

CISSP 考試大綱

CISSP 考試大綱每三年改版一次，新版大綱於 2027 年 4 月 15 生效。本次改版基本上沒有新增太多東西，主要是考試大綱的【結構與用字】的優化而已。

CISSP 八個 Domain 的配分比重也調整的更為平衡。Domain 1 由 16% 減為 13.6%，Domain 2 則由 10% 改為 12%，是變動比例最高的二個 Domain。

Domain 1 標題把 Security Management 的概念升級為 Security Governance，正式標題改成 Security Governance and Risk Management。

The image shows a side-by-side comparison of the CISSP Certification Exam Outline and CAT Examination Information for the 2027 and 2024 versions. The 2027 version is on the left, and the 2024 version is on the right. The top section shows the CISSP logo and the title 'Certified Information Systems Security Professional ISC2 Certification'. The middle section shows the 'Certification Exam Outline' with the effective date 'April 15, 2027' for the 2027 version and 'April 15, 2024' for the 2024 version. The bottom section shows the 'CISSP CAT Examination Information' and 'CISSP CAT Examination Weights'.

CISSP CAT Examination Information

The CISSP exam uses Computerized Adaptive Testing (CAT) for all English, German, Spanish-Modern, Japanese, Simplified Chinese exams. You can learn more about CISSP CAT at www.isc2.org/certifications/CISSP-CAT.

Length of exam	3 hours
Number of items	100 - 150
Item format	Multiple choice and advanced item types
Passing grade	700 out of 1000 points
Exam language availability	Chinese, English, German, Japanese, Spanish
Testing center	ISC2 Authorized PPC and PUTC Select Pearson Testing Centers

CISSP CAT Examination Weights

Domains	Average Weight
1. Security Governance and Risk Management	13.6%
2. Asset Security	12%
3. Security Architecture and Engineering	12.8%
4. Communication and Network Security	12.8%
5. Identity and Access Management (IAM)	13.6%
6. Security Assessment and Testing	11.2%
7. Security Operations	12.8%
8. Software Development Security	11.2%
Total:	100%

The 2027 version shows a change in the average weight for Domain 1 from 16% to 13.6% and for Domain 2 from 10% to 12%.

Domain 1

1.1 新增 Ethics in Artificial Intelligence (AI)。重點在**道德**，而不是 AI 的技術或模型。

1.3 將 PCI 改成 PCI DSS。但 **standard** 跟 **framework** 是不同概念，我們並不認同把 **standard** 跟 **framework** 混為一談。Due care/due diligence 改成 Due care and due diligence 讓語意/義更清楚。

1.5 標題的舉例刪除 industry standards 以**符合邏輯**，因為 industry standards 是標準，而不是一種調查類型(investigation type)。

1.8 廠商及合約的控制舉例加入 SLA（原本是 7.4 的子標題，現在變成 1.8 的例子）。

1.9 Risk treatment 舉例新增 risk mitigation strategies。（標題用 risk treatment，但例子用 risk response，表示 **CISSP 的風險觀理概念沒有統一或不一致**）

1.12 教育訓練與意識提升方法與技巧的舉例保留安全冠軍與遊戲化，刪除社交工程與釣魚，讓**邏輯更一致**。因為社交工程及釣魚是攻擊技巧，不是防止的方法。教育訓練方案的有效性估一項多加利害關係人參與(stakeholder engagement)。

CISSP Certified Information Systems Security Professional ISC2 Certification		CISSP Certified Information Systems Security Professional ISC2 Certification
Domain 1: Security Governance and Risk Management		Domain 1: Security and Risk Management
1.1 Understand, adhere to, and promote professional ethics - ISC2 Code of Professional Ethics - Organizational code of ethics Ethics in Artificial Intelligence (AI)		1.1 Understand, adhere to, and promote professional ethics - ISC2 Code of Professional Ethics - Organizational code of ethics
1.2 Understand and apply security concepts Confidentiality, integrity, availability, authenticity, and non-repudiation		1.2 Understand and apply security concepts Confidentiality, integrity, and availability, authenticity, and nonrepudiation (5 Pillars of Information Security)
1.3 Evaluate, apply, and sustain security governance principles - Alignment of the security function to business strategy, goals, mission, and objectives - Organizational processes (e.g., acquisitions, divestitures, governance committees) - Organizational roles and responsibilities - Security control frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry Data Security Standard (PCI DSS), Federal Risk and Authorization Management Program (FedRAMP)) Due care and due diligence		1.3 Evaluate and apply security governance principles - Alignment of the security function to business strategy, goals, mission, and objectives - Organizational processes (e.g., acquisitions, divestitures, governance committees) - Organizational roles and responsibilities - Security control frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP)) Due care/due diligence
1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context - Cybercrimes and data breaches - Licensing and Intellectual Property IP requirements - Import/export controls - Transborder data flow - Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act, The Health Insurance Portability and Accountability Act (HIPAA)) - Contractual, legal, industry standards, and regulatory requirements		1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context - Cybercrimes and data breaches - Licensing and Intellectual Property requirements - Import/export controls - Transborder data flow - Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act) - Contractual, legal, industry standards, and regulatory requirements
1.5 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory)		1.5 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
1.6 Develop, document, and implement security policy, standards, procedures, and guidelines		1.6 Develop, document, and implement security policy, standards, procedures, and guidelines
1.7 Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements - Business Impact Analysis (BIA) - External dependencies		1.7 Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements - Business impact analysis (BIA) - External dependencies
CISSP Certification Exam Outline 4		CISSP Certification Exam Outline 4

CISSP Certified Information Systems Security Professional ISC2 Certification 1.8 Contribute to and enforce personnel security policies and procedures » Candidate screening and hiring » Employment agreements and policy driven requirements 1.9 Understand and apply risk management concepts » Threat and vulnerability identification » Risk analysis, assessment, and scope » Risk response and treatment (e.g., cybersecurity insurance, risk mitigation strategies) » Applicable types of controls (e.g., preventive, detection, corrective) » Control assessments (e.g., security and privacy) » Continuous monitoring and measurement » Reporting (e.g., internal, external) 1.10 Understand and apply threat modeling concepts and methodologies 1.11 Apply Supply Chain Risk Management (SCRM) concepts » Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants, reputational) » Risk mitigations (e.g., third-party assessment and monitoring, minimum security requirements, service level requirements, silicon root of trust, physically unclonable function, Software Bill of Materials (SBOM)) 1.12 Establish, maintain, and measure a security awareness, education, and training program » Methods and techniques to increase awareness and training (e.g., security champions, gamification) » Periodic content reviews to include emerging technologies and trends (e.g., cryptocurrency, Artificial Intelligence (AI), blockchain) » Program effectiveness evaluation and stakeholder engagement		CISSP Certified Information Systems Security Professional ISC2 Certification 1.8 Contribute to and enforce personnel security policies and procedures » Candidate screening and hiring » Employment agreements and policy driven requirements 1.9 Understand and apply risk management concepts » Threat and vulnerability identification » Risk analysis, assessment, and scope » Risk response and treatment (e.g., cybersecurity insurance) » Applicable types of controls (e.g., preventive, detection, corrective) » Control assessments (e.g., security and privacy) » Continuous monitoring and measurement » Reporting (e.g., internal, external) 1.10 Understand and apply threat modeling concepts and methodologies 1.11 Apply supply chain risk management (SCRM) concepts » Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants) » Risk mitigations (e.g., third-party assessment and monitoring, minimum security requirements, service level requirements, silicon root of trust, physically unclonable function, software bill of materials) 1.12 Establish and maintain a security awareness, education, and training program » Methods and techniques to increase awareness and training (e.g., security champions, gamification) » Periodic content reviews to include emerging technologies and trends (e.g., cryptocurrency, artificial intelligence (AI), blockchain) » Program effectiveness evaluation
---	--	---

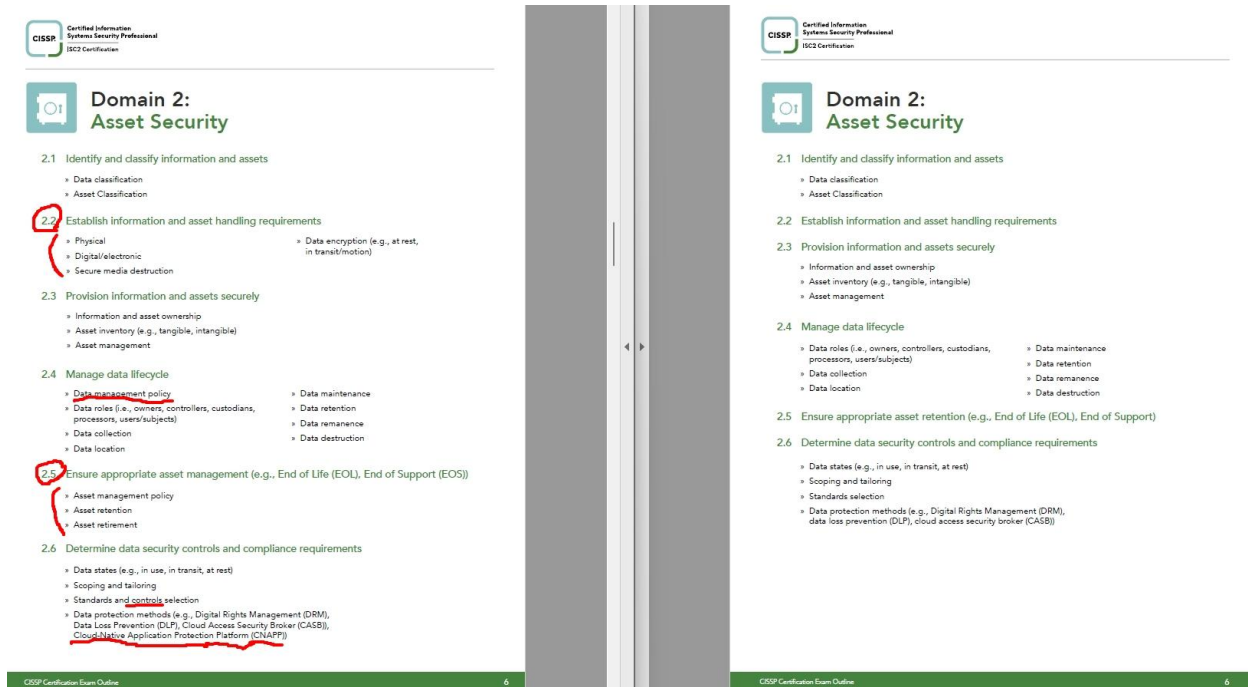
Domain 2

2.2 制定資訊與資產處要求多了 4 項子標題（舊版只有大標題，沒有子標題）。

2.4 管理資料生命週期多了資料管理政策。

2.5 將標題由資產保留改成資產管理，並刪除舊版的子標題，新版不提供子標題。

2.6 多了雲原生應用保護平台(CNAPP)



Domain 3

3.1 最小特權用字改成**最小特權原則**，並簡寫成 PoLP；KISS 改成 **KISS 原則**。新增架構良好的框架(well-architected framework)、工作輪調(rotation of duties)與二人完整性(two-person integrity)。

3.4 多了 Hardware Security Module (HSM)。

3.5 ICS 加上 OT、雲服務模型多了 FaaS (取代舊版的 serverless)、微服務加上容器化(原本是獨立子標題)。多了供應鍊風險、**無人系統(autonomous systems)**及量子運算。

3.6 PKI 舉例刪除 quantum 一詞(將 quantum key distribution 改成 key distribution)。

3.7 多了零日(zero-day)攻擊與 AI 的威脅。

3.10 架構設計改成**安全架構設計(secure architectural design)**、除役(disposal)改成安全的除役(secure disposal)；新增連續安全審查(continuous security review)。

Domain 3: Security Architecture and Engineering

3.1 Research, implement, and manage engineering processes using secure design principles

- Threat modeling
- Principle of Least privilege (PoLP)
- Defense in Depth (DiD)
- Secure defaults
- Fail securely
- Separation of Duties (SoD)
- Principles of keep it simple and small
- Zero Trust (ZT)
- Privacy by design (e.g., privacy-enhancing technologies)
- Shared responsibility
- Secure Access Service Edge (SASE)
- Well-architected framework
- Rotation of duties
- Two-person integrity
- Keep it simple and small
- Zero trust ~~architecture~~
- Privacy by design
- Shared responsibility
- Secure access service edge

3.2 Understand the fundamental concepts of security models (e.g., Biba, Star, Bell-LaPadula)

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), **Hardware Security Module (HSM)**, encryption/decryption)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Operational Technology (OT) and Industrial Control Systems (ICS)**
- Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Serverless, **Function as a Service (FaaS)**)
- Distributed systems
- Internet of Things (IoT)
- Microservices and **containerization**
- Embedded systems
- High-Performance Computing systems
- Edge computing systems
- Virtualized systems
- Supply chain risk
- Autonomous systems
- Quantum computing
- Internet of Things (IoT)
- Microservices (e.g., application programming interface (API))
- Containerization
- Control plane**
- Embedded systems
- High-Performance Computing systems
- Edge computing systems
- Virtualized systems

3.6 Select and determine cryptographic solutions

- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curve, post-quantum)
- Public key infrastructure (PKI) (e.g., key distribution)
- Key management practices (e.g., rotation, **process**, **protection**)
- Digital signatures and digital certificates (e.g., non-repudiation, integrity)
- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- Public key infrastructure (PKI) (e.g., **quantum** key distribution)
- Key management practices (e.g., rotation)
- Digital signatures and digital certificates (e.g., non-repudiation, integrity)

CISSP Certified Information Systems Security Professional ISC2 Certification	CISSP Certified Information Systems Security Professional ISC2 Certification
3.7 Understand methods of cryptanalytic attacks - Brute force - Ciphertext only - Known plaintext - Frequency analysis - Chosen ciphertext - Implementation attacks - Side-channel - Fault injection - Timing - Adversary-in-the-Middle (MITM) - Pass the hash - Kerberos exploitation - Ransomware - Zero-Day attacks - Artificial intelligence (AI) threats (e.g., adversarial AI, AI model poisoning, deepfake attacks) 3.8 Apply security principles to site and facility design 3.9 Design site and facility security controls - Wiring closets/intermediate distribution frame - Server rooms/data centers - Media storage facilities - Evidence storage - Restricted and work area security - Utilities and heating, ventilation, and air conditioning (HVAC) - Environmental issues (e.g., natural disasters, man-made) - Fire prevention, detection, and suppression - Power (e.g., redundant, backup) 3.10 Manage the information system lifecycle - Stakeholder needs and requirements - Requirements analysis - Secure Architectural design - Development/Implementation - Integration - Verification and validation - Continuous security review - Transition/deployment - Operations and maintenance/sustainment - Retirement/secure disposal	3.7 Understand methods of cryptanalytic attacks - Brute force - Ciphertext only - Known plaintext - Frequency analysis - Chosen ciphertext - Implementation attacks - Side-channel - Fault injection - Timing - Man-in-the-Middle (MITM) - Pass the hash - Kerberos exploitation - Ransomware 3.8 Apply security principles to site and facility design 3.9 Design site and facility security controls - Wiring closets/intermediate distribution facilities - Server rooms/data centers - Media storage facilities - Evidence storage - Restricted and work area security - Utilities and heating, ventilation, and air conditioning (HVAC) - Environmental issues (e.g., natural disasters, man-made) - Fire prevention, detection, and suppression - Power (e.g., redundant, backup) 3.10 Manage the information system lifecycle - Stakeholders needs and requirements - Requirements analysis - Architectural design - Development/implementation - Integration - Verification and validation - Transition/deployment - Operations and maintenance/sustainment - Retirement/disposal
CISSP Certification Exam Outline 8	CISSP Certification Exam Outline 8

Domain 4

4.1 多了軟體定義安全(software-defined security)；本項原本放在 8.5。

4.3 遠端存取的舉例多了遠端工作(remote working)。

Domain 4:
Communication and Network Security

4.1 Apply secure design principles in network architectures

- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol version 4 (IPv4) and 6 (IPv6) (e.g., unicast, broadcast, multicast, anycast)
- Secure protocols (e.g., Internet Protocol Security (IPSec), Secure Shell (SSH), Secure Sockets Layer (SSL)/Transport Layer Security (TLS))
- Implications of multilayer protocols
- Converged protocols (e.g., Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP), InfiniBand over Ethernet, Compute Express Link)
- Transport architecture (e.g., topology, data/control/management plane, cut-through/store-and-forward)
- Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)
- Traffic flows (e.g., north-south, east-west)
- Physical segmentation (e.g., in-band, out-of-band, air-gapped)
- Logical segmentation (e.g., Virtual Local Area Networks (VLANs), Virtual Private Networks (VPN), Virtual Routing and Forwarding, Virtual Domain)
- Micro-segmentation (e.g., network overlays/encapsulation, distributed firewalls, routers, intrusion detection system (IDS)/intrusion prevention system (IPS), Zero Trust)
- Edge networks (e.g., ingress/egress, peering)
- Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, satellite)
- Cellular/mobile networks (e.g., 4G, 5G)
- Content Delivery Networks (CDN)
- Software Defined Networks (SDN), (e.g., Application Programming Interface (API), Software-Defined Wide-Area Network (SDWAN), network functions virtualization)
- Virtual Private Cloud (VPC)
- Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)
- Software-defined security

4.2 Secure network components

- Operation of infrastructure (e.g., redundant power, warranty, support) - Transmission media (e.g., physical security of media, signal propagation quality)	- Network Access Control (NAC) systems (e.g., physical, and virtual solutions) - Endpoint security (e.g., host-based)
---	--

4.3 Implement secure communication channels according to design

- Voice, video, and collaboration (e.g., conferencing, video meeting rooms) - Remote access (e.g., network administrative functions, <u>remote working</u>)	- Data communications (e.g., backhaul networks, satellite) - Third-party connectivity (e.g., telecom providers, hardware support)
--	--

Domain 4:
Communication and Network Security

4.1 Apply secure design principles in network architectures

- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) version 4 and 6 (IPv6) (e.g., unicast, broadcast, multicast, anycast)
- Secure protocols (e.g., Internet Protocol Security (IPSec), Secure Shell (SSH), Secure Sockets Layer (SSL)/Transport Layer Security (TLS))
- Implications of multilayer protocols
- Converged protocols (e.g., Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP), InfiniBand over Ethernet, Compute Express Link)
- Transport architecture (e.g., topology, data/control/management plane, cut-through/store-and-forward)
- Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)
- Traffic flows (e.g., north-south, east-west)
- Physical segmentation (e.g., in-band, out-of-band, air-gapped)
- Logical segmentation (e.g., virtual local area networks (VLANs), virtual private networks (VPNs), virtual routing and forwarding, virtual domain)
- Micro-segmentation (e.g., network overlays/encapsulation; distributed firewalls, routers, intrusion detection system (IDS)/intrusion prevention system (IPS), zero trust)
- Edge networks (e.g., ingress/egress, peering)
- Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, satellite)
- Cellular/mobile networks (e.g., 4G, 5G)
- Content distribution networks (CDN)
- Software defined networks (SDN), (e.g., application programming interface (API), Software-Defined Wide-Area Network, network functions virtualization)
- Virtual Private Cloud (VPC)
- Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)

4.2 Secure network components

- Operation of infrastructure (e.g., redundant power, warranty, support) - Transmission media (e.g., physical security of media, signal propagation quality)	- Network Access Control (NAC) systems (e.g., physical, and virtual solutions) - Endpoint security (e.g., host-based)
---	--

4.3 Implement secure communication channels according to design

- Voice, video, and collaboration (e.g., conferencing, Zoom rooms) - Remote access (e.g., network administrative functions)	- Data communications (e.g., backhaul networks, satellite) - Third-party connectivity (e.g., telecom providers, hardware support)
--	--

Domain 5

5.1 標題多了舉例(供裝、控制、審查、吊銷)，子標題多了**身份(identities)**一項。

5.2 AAA 不舉例(刪除 MFA 及無密碼驗證)，但將無密碼驗證改成獨立子標題，並舉例(**FIDO, WebAuthn, Passkeys, 生物特徵**)。

5.4 授權機制把 Rule-based access control 簡稱為 RuBAC；把原來的 Risk-based access control 改成 **risk-adaptable** access control 並簡稱為 RadAC。

5.5 提權舉例把 sudo 改成 administrator groups/sudo，以避免綁定 Linux 系統。

5.6 建置身份驗證系統改成建置身份驗證與授權系統。

Domain 5: Identity and Access Management (IAM)

2025 Outline (Left):

- 5.1 Manage physical and logical access to assets (e.g., provision, control, review, revoke)
 - Information
 - Systems
 - Devices
 - Facilities
 - Applications
 - Services
 - Identities**
- 5.2 Design identification and authentication strategy (e.g., people, devices, and services)
 - Groups and Roles
 - Authentication, Authorization, Accounting (AAA)
 - Session management
 - Registration, proofing, and establishment of identity
 - Federated Identity Management (FIM)
 - Credential management systems (e.g., Password vault)
 - Single sign-on (SSO)
 - Just-In-Time
 - Passwordless authentication (e.g., Fast Identity Online (FIDO), WebAuthn, Passkeys, Biometrics)**
- 5.3 Federated identity with a third-party service
 - On-premises
 - Cloud
 - Hybrid
- 5.4 Implement and manage authorization mechanisms
 - Role-based access control (RBAC)
 - Rule-based access control (RuBAC)
 - Mandatory access control (MAC)
 - Discretionary access control (DAC)
 - Attribute-based access control (ABAC)
 - Risk-adaptable Access Control (RADAC)**
 - Access policy enforcement (e.g., policy decision point, policy enforcement point)
- 5.5 Manage the identity and access provisioning lifecycle
 - Account access review (e.g., user, system, service)
 - Provisioning and deprovisioning (e.g., on/off boarding and transfers)
 - Role definition and transition (e.g., people assigned to new roles)
 - Privilege escalation (e.g., use of **administrator groups/sudo**, auditing its use, Principle of Least Privilege (PoLP))
 - Service accounts management
- 5.6 Implement authentication and authorization systems

2026 Outline (Right):

- 5.1 Control physical and logical access to assets
 - Information
 - Systems
 - Devices
 - Facilities
 - Applications
 - Services
- 5.2 Design identification and authentication strategy (e.g., people, devices, and services)
 - Groups and Roles
 - Authentication, Authorization and Accounting (AAA) (**passwordless authentication, MFA**)
 - Credential management systems (e.g., Password vault)
 - Single sign-on (SSO)
 - Just-In-Time
 - Federated Identity Management (FIM)
 - Registration, proofing, and establishment of identity
- 5.3 Federated identity with a third-party service
 - On-premises
 - Cloud
 - Hybrid
- 5.4 Implement and manage authorization mechanisms
 - Role-based access control (RBAC)
 - Rule-based access control
 - Mandatory access control (MAC)
 - Discretionary access control (DAC)
 - Attribute-based access control (ABAC)
 - Risk-based access control**
 - Access policy enforcement (e.g., policy decision point, policy enforcement point)
- 5.5 Manage the identity and access provisioning lifecycle
 - Account access review (e.g., user, system, service)
 - Provisioning and deprovisioning (e.g., on/off boarding and transfers)
 - Service accounts management
 - Role definition and transition (e.g., people assigned to new roles)
 - Privilege escalation (e.g., use of sudo, auditing its use)
- 5.6 Implement authentication systems

Domain 6

6.2 滲透測試刪除舉例(紅/藍/粉紅隊)、入侵攻擊模擬(breach attack simulation)刪除入侵變成 attack simulation。

6.4 標題 Analyze test output 改成 Analyze test/audit output (加了 audit)。

The image displays a side-by-side comparison of the CISSP Domain 6: Security Assessment and Testing content from two different versions of the exam outline. The left version is the current one, and the right version shows the changes. Red highlights and strikethroughs indicate the modifications.

Domain 6: Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies

- Internal (e.g., within organization control)
- External (e.g., outside organization control)
- Third-party (e.g., outside of enterprise control)
- Location (e.g., on-premise, cloud, hybrid)

6.2 Conduct security controls testing

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions/benchmarks
- Code review and testing
- Misuse case testing
- Coverage analysis
- Interface testing (e.g., user interface, network interface, Application Programming Interface (API))
- ~~Attack simulations~~
- Compliance checks

6.3 Collect security process data (e.g., technical, administrative)

- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster Recovery (DR) and Business Continuity (BC)

6.4 Analyze test/audit output and generate report

- Remediation
- Exception handling
- Responsible disclosure

6.5 Conduct or facilitate security audits

- Internal (e.g., within organization control)
- External (e.g., outside organization control)
- Third-party (e.g., outside of enterprise control)
- Location (e.g., on-premises, cloud, hybrid)

Changes in the right version:

- 6.2 Conduct security control testing**
 - ~~Penetration testing (e.g., red, blue, and pink/red teams)~~
 - ~~Attack simulations~~
- 6.4 Analyze test output and generate report**
 - ~~Responsible disclosure~~

Domain 7

7.1 子標題把調查技巧放在報告與文件化前面，以符合順序與邏輯。

7.2 多了 SOAR；Egress monitoring 多了舉例(DLP).

7.4 主標題多了舉例(Defense in Depth).

7.5 媒體保護技巧多了舉例；原子標題 Data at rest/data in transit 改成 data states, 並舉例(in use, in transit, at rest), 由二個狀態變成完整的資料三態。

7.7 白名單/黑名單的用字由 whitelisting/blacklisting 改成 allowlist/denylist; 第三方安全服務多了舉例(DDoS scrubbing 洗流量, 受管理安全服務供應商)；反惡意軟體(anti-malware) 改成端點保護並舉例(EDR, XDR)。

7.8 標題由弱點管理(vulnerability management)改成以弱點為基礎的管理(vulnerability based management)。

7.10 備份儲存策略的舉例多了不可更改(immutable)與加密(encrypted)；復原站點策略舉例多了溫站點(原本只有提到冷與熱站點)。

7.11 溝通的舉例多了排定優先順序(prioritization)；多了衡量指標(metrics)並舉例(MTTR, MTBF)，但 MTTR 這邊出現多了項目符號的排版錯誤。

7.12 DRP 測試把平行與全中斷這二個子標題合併成平行全中斷(Parallel Full interruption)，這可能是排版的錯誤，正確應該是二個獨立的子標題。溝通舉例改成內部/外部(原本是利害關係人、測試狀態與主管機關)。

7.14 實體安全原本分為週邊/邊界安全控制(perimeter security control)與內部安全控制，新版改成外部安全控制與內部安全控制，比較符合邏輯。

7.15 資安訓練與意識刪除舉例(內部威脅、社交媒體衝擊、雙因子驗證疲勞攻擊)

Domain 7: Security Operations 7.1 Understand and comply with investigations - Evidence collection and handling - Investigative techniques - Reporting and documentation 7.2 Conduct logging and monitoring activities - Intrusion Detection and Prevention (DPS) - Security Information and Event Management (SIEM) - Security Orchestration, Automation and Response (SOAR) - Continuous monitoring and tuning 7.3 Perform Configuration Management (CM) (e.g., provisioning, baselining, automation) 7.4 Apply foundational security operations concepts (e.g., <u>Defense in Depth (DID)</u>) - Need-to-know/least privilege - Separation of Duties (SoD) and responsibilities 7.5 Apply resource protection - Media management - Media protection techniques (e.g., <u>archiving, encryption, disposal/reuse</u>) 7.6 Conduct incident management - Detection - Response - Mitigation - Reporting	Domain 7: Security Operations 7.1 Understand and comply with investigations - Evidence collection and handling - Reporting and documentation - Investigative techniques 7.2 Conduct logging and monitoring activities - Intrusion detection and prevention (DPS) - Security information and event management (SIEM) - Continuous monitoring and tuning - Egress monitoring 7.3 Perform configuration management (CM) (e.g., provisioning, baselining, automation) 7.4 Apply foundational security operations concepts - Need-to-know/least privilege - Segregation of Duties (SoD) and responsibilities - Privileged account management 7.5 Apply resource protection - Media management - Media protection techniques 7.6 Conduct incident management - Detection - Response - Mitigation - Reporting
7.7 Operate and maintain detection and preventative measures - Firewalls (e.g., next generation, web application, network) - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) - Allow/denylist - Third-party provided security services (e.g., <u>Distributed Denial of Service (DDoS) scrubbing services, managed security service provider</u>) 7.8 Implement and support patch and vulnerability based management 7.9 Understand and participate in change management processes 7.10 Implement recovery strategies - Backup storage strategies (e.g., cloud storage, onsite, offsite, <u>immutable, encrypted</u>) - Recovery site strategies (e.g., cold vs. <u>warm</u> vs. hot, resource capacity agreements) 7.11 Implement Disaster Recovery (DR) processes - Response - Personnel - Communications (e.g., methods, prioritization) - Assessment - Restoration 7.12 Test disaster recovery plans (DRP) - Read-through/tabletop - Walkthrough - Simulation 7.13 Participate in Business Continuity (BC) planning exercises 7.14 Implement and manage physical security - External security controls 7.15 Address personnel safety and security concerns - Travel - Security training and awareness	7.7 Operate and maintain detection and preventative measures - Firewalls (e.g., next generation, web application, network) - Intrusion detection systems (IDS) and intrusion prevention systems (IPS) - Whitelisting/blacklisting - Third-party provided security services 7.8 Implement and support patch and vulnerability management 7.9 Understand and participate in change management processes 7.10 Implement recovery strategies - Backup storage strategies (e.g., cloud storage, onsite, offsite) - Recovery site strategies (e.g., cold vs. hot, resource capacity agreements) 7.11 Implement disaster recovery (DR) processes - Response - Personnel - Communications (e.g., methods) - Assessment 7.12 Test disaster recovery plans (DRP) - Read-through/tabletop - Walkthrough - Simulation - Parallel 7.13 Participate in Business Continuity (BC) planning and exercises 7.14 Implement and manage physical security - Perimeter security controls - Internal security controls 7.15 Address personnel safety and security concerns - Travel - Security training and awareness

Domain 8

8.1 新增 SSDF 與 SBOM，以及左移(shift left)。我們課程強調全面品質管理，把左移視為落伍的觀念，因此完全不談左移。

8.2 程式語言多了舉例(memory safe 及物件導向)。

8.4 Open source 多了舉例(軟體組成分析 SCA)。雲服務多了 FaaS。

8.5 刪除軟體定義安全(software-defined security)，改放在 4.1。

Domain 8: Software Development Security

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

- Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framework)
- Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
- Operation and maintenance
- Change management
- Integrated Product Team
- Secure Software Development Framework (SSDF) and Software Bill of Materials (SBOM) requirements
- Shift left

8.2 Identify and apply security controls in software development ecosystems

- Programming languages (e.g., memory safe, object-oriented)
- Libraries
- Tool sets
- Integrated Development Environment
- Runtime
- Continuous Integration and Continuous Delivery (CI/CD)
- Software configuration management (CM)
- Code repositories
- Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))

8.3 Assess the effectiveness of software security

- Auditing and logging of changes
- Risk analysis and mitigation

8.4 Assess security impact of acquired software

- Commercial-Off-The-Shelf (COTS)
- Open source (e.g., Software Composition Analysis (SCA))
- Third-party
- Managed services (e.g., enterprise applications)
- Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Function as a Service (FaaS))

8.5 Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of Application Programming Interfaces (API)
- Secure coding practices

2026 Changes (Green Annotations):

- Added: Software configuration management (CM)
- Added: Code repositories
- Added: Application security testing (e.g., static application security testing (SAST), dynamic application security testing (DAST), software composition analysis, ~~source code review~~)
- Added: Continuous Integration and Continuous Delivery (CI/CD)
- Added: Managed services (e.g., enterprise applications)
- Added: Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Function as a Service (FaaS))
- Added: Secure coding practices