risk

Asset	Threat / Vulnerability	Current Likelihood	Current Impact	Score (L x I)	Treatment Approach	Treatment Plan	Residual Scoring
SharePoint Online	(C): Breach due to poor access controls	4	4	16	Mitigate	Enable MFA and Zero Trust Controls	2 x 4 = 8 Low

Confidentiality
Integrity
Availability

		Impact				
		1 Negligible	2 Small	3 Moderate	4 Major	5 Catastrophic
Likelihood	5 Very Likely	5 Low	10 Medium	15 Medium	20 High	25 High
	4 Likely	4 Low	8 Low	12 Medium	16 Medium	20 High
	3 Possible	3 Low	6 Low	9 Medium	12 Medium	15 Medium
	2 Unlikely	2 Low	4 Low	6 Low	8 Low	10 Medium
	1 Very Unlikely	1 Low	2 Low	3 Low	4 Low	5 Low

Threat Modelling (SOC)



Component → Risk → Actor → Attack → Log Source → Detection

SharePoint Online

C: Data Breach

I: Unauthorised Access

A: Data Loss or Deletion

CIA: Ransomware

Inside Risk (Admin)

External Attacker

Inside Risk (Standard User)

Guest User

Phished Credentials

Brute Force Portal

Exploited Misconfiguration

Microsoft Graph API

Abnormal Login

Successful Brute Force

Exfiltration from Cloud

Source: NCSC
https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/onboarding-systems-and-log-sources/threat-modelling

Compliance

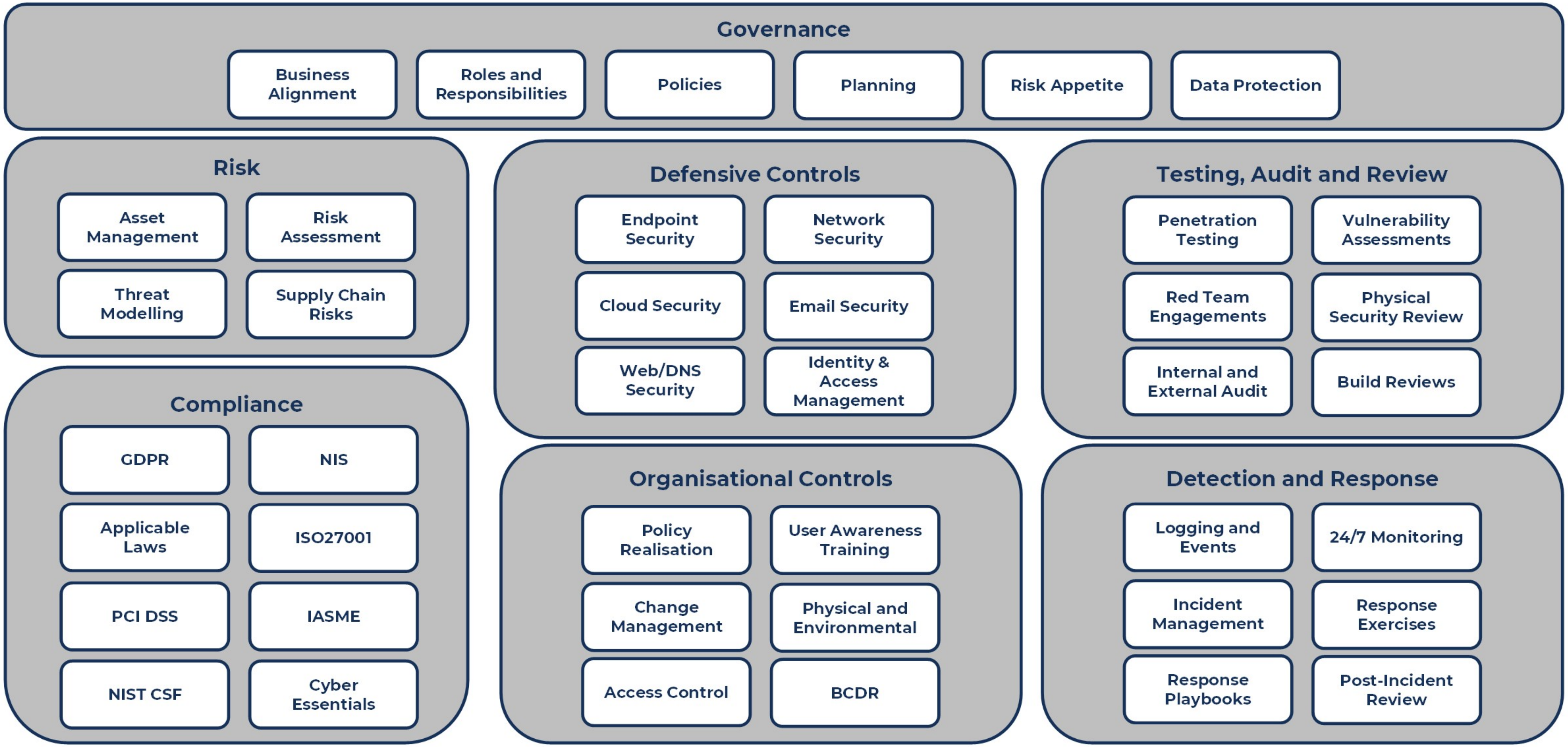
Legal and Regulatory Landscape

- GDPR
- PECR
- NIS Regulations
- Computer Misuse Act
- Malicious Comms Act
- Copyright Regulations
- Companies Act
- Malicious Comms Act
- RIPA

Frameworks and Certifications

- ISO27001
- PCI DSS
- IASME Cyber Assurance
- Cyber Essentials
- NIST CSF
- NHS DSP Toolkit
- NCSC CAF
- IoTSF
- MITRE ATT&CK

GRC



Governance

- Business Alignment
- Roles and Responsibilities
- Policies
- Planning
- Risk Appetite
- Data Protection

Risk

- Asset Management
- Risk Assessment
- Threat Modelling
- Supply Chain Risks

Compliance

- GDPR
- NIS
- Applicable Laws
- ISO27001
- PCI DSS
- IASME
- NIST CSF
- Cyber Essentials

Defensive Controls

- Endpoint Security
- Network Security
- Cloud Security
- Email Security
- Web/DNS Security
- Identity & Access Management

Organisational Controls

- Policy Realisation
- User Awareness Training
- Change Management
- Physical and Environmental
- Access Control
- BCDR

Testing, Audit and Review

- Penetration Testing
- Vulnerability Assessments
- Red Team Engagements
- Physical Security Review
- Internal and External Audit
- Build Reviews

Detection and Response

- Logging and Events
- 24/7 Monitoring
- Incident Management
- Response Exercises
- Response Playbooks
- Post-Incident Review

When Things Go Wrong

- In 2018, British Airways suffered a cyber-attack that exploited multiple vulnerabilities and breached 400,000 data records, including credit card information.
- The initial attack vector was via compromised supplier Citrix accounts.
- There was no MFA on Citrix, even though BA's policies stated it must be.
- The organisation said it had risk-assessed its Citrix environment – but nobody could locate the risk assessment during the ICO's investigation.
- BA didn't detect any element of the attack. A third party informed them that card payments were being redirected.
- **Governance** failed as the organisation did not manage its **risk**. As such, it failed in its **compliance** obligations.
- The ICO fined BA £20m; however, this fine was reduced due to Covid. The initial fine was £184m.

BRITISH AIRWAYS

Questions?