First published in 2026 by UE Campus

Unit specifications can be found on the UE Campus Portal: https://uecampus.com/

Contents

Using your Study Guide

Welcome to the study guide, designed to support you in completing your Level 4 Diploma in Cyber Security.

This study guide follows the order of the syllabus, which is the basis for your studies. Each chapter starts by listing the syllabus learning outcomes covered and the assessment criteria.

Level 4 Units

The Level 4 Diploma in Cyber Security consists of the following units:

Unit Title	Credits	Status
Cyber Security Threat and Risk	20	Mandatory
Network Security and Data Communications	20	Mandatory
Database Security and Computer Programming	20	Mandatory
Incident Response, Investigations and Forensics	20	Mandatory
Security Strategy: Laws, Policies and Implementation	20	Mandatory
Cyber Security Threats and Risk: Banking and Finance	20	Optional
Cyber Wars	20	Optional

The study guide includes a number of features to enhance your studies:

📝	**'Over to you:'** activities for you to apply what you have learned.
🌎	**'Industry Insights:'** discover up-to-date trends, expert opinions, and real-world examples.
🧭	**'Did you know?'** highlights interesting facts or surprising information.
💼	**'Case studies:'** realistic business scenarios to reinforce and test your understanding.
❗	**'Need to know:'** key pieces of information highlighted in the text.
💡	**'Examples:'** illustrating points made in the text to show how it works in practice.

Note: Website addresses current as of March 2026.

Level 4 Security Strategy: Laws, Policies and Implementation

About this unit

Knowing how to build a cyber defence strategy, what legal tools require consideration, and how policies can be written and embedded are all vital ingredients to successful in-house cyber security practices. This unit brings together knowledge acquired from previous units and builds on it in relation to developing plausible strategic plans, securing executive buy-in, and achieving legal compliance.

This unit poses key questions that every cyber security professional must be able to answer: What is 'strategy' and what can a cyber security strategy look like? How do we achieve senior-level buy-in for security investments? How do we monitor and safeguard compliance, particularly if our operations are dispersed across a multinational environment? What are the key legal requirements and industry standards that can assist and enhance our cyber security strategies and practices?

By the end of this unit, you will be able to assess the value of strategic management for cyber security, evaluate legislation and standards, assess training and accreditation schemes, design and implement PDCA-based security policies, investigate international approaches to information security, and design security audit plans that reflect the legal and political environment.

Unit code: **A/617/1133**

RQF level: **4**

Credits: **20**

Assessment: **Written Assignment – Cyber Security Strategy and Policy Framework Report**

Chapter One – Strategy, Strategic Management and Cyber Security

Introduction

This chapter explores the concept of strategy and strategic management as applied to information security and cyber-enabled business environments. Cyber security can no longer be treated as a purely technical function delegated to the IT department – it is a strategic business imperative that requires board-level attention, alignment with business objectives, and integration into the organisation's overall governance framework.

You will examine what 'strategy' means in the context of cyber security, how to develop a comprehensive cyber security strategy, and critically, how to achieve the senior-level buy-in necessary to secure resources and embed security throughout the organisation. The chapter draws on established strategic management frameworks and applies them specifically to the cyber security domain.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand the concept of strategy, strategic management, planning and buy-in in relation to cyber security.**

Assessment Criteria

1.1 Assess the value of strategic management and planning as applied to information security and cyber-enabled business environments.

1.1 Strategic management and planning for cyber security

Over to you – Video Watch: Cyber Security Strategy

Watch these videos:

Video 1: What is Cyber Security Strategy? – SANS Institute

Link: https://youtu.be/vnyUECXz6JA?si=PdCi6K5jfY5l1cNs

Video 2: How to Get Executive Buy-In for Security – CISO Series

Link: https://youtu.be/JxJ4wYtk2qc?si=Z4M61gfLITgmdOZG

After watching both, answer: What distinguishes a cyber security strategy from a list of security tools? Why do CISOs struggle to gain board-level support, and what can they do about it?

What is Strategy?

Strategy, derived from the Greek word 'strategos' (meaning 'general'), is the art and science of planning and directing large-scale operations toward desired outcomes. In a business context, strategy is the set of decisions and actions that determine the long-term direction and scope of an organisation. Henry Mintzberg identified five definitions of strategy (the 5 Ps): Plan (a consciously intended course of action), Ploy (a manoeuvre to outwit competitors), Pattern (a consistent pattern of behaviour over time), Position (the

organisation's place in its environment), and Perspective (the organisation's fundamental way of doing things).

Michael Porter's competitive strategy framework, the resource-based view of the firm, and balanced scorecard methodology all provide lenses through which cyber security strategy can be understood. A cyber security strategy is not simply a technical plan for deploying security tools – it is a business strategy that aligns security investments with organisational objectives, risk appetite, and stakeholder expectations.

! Need to know – What a Cyber Security Strategy Looks Like

A comprehensive cyber security strategy typically includes the following components:

1. Vision and objectives – what the organisation aims to achieve through its security programme. 2. Scope – which systems, data, people, and processes are covered. 3. Current state assessment – an honest evaluation of the current security posture, including maturity assessments and gap analyses. 4. Risk assessment – identification and prioritisation of cyber risks aligned with business objectives. 5. Strategic priorities – the key areas of focus for the strategy period (typically 3-5 years). 6. Governance framework – roles, responsibilities, and accountability structures. 7. Resource plan – budget, staffing, and technology investments. 8. Implementation roadmap – phased plan with milestones and deliverables. 9. Metrics and KPIs – how success will be measured. 10. Review and update mechanisms – how the strategy will evolve over time.

Strategic Management Frameworks Applied to Cyber Security

Several established strategic management frameworks can be applied to cyber security planning:

- **SWOT Analysis** – assessing the organisation's Strengths (existing security capabilities, skilled staff, mature processes), Weaknesses (gaps in defences, skills shortages, legacy systems), Opportunities (emerging technologies, regulatory changes that incentivise investment), and Threats (evolving threat landscape, new attack vectors, geopolitical risks). SWOT provides a structured approach to situational analysis.
- **PESTLE Analysis** – examining the Political (government cyber strategies, geopolitical tensions), Economic (budget constraints, cost of cyber crime), Social (remote working trends, security awareness culture), Technological (cloud adoption, AI, IoT), Legal (GDPR, NIS Regulations, sector-specific requirements), and Environmental (data centre sustainability, climate-related business disruption) factors that influence cyber security strategy.
- **Balanced Scorecard** – translating strategy into measurable objectives across four perspectives: Financial (return on security investment, cost of breaches avoided), Customer (trust, service availability, data protection), Internal Processes (incident response time, patch management compliance, vulnerability remediation rate), and Learning and Growth (staff training, certification rates, innovation).
- **Porter's Five Forces** – analysing competitive pressures including the threat of new cyber threats, the bargaining power of security vendors, the availability of substitute security solutions, the intensity of the threat landscape, and the potential for new threat actors.
- **Maturity models** – frameworks such as the NIST Cybersecurity Framework, CMMI (Capability Maturity Model Integration), and the C2M2 (Cybersecurity Capability Maturity Model) provide structured approaches for assessing and improving an

organisation's security maturity from initial (ad hoc) through to optimising (continuous improvement).

Achieving Senior-Level Buy-In

One of the greatest challenges facing cyber security leaders is securing executive and board-level support for security investments. Without senior buy-in, security programmes lack adequate resources, authority, and organisational commitment. Strategies for achieving buy-in include:

- **Speak the language of business** – frame security in terms of business risk, not technical jargon. Instead of 'we need a next-generation firewall', say 'we need to reduce the risk of a customer data breach that could cost £5 million and damage customer trust.' Quantify risks in financial terms wherever possible.
- **Align with business objectives** – demonstrate how the security strategy supports the organisation's strategic goals. If the business is expanding into new markets, show how security enables safe digital transformation. If the business is focused on customer trust, show how security protects the brand.
- **Use risk quantification** – methodologies such as FAIR (Factor Analysis of Information Risk) enable cyber risks to be expressed in financial terms that executives and board members can understand and compare with other business risks. Risk quantification transforms security from a cost centre into a risk management function.
- **Leverage regulatory requirements** – regulatory obligations (GDPR, NIS Regulations, PCI DSS, FCA requirements) provide a compelling case for security investment. Non-compliance carries defined penalties that can be compared with the cost of compliance.
- **Present peer comparisons** – benchmarking against industry peers and demonstrating where the organisation's security maturity lags behind competitors can create urgency. Industry reports and benchmarking studies provide useful reference points.
- **Report on metrics and trends** – regular, concise security reporting to the board builds awareness and accountability over time. Dashboards showing key risk indicators, incident trends, and programme progress keep security visible at the executive level.

Industry Insight – The CISO's Seat at the Board Table

Research consistently shows that organisations where the CISO has direct access to the board achieve better security outcomes. A 2023 Gartner survey found that by 2026, 70% of boards will include a member with cyber security expertise. The UK Government's Cyber Governance Code of Practice (2024) explicitly states that boards should ensure cyber security risks are integrated into their existing governance structures and treated with the same rigour as financial and legal risks. This shift from viewing cyber security as an IT issue to a board-level governance responsibility represents a fundamental change in how organisations approach security strategy.

Read more: https://www.gov.uk/government/publications/cyber-governance-code-of-practice

Case Study – Uber's Security Strategy Failures (2016-2022)

Uber's security history illustrates the consequences of poor security strategy and governance. In 2016, Uber suffered a data breach affecting 57 million users and drivers. Rather than disclosing the breach as required by law, Uber's Chief Security Officer paid the hackers $100,000 to delete the stolen data and keep the breach quiet. The cover-up was discovered in 2017, leading to the CSO's criminal prosecution and conviction in 2022 – the first time a senior executive was personally convicted for concealing a data breach.

In September 2022, Uber was breached again when a teenage hacker used social engineering to compromise an employee's MFA-protected account. The attacker gained broad access to internal systems including source code repositories, Slack, and financial dashboards. The breach revealed that Uber had not adequately addressed the systemic security governance failures exposed by the 2016 incident.

Task: (1) Analyse the strategic failures that led to both breaches. (2) How did the lack of board-level security governance contribute? (3) What are the legal and ethical implications of concealing a breach? (4) Design a five-point strategic improvement plan for Uber's security programme following the 2022 breach. (5) What lessons can other organisations learn about the relationship between security strategy and corporate culture? Write a comprehensive 800-word analysis.

Did you know?

The UK Government's National Cyber Strategy 2022 set out a five-year plan to make the UK a leading responsible and democratic cyber power. The strategy's five pillars are: strengthening the UK cyber ecosystem, building resilience, taking the lead in securing emerging technologies, advancing UK global leadership, and detecting, disrupting, and deterring adversaries. This national-level strategy provides context for organisational cyber security strategies, which should align with and be informed by national priorities.

Over to you – Strategy Development Exercise

You are the newly appointed CISO of a mid-sized online retailer (500 employees, £150 million annual revenue, primarily online sales). The company has experienced rapid growth but has invested minimally in cyber security. The board has asked you to develop a 3-year cyber security strategy. Prepare a 1,000-word executive summary covering: (a) a SWOT analysis of the company's current security position, (b) three strategic priorities for each year, (c) a governance framework, (d) estimated budget requirements, (e) key metrics and KPIs, and (f) how you would present this to the board for approval.

Reading List

- Johnson, G., Whittington, R., Angwin, D., Regnr, P. and Scholes, K. (2023) *Exploring Strategy: Text and Cases.* 13th edn. Harlow: Pearson.
- Kaplan, R.S. and Norton, D.P. (2023) *The Balanced Scorecard: Translating Strategy into Action.* 2nd edn. Boston, MA: Harvard Business Review Press.
- Hubbard, D.W. and Seiersen, R. (2023) *How to Measure Anything in Cybersecurity Risk.* 2nd edn. Hoboken, NJ: Wiley.

- Creasey, J. (2022) *Cyber Security Strategy: An Executive Guide.* Ely: IT Governance Publishing.
- UK Government (2022) *National Cyber Strategy 2022.* London: HMSO. Available at: https://www.gov.uk/government/publications/national-cyber-strategy-2022 (Accessed: 15 March 2026).
- NCSC (2024) *Board Toolkit: Five Questions for Your Board's Agenda.* London: NCSC. Available at: https://www.ncsc.gov.uk/collection/board-toolkit (Accessed: 15 March 2026).

Summary

In this chapter, you have explored the concept of strategy and strategic management as applied to cyber security. You have examined frameworks including SWOT, PESTLE, the Balanced Scorecard, and maturity models, and applied them to cyber security planning. You have analysed the critical challenge of achieving senior-level buy-in, including strategies for communicating security risk in business terms, and have studied the consequences of poor security governance through the Uber case study. These foundations set the stage for the legislative, standards, and policy frameworks examined in the following chapters.

Chapter Two – Legislation, Standards, Training and Accreditations

Introduction

This chapter evaluates the legislative landscape and industry standards that impact and assist cyber security planning, and assesses the key training and accreditation schemes available to cyber security professionals and organisations. Legislation and standards provide both obligations and guidance – they define what organisations must do and provide frameworks for how to do it effectively.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand how legislation, formal industry standards, training and accreditations support cyber security.**

Assessment Criteria

2.1 Evaluate key legislation and industry standards that impact and assist cyber security planning.

2.2 Assess the key training and accreditation schemes relating to cyber security.

2.1 Key legislation and industry standards

UK and International Legislation

Legislation	Impact on Cyber Security Planning
UK GDPR / DPA 2018	The most significant data protection legislation. Requires organisations to implement 'appropriate technical and organisational measures' to protect personal data. Mandates 72-hour breach notification to the ICO. Introduces Data Protection by Design and Default. Fines up to £17.5 million or 4% of global annual turnover. Requires Data Protection Impact Assessments (DPIAs) for high-risk processing.
NIS Regulations 2018 (updated 2022)	Implements the EU Network and Information Security Directive in the UK. Applies to Operators of Essential Services (OES) in sectors including energy, transport, health, water, and digital infrastructure, and to Relevant Digital Service Providers (RDSPs). Requires risk management measures and incident reporting. Competent authorities can impose fines up to £17 million.
Computer Misuse Act 1990	Criminalises unauthorised access to computer systems. Three main offences with penalties up to life imprisonment (for attacks on CNI, following 2015 amendments). Directly relevant to security strategy as it defines the legal boundaries of authorised security testing.

Telecommunications (Security) Act 2021	Imposes security duties on UK telecoms providers and gives Ofcom enforcement powers. Relevant for organisations providing or using telecoms services. Mandates specific security standards and incident reporting.
Product Security and Telecommunications Infrastructure Act 2022	Requires manufacturers of IoT devices to meet minimum security requirements, including banning default passwords, providing a vulnerability disclosure policy, and being transparent about security update periods. A significant development for supply chain security.
Online Safety Act 2023	Imposes duties on online platforms to protect users from harmful content and illegal activity. Includes provisions for end-to-end encryption and law enforcement access that have significant implications for privacy and security.
Cyber Security and Resilience Bill 2025	Proposed legislation to update the NIS Regulations, expanding scope to more organisations, strengthening incident reporting requirements, and giving regulators more flexibility to respond to the evolving threat landscape.

Industry Standards and Frameworks

- **ISO/IEC 27001:2022** – the international standard for Information Security Management Systems (ISMS). Provides a systematic approach to managing information security through a risk-based framework. ISO 27001 is certifiable, providing external validation of an organisation's security management. The 2022 revision updated the Annex A controls to reflect modern threats and technologies including cloud security, threat intelligence, and secure coding.
- **ISO/IEC 27002:2022** – the companion to ISO 27001, providing detailed guidance on implementing the 93 controls organised into four themes: Organisational, People, Physical, and Technological. Essential reference for security policy development.
- **NIST Cybersecurity Framework 2.0** – the six-function framework (Govern, Identify, Protect, Detect, Respond, Recover) providing a common language and structured approach to cyber security. Widely adopted beyond US government agencies.
- **PCI DSS v4.0** – the Payment Card Industry Data Security Standard, mandatory for organisations that process, store, or transmit cardholder data. PCI DSS v4.0 (2022) introduced more flexible approaches while strengthening requirements for authentication and encryption.
- **Cyber Essentials / Cyber Essentials Plus** – the UK Government-backed certification scheme providing a baseline of cyber security for organisations of all sizes. Cyber Essentials covers five key controls: firewalls, secure configuration, user access control, malware protection, and security update management. Cyber Essentials Plus includes a hands-on technical verification. Mandatory for many government contracts.
- **SOC 2 (Service Organisation Control 2)** – an auditing framework developed by AICPA for service organisations, evaluating security, availability, processing integrity, confidentiality, and privacy controls. Increasingly required by customers of cloud service providers.
- **CIS Controls v8.1** – a prioritised set of 18 security controls developed by the Center for Internet Security, organised into three Implementation Groups based on organisational size and resources.

Example – Mapping Standards to Regulatory Requirements

A UK financial services company needs to comply with UK GDPR, NIS Regulations, PCI DSS, and FCA requirements. Rather than treating each as a separate compliance exercise, the company implements ISO 27001 as its overarching ISMS framework and maps the specific requirements of each regulation to ISO 27001 controls. This approach eliminates duplication, reduces audit fatigue, and provides a single coherent security management framework. For example, the ISO 27001 control for access management satisfies requirements in GDPR (Article 32), PCI DSS (Requirement 7), NIS Regulations (security measures), and FCA (SYSC 13 operational risk management).

Over to you – Compliance Mapping Exercise

Select an industry sector (e.g. healthcare, financial services, retail, or education). Identify the three most important cyber security regulations and standards for that sector. Create a compliance mapping matrix showing how ISO 27001 controls address the requirements of each regulation. Identify any gaps where ISO 27001 alone is insufficient and recommend additional controls. Present your analysis as a 600-word report.

2.2 Training and accreditation schemes

Professional Certifications

Certification	Provider	Focus and Level
CompTIA Security+	CompTIA	Entry-level security certification covering threats, vulnerabilities, tools, and technologies. Vendor-neutral. Often a baseline requirement for security roles.
CISSP	(ISC)²	The gold standard for experienced security professionals. Covers eight domains including security management, risk management, and governance. Requires 5 years of experience.
CISM	ISACA	Focused on security management and governance. Four domains: governance, risk management, programme development, and incident management. Requires 5 years management experience.
CISA	ISACA	Information systems audit certification. Five domains covering audit processes, IT governance, information systems acquisition, and operations. Essential for security auditors.
CEH	EC-Council	Certified Ethical Hacker. Covers penetration testing tools and techniques. Validates offensive security skills.

GIAC Certifications	SANS Institute	Specialised certifications across multiple domains: GSEC (Security Essentials), GCIH (Incident Handler), GCFE (Forensic Examiner), GPEN (Penetration Tester), and many more.
Cyber Essentials Assessor	IASME	Qualification to assess organisations against the Cyber Essentials scheme. Relevant for those in consultancy and audit roles.
NCSC Certified Degrees	NCSC	UK university degrees certified by the NCSC as meeting a defined standard of cyber security education. Available at Bachelor's, Master's, and Integrated Master's levels.

Organisational Accreditation Schemes

- **ISO 27001 certification** – organisations can be independently audited and certified against ISO 27001 by accredited certification bodies. Certification demonstrates to customers, regulators, and stakeholders that the organisation has implemented a mature ISMS.
- **Cyber Essentials certification** – the UK Government's baseline certification scheme. Increasingly required for government contracts and used as a minimum security benchmark across sectors.
- **SOC 2 Type II reports** – independent audit reports that verify an organisation's controls over an extended period (typically 6-12 months). Increasingly demanded by enterprise customers of SaaS and cloud service providers.
- **CREST membership** – the Council for Registered Ethical Security Testers accredits organisations providing penetration testing, incident response, and threat intelligence services. CREST accreditation is often required for government and regulated sector work.

Over to you – Career Path Planning Activity

Research three different career paths in cyber security (e.g. security analyst, penetration tester, security architect, CISO, forensic investigator, compliance officer). For each path: (a) identify the typical certifications required at each stage (entry, mid-career, senior), (b) estimate the average salary in the UK, (c) describe the key skills needed beyond technical knowledge, and (d) identify one professional body or community that supports this career path. Present your findings in a comparison table with a 300-word reflection on which path interests you most and why.

Reading List

- Calder, A. (2024) *A Pocket Guide to ISO 27001:2022.* Ely: IT Governance Publishing.
- NCSC (2024) *Cyber Essentials: Requirements for IT Infrastructure.* London: NCSC. Available at: https://www.ncsc.gov.uk/cyberessentials (Accessed: 15 March 2026).

- UK Parliament (2018) *Data Protection Act 2018.* London: The Stationery Office. Available at: https://www.legislation.gov.uk/ukpga/2018/12 (Accessed: 15 March 2026).
- PCI SSC (2022) *Payment Card Industry Data Security Standard v4.0.* Available at: https://www.pcisecuritystandards.org (Accessed: 15 March 2026).
- ICO (2024) *Guide to the UK General Data Protection Regulation.* Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/ (Accessed: 15 March 2026).

Summary

In this chapter, you have evaluated the key UK and international legislation that impacts cyber security planning, including UK GDPR, the NIS Regulations, the Computer Misuse Act, and newer legislation such as the Product Security Act and Online Safety Act. You have examined major industry standards including ISO 27001, NIST CSF, PCI DSS, and Cyber Essentials. You have also assessed professional certifications and organisational accreditation schemes that support cyber security competence and credibility.

Chapter Three – Implementing PDCA Security and Risk Management Policies

Introduction

This chapter examines how to design, monitor, implement, and continuously improve security policies using the Plan-Do-Check-Act (PDCA) cycle. Effective security policies are the bridge between strategy and operations – they translate strategic objectives into specific, actionable requirements that guide the behaviour of people, processes, and technology throughout the organisation.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand how to implement Plan, Do, Check and Act security and risk management policies.**

Assessment Criteria

3.1 Assess how to design, monitor, implement and continuously improve policies in relation to cyber and information risk business environments.

3.1 Designing, monitoring, implementing and improving policies

! Need to know – The PDCA Cycle (Deming Cycle)

Plan – Establish security objectives, assess risks, and develop policies and procedures. Define what needs to be achieved, how it will be measured, and what resources are required.

Do – Implement the policies and procedures. Deploy security controls, conduct training, and put the plan into action across the organisation.

Check – Monitor and measure the effectiveness of the policies against objectives. Conduct audits, review metrics, analyse incidents, and gather feedback to assess whether the policies are working.

Act – Take corrective and preventive actions based on the results of the Check phase. Update policies, improve controls, address gaps, and feed lessons learned back into the next Plan phase.

The PDCA cycle is iterative and continuous – each cycle builds on the previous one, creating a spiral of continuous improvement. ISO 27001 explicitly adopts the PDCA approach for its ISMS.

Security Policy Framework

An effective security policy framework consists of several layers, each serving a different purpose:

- **Information Security Policy (top-level)** – a high-level statement approved by the board that sets out the organisation's commitment to information security, defines the

scope of the ISMS, and establishes the principles that guide all security activities. Typically 2-4 pages and reviewed annually.

- **Topic-specific policies** – detailed policies addressing specific areas of security. Common examples include: Acceptable Use Policy, Access Control Policy, Password Policy, Data Classification Policy, Incident Response Policy, Remote Working Policy, BYOD Policy, Third-Party Security Policy, and Data Retention Policy.
- **Standards** – mandatory requirements specifying how policies are to be implemented. For example, a Password Standard might specify minimum length (14 characters), complexity requirements, and rotation periods.
- **Procedures** – step-by-step instructions for performing specific tasks. For example, an Incident Reporting Procedure describes exactly how to report a suspected security incident.
- **Guidelines** – recommended practices that support policies but are not mandatory. For example, a Secure Coding Guideline provides recommendations for developers.

Writing Effective Security Policies

Security policies are only effective if they are clear, practical, and enforceable. Key principles for writing effective policies include:

- **Clarity and simplicity** – policies should be written in plain language that all employees can understand. Avoid technical jargon unless the policy is specifically for a technical audience. If a policy cannot be understood, it cannot be followed.
- **Specificity** – policies should clearly state what is required, what is prohibited, and what the consequences of non-compliance are. Vague policies create confusion and are difficult to enforce.
- **Practicality** – policies must be achievable within the organisation's operational context. Impractical policies will be ignored or worked around, undermining the entire policy framework.
- **Measurability** – policies should include criteria by which compliance can be assessed. If you cannot measure compliance, you cannot manage it.
- **Alignment** – policies must align with the organisation's risk appetite, business objectives, legal obligations, and cultural context. A policy that conflicts with business operations will generate resistance.
- **Ownership and accountability** – each policy should have a named owner who is responsible for its maintenance and a defined review cycle.

Case Study – Policy Implementation at a Multinational Organisation

A multinational technology company with operations in 30 countries needed to implement a unified information security policy framework while respecting local legal requirements and cultural differences. The company adopted a tiered approach: a global Information Security Policy set mandatory minimum standards applicable to all operations worldwide. Regional policy supplements addressed jurisdiction-specific requirements (e.g. GDPR for European operations, PDPA for Singapore operations, LGPD for Brazil operations). Local implementation guides provided practical guidance for each office, adapting global requirements to local infrastructure and working practices.

The implementation used a phased approach: Phase 1 – Policy development and legal review (3 months), Phase 2 – Management training and awareness (2 months), Phase 3

– Employee training and acknowledgment (3 months), Phase 4 – Monitoring and compliance verification (ongoing). Key challenges included language translation, varying levels of IT maturity across offices, cultural attitudes to authority and compliance, and coordinating across time zones.

Task: (1) Evaluate the tiered policy approach – what are its advantages and disadvantages? (2) What challenges might arise when implementing a single password policy across 30 countries with different regulatory requirements? (3) How would you measure policy compliance across a dispersed organisation? (4) Design a policy awareness campaign that would work across different cultures. Write a 700-word analysis.

Over to you – Policy Writing Exercise

Write a complete Acceptable Use Policy for a medium-sized company (200 employees). Your policy should include: (a) purpose and scope, (b) definitions, (c) policy statements covering internet use, email use, social media, personal devices, removable media, and software installation, (d) monitoring and enforcement provisions, (e) consequences of non-compliance, (f) related policies, and (g) review schedule. Aim for 1,000-1,500 words. Ensure the policy is clear, practical, and enforceable.

Reading List

- Peltier, T.R. (2024) *Information Security Policies, Procedures, and Standards: A Practitioner's Reference.* 3rd edn. Boca Raton, FL: Auerbach Publications.
- ISO (2022) *ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Controls.* Geneva: ISO.
- Barman, S. (2023) *Writing Information Security Policies.* 2nd edn. Indianapolis, IN: New Riders.
- NCSC (2024) *Small Business Guide: Cyber Security.* Available at: https://www.ncsc.gov.uk/collection/small-business-guide (Accessed: 15 March 2026).

Summary

In this chapter, you have examined the PDCA cycle as a framework for continuous improvement in security policy management. You have explored the structure of a security policy framework, including the hierarchy from top-level policies through standards, procedures, and guidelines. You have learned principles for writing effective security policies and examined the practical challenges of implementing policies across multinational organisations.

Chapter Four – The Future Legal and Technical Environment

Introduction

This chapter investigates how large influential countries approach information security and examines the national and international regulatory landscape. Cyber security is an inherently global challenge – cyber threats cross borders effortlessly, and organisations operating internationally must navigate a complex patchwork of national regulations, international standards, and geopolitical considerations.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand the future legal and technical environment and the impact on cyber security planning and digital risk management.**

Assessment Criteria

4.1 Investigate the approaches of large influential countries in the information security domain.

4.2 Discuss relevant national/international regulatory and standards relating to cyber security environments.

4.1 Approaches of large influential countries

Country	Approach to Cyber Security
United Kingdom	The UK's approach is coordinated through the NCSC (part of GCHQ). The National Cyber Strategy 2022 focuses on resilience, deterrence, and technological leadership. Key initiatives include Cyber Essentials, the Active Cyber Defence programme, and the proposed Cyber Security and Resilience Bill. The UK has a strong focus on public-private partnerships and information sharing.
United States	The US approach involves multiple agencies (CISA, NSA, FBI) coordinated under the National Cybersecurity Strategy 2023. Key themes include shifting liability from users to technology providers, prioritising long-term investments, and forging international partnerships. Executive Order 14028 mandated Zero Trust adoption across federal agencies. The US has the most extensive cyber offensive and defensive capabilities globally.
European Union	The EU has implemented the NIS2 Directive (2022) expanding cybersecurity obligations to more sectors, the Cyber Resilience Act (2024) requiring cybersecurity standards for all digital products sold in the EU, and the Digital Operational Resilience Act (DORA, 2024) imposing ICT risk management requirements on financial institutions. ENISA (EU Agency for Cybersecurity) coordinates EU-wide cyber security efforts.
China	China's Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (PIPL, 2021) create a

	comprehensive regulatory framework emphasising data sovereignty, critical information infrastructure protection, and state control. China has extensive cyber capabilities and a focus on protecting domestic digital infrastructure. Data localisation requirements affect multinational organisations operating in China.
Russia	Russia's approach emphasises 'information security' rather than 'cyber security' – a broader concept encompassing information warfare and narrative control. The Federal Law on Critical Information Infrastructure Protection (2017) requires organisations in key sectors to share incident data with the state. Russia is widely cited as a major source of state-sponsored cyber operations.
Israel	Israel is widely regarded as a global leader in cybersecurity innovation. The Israel National Cyber Directorate (INCD) coordinates national cyber defence. Israel's approach leverages its military-intelligence expertise (Unit 8200 alumni are prominent in the cybersecurity industry) and strong public-private partnerships. The country exports a disproportionately high share of global cybersecurity technology.
India	India's approach is coordinated by CERT-In and governed by the IT Act 2000 (amended 2008) and the Digital Personal Data Protection Act 2023. India faces challenges from rapid digitalisation, limited cybersecurity workforce, and increasing cyber attacks on critical infrastructure. The country has been investing heavily in cybersecurity capacity building.

Over to you – International Comparison Research

Select two countries from the table above and conduct a detailed comparison of their cyber security approaches. Consider: (a) national strategy and governance structure, (b) key legislation, (c) enforcement mechanisms and penalties, (d) government investment in cyber security, (e) public-private partnership models, (f) approach to cyber offensive capabilities, and (g) implications for multinational organisations operating in both countries. Present your findings as a 700-word comparative analysis.

4.2 National and international regulatory standards

The international regulatory landscape for cyber security is evolving rapidly. Key developments that will shape the future environment include:

- **AI and cyber security** – the EU AI Act (2024) introduces regulatory requirements for artificial intelligence systems based on their risk level. AI is increasingly used in both offensive cyber operations (automated vulnerability discovery, deepfake social engineering) and defensive operations (threat detection, automated response). Regulating AI in cyber security will be one of the defining challenges of the next decade.
- **Quantum computing threats** – quantum computers will eventually be able to break current public-key encryption algorithms (RSA, ECC). NIST published post-quantum cryptography standards in 2024, and organisations need to begin planning the transition to quantum-resistant algorithms. This 'crypto-agility' will require significant strategic planning and investment.

- **Supply chain security regulations** – following high-profile supply chain attacks (SolarWinds, Log4Shell, MOVEit), regulators are increasingly mandating supply chain security measures. The EU Cyber Resilience Act requires manufacturers to ensure cybersecurity throughout a product's lifecycle, and the US Executive Order 14028 mandates Software Bills of Materials (SBOMs) for software sold to federal agencies.
- **Operational resilience** – regulators in financial services (Bank of England, FCA, PRA in the UK; DORA in the EU) are shifting focus from preventing failures to ensuring organisations can continue operating despite them. This regulatory emphasis on resilience aligns with the broader trend from pure cyber security toward cyber resilience.
- **Data sovereignty and localisation** – an increasing number of countries are requiring that certain categories of data be stored and processed within their national borders. This trend complicates multinational operations and cloud strategies, requiring organisations to design architectures that can accommodate diverse data sovereignty requirements.

Did you know?

The Budapest Convention on Cybercrime (2001), drafted by the Council of Europe, is the only binding international treaty on cyber crime. As of 2024, it has been ratified by 68 countries including the UK, US, and most EU member states. However, major cyber powers including Russia, China, and India have not signed. In 2022, the UN began negotiating a new international cybercrime treaty, but progress has been complicated by fundamental disagreements between nations about the scope of the treaty and the balance between security and privacy.

Reading List

- Shackelford, S.J. (2022) *Governing New Frontiers in the Information Age: Toward Cyber Peace.* Cambridge: Cambridge University Press.
- EU (2022) *Directive (EU) 2022/2555 (NIS2).* Official Journal of the European Union. Available at: https://eur-lex.europa.eu (Accessed: 15 March 2026).
- NIST (2024) *Post-Quantum Cryptography Standards.* Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography (Accessed: 15 March 2026).
- Kosseff, J. (2022) *Cybersecurity Law.* 3rd edn. Hoboken, NJ: Wiley.

Summary

In this chapter, you have investigated the cyber security approaches of seven influential countries and examined how national strategies, cultural factors, and geopolitical considerations shape their approaches. You have analysed emerging regulatory trends including AI regulation, quantum computing preparedness, supply chain security, operational resilience, and data sovereignty. Understanding this evolving landscape is essential for designing security strategies that are both effective and compliant in a global context.

Chapter Five – Planning and Designing a Security Audit

Introduction

This final chapter brings together knowledge from all previous chapters to examine how to plan and design a comprehensive security audit for a cyber network. A security audit is a systematic evaluation of an organisation's information systems, policies, and procedures against established criteria – whether internal standards, regulatory requirements, or industry frameworks. Security audits are essential for verifying compliance, identifying gaps, and providing assurance to stakeholders.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand how to plan and design a security audit for a cyber network.**

Assessment Criteria

5.1 Design security plans that reflect the legal and political environment.

5.1 Designing security plans reflecting legal and political environments

Types of Security Audit

- **Compliance audits** – assess whether the organisation meets the requirements of specific regulations, standards, or frameworks (e.g. ISO 27001 certification audit, PCI DSS assessment, GDPR readiness review).
- **Technical audits** – evaluate the technical security of systems, networks, and applications through vulnerability assessments, penetration tests, and configuration reviews.
- **Process audits** – examine security processes and procedures, such as incident response, change management, access control, and patch management, to verify they are documented, followed, and effective.
- **Third-party/supplier audits** – assess the security of third-party suppliers and service providers who have access to the organisation's data or systems. Essential for supply chain risk management.
- **Internal audits** – conducted by the organisation's own staff to verify compliance with internal policies and identify improvement opportunities. Internal audits should be independent of the teams being audited.
- **External audits** – conducted by independent third parties to provide objective assurance. Required for ISO 27001 certification and SOC 2 reporting.

The Security Audit Lifecycle

A structured security audit follows a defined lifecycle:

- **Planning** – defining the scope, objectives, criteria, and methodology of the audit. Scope defines what will be audited (systems, processes, locations). Objectives

define what the audit aims to achieve (compliance verification, gap identification, maturity assessment). Criteria define the standards against which the organisation will be assessed. Methodology defines the audit approach (document review, interviews, technical testing, observation).

- **Preparation** – gathering background information, reviewing documentation (policies, procedures, risk registers, previous audit reports), identifying key stakeholders and interviewees, and scheduling audit activities. Preparation should include a pre-audit meeting with the audited organisation to confirm scope, logistics, and expectations.
- **Fieldwork** – executing the audit plan. This includes reviewing evidence (documents, logs, configurations), conducting interviews with relevant personnel, performing technical testing, and observing processes in action. All findings should be documented with supporting evidence and cross-referenced to audit criteria.
- **Analysis and reporting** – analysing the evidence gathered during fieldwork, identifying findings (both positive and negative), assessing the significance of non-conformities, and preparing the audit report. The report should include an executive summary, scope and methodology, detailed findings with evidence references, risk ratings for each finding, and specific recommendations for remediation.
- **Follow-up** – tracking the implementation of remediation actions, verifying that identified issues have been resolved, and confirming that improvements are sustained. Follow-up may involve a formal re-audit of specific areas.

Example – Security Audit Plan Template

Audit Title: Annual Information Security Audit 2026

Scope: All UK operations including corporate network, cloud infrastructure (AWS), web applications, and remote working arrangements. Excludes Singapore and US offices (audited separately).

Criteria: ISO 27001:2022 Annex A controls, UK GDPR requirements, Cyber Essentials Plus requirements, internal Information Security Policy v4.2.

Methodology: Document review (Week 1), Staff interviews across IT, HR, Legal, and Operations (Week 2), Technical testing including vulnerability scanning and configuration review (Week 2-3), Management review and reporting (Week 4).

Deliverables: Draft audit report (Day 22), Management response period (5 working days), Final audit report with management responses and remediation plan (Day 30).

Case Study – TalkTalk Security Audit Failures (2015)

In October 2015, UK telecoms company TalkTalk suffered a cyber attack that compromised the personal data of 156,959 customers, including bank account details and sort codes. The ICO investigation found that TalkTalk had failed to implement basic security measures: the database breached was running outdated software with known vulnerabilities, the company did not conduct adequate security audits, and there was a lack of governance and oversight of information security. TalkTalk was fined £400,000 – the largest fine issued by the ICO at the time under the pre-GDPR Data Protection Act.

The ICO report specifically noted that a properly conducted security audit would have identified the unpatched databases and inadequate access controls that enabled the attack. The case powerfully illustrates why regular, thorough security audits are not just good practice but a regulatory expectation.

Task: (1) Design a security audit plan that, if implemented before the breach, would have identified the vulnerabilities exploited. Include scope, criteria, methodology, and timeline. (2) What governance failures contributed to the inadequacy of TalkTalk's security auditing? (3) How would the fine have differed under UK GDPR (compare the maximum penalties)? (4) What ongoing audit programme would you recommend for a telecoms company handling this volume of customer data? Write a comprehensive 800-word analysis.

Designing Audit Plans for Different Environments

Security audit plans must be tailored to the organisation's specific context, including its legal environment, industry sector, geographic footprint, and risk profile:

- **Regulated industries** – audits in financial services, healthcare, and telecoms must address sector-specific requirements (FCA, NHS DSPT, Ofcom). The audit plan must map findings to specific regulatory requirements and assess compliance in a way that satisfies the regulator.
- **Multinational environments** – auditing across multiple jurisdictions requires understanding local data protection laws, cultural factors affecting compliance, and logistical challenges of remote auditing. The audit plan should specify how local requirements are addressed and how findings are consolidated globally.
- **Cloud and hybrid environments** – auditing cloud infrastructure requires understanding the shared responsibility model and obtaining appropriate assurance from cloud providers (SOC 2 reports, ISO 27001 certificates). The audit must assess the organisation's configuration and management of cloud services, not just the provider's infrastructure.
- **Remote and hybrid working** – the shift to remote working has expanded the audit scope to include home working environments, personal device security, VPN configurations, and collaboration tool settings.

Over to you – Capstone Exercise: Security Audit Design

This is the capstone exercise for the unit, drawing together knowledge from all previous chapters. You are a security consultant engaged to design a comprehensive security audit for a UK-based fintech company (300 employees, operating in the UK and EU, processing payment card data, using AWS cloud infrastructure, with 60% of staff working remotely).

Design a complete security audit plan covering: (1) Audit scope and objectives, (2) Applicable regulations and standards (identify at least five), (3) Audit methodology (document review, interviews, technical testing), (4) Detailed audit schedule (timeline with milestones), (5) Resource requirements (auditor skills and number of audit days), (6) Risk assessment approach for audit findings, (7) Reporting format and distribution, (8) Follow-up and remediation tracking process. Present your audit plan as a professional document of 1,500-2,000 words.

Over to you – Video Watch: Security Auditing

Title: ISO 27001 Audit Process Explained – Advisera

Link: **https://www.youtube.com/live/seED4gX8nGM?si=59vmDB-Utm0_H79D**

After watching, explain the difference between a Stage 1 and Stage 2 ISO 27001 audit. What are the most common non-conformities found during certification audits?

Reading List

- Kohnke, A., Sigler, K. and Shoemaker, D. (2023) *The Complete Guide to Cybersecurity Risks and Controls.* 2nd edn. Boca Raton, FL: Auerbach Publications.
- Davis, C. and Schiller, M. (2022) *IT Auditing Using Controls to Protect Information Assets.* 3rd edn. New York: McGraw-Hill.
- ISACA (2024) *COBIT 2019 Framework: Governance and Management Objectives.* Rolling Meadows, IL: ISACA.
- Calder, A. and Watkins, S. (2024) *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002.* 8th edn. London: Kogan Page.

Summary

In this final chapter, you have explored the planning and design of security audits, including the different types of audit, the audit lifecycle, and how to tailor audit plans for different environments. You have examined a real-world case study demonstrating the consequences of inadequate security auditing and have designed your own comprehensive audit plan through the capstone exercise. This chapter brings together the strategic, legal, policy, and technical knowledge from all previous chapters into a practical, applied capability.

Glossary

Word / Term	Explanation
Balanced Scorecard	Strategic planning framework translating objectives into measurable metrics across four perspectives.
Budapest Convention	The only binding international treaty on cybercrime (Council of Europe, 2001).
CISM	Certified Information Security Manager – ISACA certification for security management professionals.
CISSP	Certified Information Systems Security Professional – (ISC)² gold-standard security certification.
Cyber Essentials	UK Government-backed baseline certification scheme covering five key security controls.
Cyber Resilience Act	EU legislation requiring cybersecurity standards for all digital products.
DORA	Digital Operational Resilience Act – EU regulation for ICT risk management in financial services.
FAIR	Factor Analysis of Information Risk – methodology for quantifying cyber risk in financial terms.
GDPR	General Data Protection Regulation – EU/UK data protection legislation.
ISMS	Information Security Management System – systematic approach governed by ISO 27001.
ISO 27001	International standard for Information Security Management Systems.
NIS2 Directive	EU directive expanding cybersecurity obligations across more sectors (2022).
PDCA	Plan-Do-Check-Act – continuous improvement cycle (Deming Cycle).
PESTLE	Analysis framework: Political, Economic, Social, Technological, Legal, Environmental.
Post-Quantum Cryptography	Encryption algorithms resistant to quantum computing attacks.
Risk Appetite	The level of risk an organisation is willing to accept in pursuit of its objectives.
SBOM	Software Bill of Materials – list of components in a software product for supply chain security.
SOC 2	Service Organisation Control 2 – audit framework for cloud service providers.
SWOT	Analysis framework: Strengths, Weaknesses, Opportunities, Threats.

Zero Trust	Security model assuming no user or device should be trusted by default.

MCQs and True & False Questions (self-assessment)

True or False Questions

1. A cyber security strategy should align with the organisation's business objectives.
2. The PDCA cycle stands for Plan, Deploy, Check, Adapt.
3. ISO 27001 is certifiable by independent auditors.
4. Cyber Essentials covers ten key security controls.
5. UK GDPR requires breach notification to the ICO within 72 hours.
6. The balanced scorecard measures security across four perspectives.
7. FAIR is a methodology for quantifying cyber risk in financial terms.
8. The Computer Misuse Act was enacted in 2005.
9. NIS2 expands cybersecurity obligations to more sectors than the original NIS Directive.
10. A security policy framework should include only one top-level policy.
11. PESTLE analysis examines political, economic, social, technological, legal, and environmental factors.
12. Cyber Essentials Plus includes hands-on technical verification.
13. China's PIPL is a personal data protection law enacted in 2021.
14. Post-quantum cryptography standards were published by NIST in 2024.
15. A compliance audit assesses whether an organisation meets specific regulatory requirements.
16. The Budapest Convention has been ratified by Russia and China.
17. The CISO should frame security investments in business risk terms, not technical jargon.
18. ISO 27002:2022 organises controls into four themes.
19. DORA applies to financial institutions in the EU.
20. Security policies should be written in complex technical language to demonstrate expertise.
21. The UK's National Cyber Strategy 2022 has five pillars.
22. A Stage 1 ISO 27001 audit is a documentation review.
23. The Product Security Act 2022 bans default passwords on IoT devices.
24. SOC 2 Type II reports verify controls over an extended period.
25. SWOT analysis examines strengths, weaknesses, opportunities, and threats.

Multiple Choice Questions

1. PDCA stands for:

A. Plan, Deploy, Check, Adapt
B. Plan, Do, Check, Act
C. Prepare, Deliver, Control, Assess
D. Prevent, Detect, Contain, Analyse

2. Which framework quantifies cyber risk in financial terms?

A. NIST CSF
B. ISO 27001

C. FAIR
D. COBIT

3. Cyber Essentials covers how many key controls?

A. 3
B. 5
C. 10
D. 18

4. ISO 27001:2022 Annex A contains how many controls?

A. 42
B. 93
C. 114
D. 150

5. The NIS2 Directive was introduced by:

A. The UK Government
B. The European Union
C. The United States
D. The United Nations

6. Which certification requires 5 years of security management experience?

A. CompTIA Security+
B. CEH
C. CISM
D. GCFE

7. The UK's national CERT function is operated by:

A. The ICO
B. The FCA
C. The NCSC
D. GCHQ directly

8. DORA specifically applies to:

A. Healthcare organisations
B. Financial institutions
C. Educational institutions
D. Manufacturing companies

9. A Stage 2 ISO 27001 audit focuses on:

A. Documentation review only
B. Implementation effectiveness
C. Financial records
D. Staff qualifications

10. The Uber CSO was convicted for:

A. Hacking
B. Concealing a data breach
C. Insider trading

D. Negligence

11. Post-quantum cryptography addresses threats from:

A. Social engineering
B. Quantum computers
C. Ransomware
D. Phishing

12. The Budapest Convention is:

A. A trade agreement
B. An international cybercrime treaty
C. A privacy regulation
D. A military alliance

13. CREST accredits organisations providing:

A. Financial services
B. Penetration testing and incident response
C. Cloud hosting
D. Software development

14. The TalkTalk breach fine was imposed by:

A. The FCA
B. The ICO
C. OFCOM
D. The NCA

15. An SBOM is:

A. A security benchmark
B. A software component inventory
C. A backup method
D. A firewall configuration

16. Which country is NOT a signatory to the Budapest Convention?

A. UK
B. US
C. Russia
D. Germany

17. ISO 27002:2022 organises controls into:

A. Two domains
B. Four themes
C. Seven layers
D. Ten categories

18. The Product Security Act 2022 targets:

A. Financial products
B. IoT devices
C. Pharmaceutical products
D. Vehicles

19. A compliance mapping matrix is used to:

A. Track employee performance
B. Map controls to multiple regulatory requirements
C. Design network diagrams
D. Calculate financial risk

20. The NCSC Board Toolkit provides:

A. Penetration testing tools
B. Guidance for board-level cyber governance
C. Malware analysis platforms
D. Cloud migration guides

Answers to True/False Questions

1. *True.* Alignment between security strategy and business objectives is fundamental to securing executive support and resources.

2. *False.* PDCA stands for Plan, Do, Check, Act.

3. *True.* Organisations can be independently audited and certified against ISO 27001.

4. *False.* Cyber Essentials covers five key controls: firewalls, secure configuration, user access control, malware protection, and security updates.

5. *True.* UK GDPR requires notification within 72 hours of becoming aware of a notifiable breach.

6. *True.* The balanced scorecard measures across Financial, Customer, Internal Processes, and Learning and Growth.

7. *True.* FAIR enables cyber risks to be expressed in financial terms.

8. *False.* The Computer Misuse Act was enacted in 1990.

9. *True.* NIS2 significantly expands the scope of the original NIS Directive.

10. *False.* A policy framework includes a top-level policy plus multiple topic-specific policies, standards, procedures, and guidelines.

11. *True.* PESTLE examines six categories of external factors.

12. *True.* Cyber Essentials Plus includes hands-on technical verification by a qualified assessor.

13. *True.* China's Personal Information Protection Law came into effect in 2021.

14. *True.* NIST published initial post-quantum cryptography standards in 2024.

15. *True.* Compliance audits specifically assess adherence to regulations and standards.

16. *False.* Neither Russia nor China has signed the Budapest Convention.

17. *True.* Business language, not technical jargon, is essential for board-level communication.

18. *True.* The four themes are: Organisational, People, Physical, and Technological.

19. *True.* DORA applies to financial entities across the EU.

20. *False.* Policies should be written in clear, plain language that all employees can understand.

21. *True.* The five pillars are: ecosystem, resilience, technology, global leadership, and deterrence.

22. *True.* Stage 1 is primarily a documentation and readiness review.

23. *True.* The Act prohibits universal default passwords on consumer IoT devices.

24. *True.* SOC 2 Type II covers an extended observation period, typically 6-12 months.

25. *True.* SWOT is a foundational strategic analysis framework.

Answers to Multiple Choice Questions

1. (B) Plan, Do, Check, Act
2. (C) FAIR
3. (B) 5
4. (B) 93
5. (B) The European Union
6. (C) CISM
7. (C) The NCSC
8. (B) Financial institutions
9. (B) Implementation effectiveness
10. (B) Concealing a data breach
11. (B) Quantum computers
12. (B) An international cybercrime treaty
13. (B) Penetration testing and incident response
14. (B) The ICO
15. (B) A software component inventory
16. (C) Russia
17. (B) Four themes
18. (B) IoT devices
19. (B) Map controls to multiple regulatory requirements
20. (B) Guidance for board-level cyber governance