Prepared by: VIJAY VASOYA (vdvin@yahoo.com)

CHANGES TO THE CBK IN MAY 2021

This list isn't perfect, but it's a first pass look at what's new, removed, updated, or changed in the Common Body of Knowledge (CBK) as of May 1st, 2021. It doesn't align perfectly with ISC2's exam outline, so just keep that in mind; there are a lot of new topics to learn.

Domain	Topic	Status
1	Privacy shield	removed
1	Prudent actions	NEW
1	Reasonable actions	NEW
1	Data portability	NEW
1	Data localization	NEW
1	Privacy and e-discovery	NEW
1	GDPR privacy tenets	NEW
1	Public chapter (public domain)	NEW
1	unilateral NDA	NEW
1	bilateral NDA	NEW
1	multilateral NDA	NEW
1	non-compete agreement (NCA)	NEW
1	Risk: asset based, outcomes based, vulnerability based, and threat based	NEW
1	Hazard	NEW
1	Risk response	updated
1	Risk Maturity Modeling	NEW
1	micro training	NEW
1	Gamification	NEW (literally 1 sentence)
2	IT asset management lifecycle	NEW
2	Assets: materials/supplies	NEW
2	Assets: tangible/intangible	NEW
2	Kiosk service points	NEW
2	Data security lifecycle	NEW
2	Media marking?	NEW
2	Data in transit risk/recommendations	NEW
2	Pervasive encryption	NEW
2	Data lifecycle	NEW
2	Data location	NEW
2	Data maintenance	NEW
2	End of Life and End of Support	NEW
2	DRM	changed
2	Data classification policy	removed?
3	Confusion	removed
3	Diffusion	removed
3	Avalanche	removed
3	Key clustering	removed
3	Synchronous	removed
3	Asynchronous	removed
3	Meet-in-the-middle (2DES attack)	removed
3	DES/AES	reduced
3	Secure defaults	NEW
3	Fail securely	NEW
3	Keep it simple	NEW
3	Zero trust	NEW

3	Privacy by design	NEW
3	Trust but verify	NEW
3	Shared responsibility	NEW
3	Virtualized Systems	NEW
3	Hypervisor types	NEW
3	Government cloud	NEW
3	Microservices	NEW
3	VM Sprawl	NEW
3	Application container	NEW
3	Serverless systems	NEW-1 paragraph
3	High performance systems	NEW
3	Edge and Fog Computing Architectures	NEW
3	Edge Computing and Fog Computing Vulnerabilities and Mitigations	NEW
3	Quantum Cryptography	NEW
3	Key space clumping	NEW
3	Clustering?	NEW
3	Deterministic decryption	NEW
3	Cryptographic Systems Architecture	NEW
3	Bulk Encryption	NEW
3	Digital envelope	NEW
3	Complex Hybrid Cryptography	NEW
3	Public Key Infrastructure (PKI)	Updated
3	Hash	updated
3	Distributed ledger (DL) technology	NEW
3	blockchain	NEW
3	Key Management	Updated
3	Pass the hash	NEW-1 sentence
3	Threat Modeling and Internetworking	NEW
3	Kill Chains	NEW
3	Code signing	removed
3	Avalanche	removed
4	Packet loss	removed
4	Jitter	removed
4	Sequence error	removed
4	VOIP	reduced
4	Bound/unbound networks	NEW
4	LiFi	NEW
4	Acoustic wave	NEW
4	line driver	NEW
4	Amplifiers	NEW
4	Multiplexers	NEW
4	dense-wave division multiplexers (DWDMs)	NEW
4	Concentrators	NEW
4	Infiniband	NEW
4	RADSL	NEW
4	Broadband Over Powerline (BPL)	Expanded
4	frequency division multiplexing	NEW
4	WiMAX	NEW
4	Physical Layer and the Protocol Stack	NEW
4	Threats and Countermeasures to Physical Layer of OSI Model	Updated

4	PPPoE	NEW
4	Address Resolution Protocol	Updated
4	Fibre/Channel/Fibre Channel over Ethernet (FCoE)	Updated
4	Load Management	NEW
4	arbitration or deconfliction	NEW
4	polling protocols	NEW
4	contention-based protocols	NEW
4	Layer 2 Threats and Countermeasures	Updated
4	Anycast transmission	NEW
4	Geocast transmission	NEW
4	Automatic Private IP Addressing (APIPA)	NEW
4	distance vector, path vector, link-state	NEW
4	3 groups of routing protocols	NEW
4	Classical/classless	NEW
4	RIP, RIPv3, RIPing	NEW
4	Path vector protocols	NEW
4	Border gateway protocols	NEW
4	IS-IS protocol	NEW
4	Threats and Countermeasures to Network Layer	Updated
4	Threats and Countermeasures to Transport Layer	Updated
4	Layer 5 Threats and Countermeasures	Updated
4	Threats and Countermeasures to Presentation Layer	Updated
4	OSI Layer 7: Application Layer: Hypertext Transfer Protocol (HTTP and HTTPS)	NEW
4	DHCP	Updated
4	DNS	Updated
4	Should There Be a Layer 8?	NEW
4	Threats and Countermeasures to Application Layer	Updated
4	Legacy remote access	NEW
4	Zero Trust vs. Trust, but Verify	NEW
4	Zero Trust Architectures	NEW
4	microsegmentation of networks	NEW
4	root of trust or ROT	NEW
4	Immutability	NEW
4	NAC	Updated
4	802.1X NAC	NEW
4	NAC frameworks/best practices	NEW
4	NAC baselines/audits	NEW
4	VOIP	Reduced
4	Captive Portals	NEW
4	Wireless attacks	NEW
4	Legacy IRC	NEW
4	ZIGBEE	MISSING
4	VXLAN (Virtual Extensible LAN)	MISSING
4	Pure silica	removed
4	code-division multiple access	removed
5	Identity lifecycle	NEW
5	Privilege manager	removed
5	Provisioning	NEW
5	Accounting	NEW
5	User behavior review	NEW
5	Job or duties review-privil. creep	NEW

5	Disable and deprovision	NEW
5	Permission aggregation	NEW
5	Security identifiers	NEW
5	Privilege escalation	NEW
5	Vertical privilege escalation	NEW
5	Horizontal privilege escalation	NEW
5	Lateral movement	NEW
5	IAAA	NEW
5	CIANA + PS	NEW
5	Security models combined with AC models (BLP, Biba, MAC, DAC, etc.)	NEW
5	Strong star property	NEW
5	Risk based access control (RiBAC)	NEW
5	Dual custody	NEW
5	Access Control as a System	NEW
5	Logical access control	Expanded
5	Physical access control systems	Expanded
5	Facilities	Expanded
5	Identity Store	NEW
5	Just in time identity	NEW
5	Self-service	NEW
5	Identity management	NEW
5	FIM	NEW
5	Access Control Technologies and Devices	Updated
5	Biometrics: Who Are You	reduced; no longer lists retina scan, vein patterns, etc.
5	SSO	NEW
5	Just in time identity	NEW
5	Human/non-human users	NEW
5	Escalation	NEW
5	De-escalation	NEW
5	Real-time	NEW
5	Full identity lifecycle	NEW
5	Privileged account management (PAM)	NEW
5	Privileged session management	NEW
5	Endpoint privilege management	NEW
5	Remote helpdesk	NEW
5	Session Management	NEW
5	Kerberos	NEW
5	Kerberos Tickets	NEW
5	Goal of Kerberos	NEW
5	Drawbacks of Kerberos	NEW
5	OpenID and Authentication and OpenID Connect	NEW
5	Linear succession of attributes	removed
5	Identity governance	removed
6	Audits/assessments: formal vs informal	NEW
6	Finding attributes: condition, criteria, cause, effect, recommendation	NEW
6	no notice assessment	NEW
6	NIST Risk Management Framework SP 800-37r2	NEW
6	NIST Cybersecurity Framework	NEW

6	**ISO 27000**	**NEW**
6	**Service Organization Control (SOC) Reports**	**NEW**
6	**Trust service criteria**	**NEW**
6	**SOC Reports for Clouds and Data Centers**	**NEW**
6	**Planning and Conducting a SOC Audit**	**NEW**
6	**SAS 70**	**NEW**
6	**International Adoption of SSAE**	**NEW**
6	**Internal Audit and Assessment**	**NEW**
6	**External Audit and Assessment**	**NEW**
6	**integrated audits**	**NEW**
6	**forensic audits**	**NEW**
6	**information systems audits**	**NEW**
6	**compliance, financial, operating audits**	**NEW**
6	**Third-Party Audit and Assessment**	**NEW**
6	**Managed Services and Security Assessment**	**NEW**
6	**NCSC 12 principles**	**NEW**
6	**supply chain risk management**	**NEW**
6	**ISO 28000-series**	**NEW**
6	**Control Assessment Methods and Tools**	**NEW**
6	**Judgmental sampling**	**NEW**
6	**Interview and Testing**	**NEW**
6	**Compliance and Substantive Testing**	**NEW**
6	**Testing Perspectives**	**NEW**
6	**Code Review and Testing**	**Updated**
6	**Ethical Penetration Testing**	**NEW**
6	**Rules of Engagement -ROE**	**NEW**
6	**Ethical pentest vs. Ethical hacking**	**NEW**
6	**bug bounty**	**NEW**
6	**Blind/Double-blind test**	**NEW**
6	**Ethical Penetration Testing – Basic Methodology**	**NEW**
6	**Continuous Full-Cycle Testing**	**NEW**
6	**Chaos engineering**	**NEW**
6	**Service-level agreement validation**	**NEW**
6	**Synthetic Transactions in Practice**	**NEW**
6	**Security Education, Training and Awareness**	**NEW**
6	**Backup Verification Data**	**NEW**
6	**BCDR**	**Updated**
6	**Desk check (removed in 2018)**	**NEW**
6	**Full Cutover (full interruption)**	**NEW**
6	**Remediation**	**NEW**
6	**CPI models**	**NEW**
6	**plan-do-check-act**	**NEW**
6	**six sigma**	**NEW**
6	**Exception Handling**	**NEW**
6	**Ethical Disclosure**	**NEW**
6	**Non-Disclosure**	**NEW**
6	**Full Disclosure**	**NEW**
6	**Responsible Disclosure**	**NEW**
6	**Mandatory Reporting**	**NEW**
6	**Whistleblowing**	**NEW**
7	Vulnerability testing	changed/combined
7	Penetration testing	changed/combined

7	Overt/covert	removed
7	White hat testing	removed
7	Black hat testing	removed
7	Third party	changed/combined
7	Internal/external	changed/combined
7	Black/white/grey box	removed
7	Information lifecycle	changed/combined (new is “data security lifecycle”, Domain 2)
7	Incident management	changed/combined
7	Log Management	NEW
7	Pattern matching	NEW
7	Threat Hunting and IDS/IPS	NEW
7	endpoint detection and response (EDR)	NEW
7	extended detection and response (XDR)	NEW
7	AGILITY	NEW
7	Security Information and Event Management (SIEM)	Updated
7	self hosted, self-managed SIEM, Cloud SIEM	NEW
7	Hybrid self-hosted	NEW
7	SIEM as a service	NEW
7	Real-Time Monitoring	NEW
7	Continuous Monitoring	updated
7	Information Security Continuous Monitoring (ISCM)	NEW
7	precursors	NEW
7	Threat Intelligence: external/internal	NEW
7	User and Entity Behavior Analytics (UEBA)	NEW
7	MITRE’s ATT&CK Framework	NEW
7	Monitoring Limitations	NEW
7	CHANGE MANAGEMENT	new, updated from configuration management
7	Change Enablement	NEW
7	Change Initiation	NEW
7	Change Review and Approval	NEW
7	Implementation and Change Evaluation	NEW
7	Release and Deployment Planning and Control	NEW
7	Major Change Management Activities – Patch Management	updated
7	Security Baselining	NEW
7	Configuration Automation	NEW
7	Change Management Board (CMB)	NEW
7	Incident management	Combined with Incident Response
7	Incident Response Standards	NEW
7	Cyber Forensics	NEW
7	forensic readiness	NEW
7	Incident management/response:Preparation, detection, analysis, response, and review and improvement	NEW
7	Security Operations Center	NEW
7	Security Orchestration, Automation, and Response (SOAR)	NEW
7	Security orchestration	NEW
7	security automation	NEW

7	Allowed vs. Blocked List	NEW
7	Fourth generation firewall	NEW
7	Ransomware and Ransom Attacks	NEW
7	Machine Learning and Artificial Intelligence (AI) Based Tools	NEW
7	Software-defined security (SDS)	NEW
7	SDS and Assessment	NEW
7	Backup Minimum Protection	NEW
7	3-2-1 backup strategy	NEW
7	Cloud Backup-as-a-Service	NEW
7	Crime Prevention through Environmental Design (CPTED)	NEW
7	“broken window” concept	NEW
7	Contact devices (switches)	NEW
7	Solid core/Hollow-core	NEW
7	Turnstiles	NEW
7	Building Codes	NEW
7	Restricted and Work Area Storage	NEW
7	sensitive compartmented information facilities (SCIFs)	NEW
7	American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) publishes the ANSI/ASHRAE Standard 90.4-2019	NEW
7	High density	NEW
7	ionization	NEW
7	photoelectric	NEW
7	Very Early Smoke Detection Apparatus, or VESDA	NEW
7	The 5 fire classification types	NEW – brought back from old CBK
7	Aqueous Firefighting Foam (AFFF)	NEW
7	Non-conductive, nontoxic liquid suppressants	NEW
7	Travel: condition monitoring	NEW
7	MDM	NEW
7	Bricking	NEW
7	Operationalizing Frameworks	NEW
7	Privacy Management Framework (PMF)	NEW
7	HITRUST Common Security and Privacy Framework (CSF)	NEW
7	SWIFT	NEW
7	Cloud Security Alliance Internet of Things SCF	NEW
7	Digital Forensics Tools, Tactics, and Procedures	NEW
7	BC Standards	NEW
7	National Institute of Standards and Technology Special Publication 800-34	NEW
7	International Organization of Standardization (ISO) 223XX Series	NEW
7	Maximum Allowable Outage or MAO	NEW
7	Business continuity Lessons Learned	NEW
8	Development Time vs. The Impact of Errors	NEW
8	Waterfall Software Lifecycle Development (SDLC) Model	NEW
8	Business Impact Per Stage vs. Cost to Change	NEW
8	Software Design and Coding Errors	NEW
8	Shared Responsibility	NEW
8	Security baked in	NEW

8	Partnership for Systems Approaches to Safety and Security (PSASS)	NEW
8	Designing and Writing Software	NEW
8	Emerging properties	NEW
8	Source vs Executable Code	NEW
8	Intermediate code	NEW
8	Arbitrary code	NEW
8	Nested	NEW
8	Code reuse	NEW
8	Refactoring	NEW
8	Data modeling	NEW
8	Data quality standards and practices	NEW
8	Level of abstraction	NEW
8	Lower order languages	NEW
8	High (or higher)-order languages (HOL)	NEW
8	Data type enforcement	NEW
8	Data protection or data hiding	NEW
8	Code protection or logic hiding	NEW
8	Assembly language	NEW
8	Compiled languages	NEW
8	Interpreted languages	NEW
8	constraint-based or logic programming	NEW
8	Standard Libraries, Other Libraries, and Software Reuse	NEW
8	Business needs: consult, ask, evaluate, agree, document	NEW
8	Controls for Incomplete Parameter Checking and Enforcement	NEW
8	memory leak	NEW
8	Data-centric Vulnerabilities	NEW
8	Between-the-Lines	NEW
8	Bypass attacks	NEW
8	Compromising database views used for access control	NEW
8	Exploits against alternative, but not quite equivalent, access routes	NEW
8	Data contamination	NEW
8	Improper modification of information	NEW
8	Query attacks	NEW
8	Data lakes	NEW
8	data farms	NEW
8	Network Database Management Model	Updated
8	CODASYL model, created by the Conference on Data Systems Languages	NEW
8	Parallel processing	NEW
8	Graph databases	NEW
8	candidate key	NEW
8	Non-relational Databases (NoSQL)	NEW
8	Connecting Apps to Databases	NEW
8	probabilistic method	NEW
8	statistical approach	NEW
8	Deviation and trend analysis	NEW
8	Baking in security (a few modules)	NEW
8	Protecting Against Ransomware and Ransom Attacks	NEW

8	**Cross-Disciplinary Methods, Integrated Product Team (IPT), and Integrated Product and Process Development (IPPD)**	**NEW**
8	**Strong Data Typing and Structure Enforcement by Programming Language**	**NEW**
8	**strongly typed**	**NEW**
8	**weakly typed**	**NEW**
8	**Limit Reuse to Trusted Libraries**	**NEW**
8	**REST**	**Updated**
8	**Tools, Integrated Development Environments (IDEs)**	**Updated**
8	**Security controls in software development ecosystems**	**NEW**
8	**Security of Code Repositories**	**NEW**
8	**Continuous Integration (CI) and Continuous Delivery (CD)**	**NEW**
8	**Software Assurance Policy**	**NEW**
8	**Software Assurance During Acquisition Phases**	**NEW**
8	**Orphaned Software and Systems Security Assessment**	**NEW**
8	**Mergers and Acquisitions Special Issues Regarding Software, Databases, and Systems Security Assessment**	**NEW**
8	**Commodity Systems**	**NEW**
8	**Joint analysis development**	**removed**
8	**rapid application development**	**removed**
8	**Exploratory model**	**removed**

1.2.1 Confidentiality, integrity, availability, authenticity, and nonrepudiation

- [Authenticity is a newly listed item, nonrepudiation is new in Domain 1, it also still appears as non-repudiation in 3.6]

1.9.3 Onboarding, transfers, and termination processes

- [“transfers” is new in 2021]

1.10.6 Control assessments (security and privacy)

- [Privacy control assessments is new, and this sub-sub-topic is renamed from 2018 1.9.6 “Security Control Assessment (SCA)”]

1.10.9 Continuous improvement (e.g., Risk maturity modeling)

- [“Risk maturity modeling” is new for 2021]

1.12 Apply Supply Chain Risk Management (SCRM) concepts

- [SCRM is new in 2021]

1.13.1 Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)

- [“social engineering, phishing, security champions, gamification” are new topics in 2021]

DOMAIN 2: ASSET SECURITY

2.3 Provision resources securely

- [new in 2021]

2.3.2 Asset inventory (e.g., tangible, intangible)
["tangible, intangible" new in 2021]
2.4 Manage data lifecycle

[new in 2021, potentially renamed and moved from 2018 7.5.5 Information lifecycle]
2.4.1 Data roles (i.e., owners, controllers, custodians, processors, users/subjects)

[new in 2021]
2.4.2 Data collection

[new in 2021]
2.4.3 Data location

[new in 2021]
2.4.4 Data maintenance

[new in 2021]
2.4.5 Data retention

[new in 2021]
2.4.6 Data destruction

[new in 2021]
2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

["EOL" and "EOS" are new in 2021]
2.6.1 Data states (e.g., in use, in transit, at rest)

["in use, in transit, at rest" data states are new in 2021]
2.6.4 Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))

[DLP and CASB new in 2021]

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

3.1.2 Least privilege

[new for 2021 and present in 7.4.1]
3.1.3 Defense in depth

[new in 2021]
3.1.4 Secure defaults

[new in 2021]
3.1.5 Fail securely

[new in 2021]

3.1.7 Keep it simple

[new in 2021]
3.1.8 Zero Trust

[new in 2021]
3.1.9 Privacy by design

[new in 2021]
3.1.10 Trust but verify

[new in 2021]
3.1.11 Shared responsibility

[new in 2021]
3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

["Biba, Star Model, Bell-LaPadula" new in 2021]
3.5.6 Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

[SaaS, IaaS, and PaaS new in 2021]
3.5.9 Microservices

[new in 2021]
3.5.10 Containerization

[new in 2021]
3.5.11 Serverless

[new in 2021]
3.5.13 High-Performance Computing (HPC) systems

[new in 2021]
3.5.14 Edge computing systems

[new in 2021]
3.5.15 Virtualized systems

[new in 2021]
3.6.2 Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)

["quantum" new in 2021]
3.6.5 Digital signatures and digital certificates

["Digital certificates" new in 2021]
3.7.1 Brute force

[new in 2021]
3.7.2 Ciphertext only

[new in 2021]

3.7.3 Known plaintext

[new in 2021]
3.7.4 Frequency analysis

[new in 2021]
3.7.5 Chosen ciphertext

[new in 2021]
3.7.6 Implementation attacks

[new in 2021]
3.7.7 Side-channel

[new in 2021]
3.7.8 Fault injection

[new in 2021]
3.7.9 Timing

[new in 2021]
3.7.10 Man-in-the-Middle (MITM)

[new in 2021]
3.7.11 Pass the hash

[new in 2021]
3.7.12 Kerberos exploitation

[new in 2021]
3.7.13 Ransomware

[new in 2021]
3.9.9 Power (e.g., redundant, backup)

[new in 2021]

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

4.1.2 Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)

[IPSec, IPv4, and IPv6 new in 2021]
4.1.3 Secure protocols

[new in 2021]
4.1.5 Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))

[FCoE, iSCSI, and VoIP new in 2021]
4.1.6 Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))

[Micro-segmentation, VXLAN, encapsulation, and SD-WAN new in 2021]
4.1.7 Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)

[Li-Fi, Zigbee, and satellite new in 2021]
4.1.8 Cellular networks (e.g., 4G, 5G)

[new in 2021]
4.2.1 Operation of hardware (e.g., redundant power, warranty, support)

[new in 2021]
4.3.6 Third-party connectivity

[new in 2021]

DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT (IAM)

5.1.5 Applications

[new in 2021]
5.2.5 Registration, proofing, and establishment of identity

[“Establishment of identity” new in 2021]
5.2.8 Single Sign On (SSO)

[new in 2021]
5.8.9 Just-In-Time (JIT)

[new in 2021]
5.3.3 Hybrid

[new in 2021]
5.4.6 Risk based access control

[new in 2021]
5.5.1 Account access review (e.g., user, system, service)

[“service” new in 2021]
5.5.2 Provisioning and deprovisioning (e.g., on /off boarding and transfers)

[“on /off boarding and transfers” new in 2021]
5.2.3 Role definition (e.g., people assigned to new roles)

[new in 2021]
5.2.4 Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)

[new in 2021]
5.6 Implement authentication systems

[new in 2021]
5.6.1 OpenID Connect (OIDC)/Open Authorization (Oauth)

[new in 2021]
5.6.2 Security Assertion Markup Language (SAML)

[new in 2021]
5.6.3 Kerberos

[new in 2021]
5.6.4 Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)

[new in 2021]

DOMAIN 6: SECURITY ASSESSMENT AND TESTING

6.2.9 Breach attack simulations

[new in 2021]
6.2.10 Compliance checks

[new in 2021]
6.4.1 Remediation

[new in 2021]
6.4.2 Exception handling

[new in 2021]
6.4.3 Ethical disclosure

[new in 2021]

DOMAIN 7: SECURITY OPERATIONS

7.1.5 Artifacts (e.g., computer, network, mobile device)

[new in 2021]
7.2.5 Log management

[new in 2021]
7.2.6 Threat intelligence (e.g., threat feeds, threat hunting)

[new in 2021]
7.2.7 User and Entity Behavior Analytics (UEBA)

[new in 2021]
7.3 Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

[new in 2021]
7.7.1 Firewalls (e.g., next generation, web application, network)

[“next generation, web application, network” new in 2021]
7.7.8 Machine learning and Artificial Intelligence (AI) based tools

[new in 2021]
7.11.7 Lessons learned

[new in 2021]

DOMAIN 8: SOFTWARE DEVELOPMENT SECURITY

8.1.1 Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps)
[“Agile, Waterfall, DevOps, DevSecOps” are new in 2021]

8.1.2 Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
[CMM and SAMM are new in 2021]

8.2.1 Programming languages
[new in 2021]

8.2.2 Libraries
[new in 2021]

8.2.3 Tool sets
[new in 2021]

8.2.4 Integrated Development Environment (IDE)

[new in 2021]
8.2.5 Runtime

[new in 2021]
8.2.6 Continuous Integration and Continuous Delivery (CI/CD)

[new in 2021]
8.2.7 Security Orchestration, Automation, and Response (SOAR)

[new in 2021]
8.2.10 Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))

[new in 2021]
8.4.1 Commercial-off-the-shelf (COTS)

[new in 2021]
8.4.2 Open source

[new in 2021]
8.4.3 Third-party

[new in 2021]
8.4.4 Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

[new in 2021]
8.5.4 Software-defined security

Upon close inspection you might recognize that some of these "new" topics are already covered or are reasonable expansions of the domains. Many of the "new" topics should be familiar to any current cybersecurity professional. Be sure to focus on these topics in your preparation as they may be slightly more prevalent in exam questions than "legacy" topics.
Note: Please refer to the full 2021 CISSP Certification Exam Outline for the complete current topic list.

Rewording issues to review

In addition to the actual new items on the 2021 CISSP exam, there are numerous rewordings of topics and detailed items. In addition to rewording, there is also some re-organization and renumbering of items. Since those have little to no impact on the exam or your preparations, I have only highlighted a few of those items that were moved or renamed that are noteworthy. I did not include items where acronyms were added or hyphenation changed.

Here is a list of some potentially important rewordings or location changes:

Domain 1: Security and Risk Management

- Understand, adhere to, and promote professional ethics
  [was promoted to 1.1 from 1.5 in order to emphasis the importance of ethics]
- 1.4 Determine compliance and other requirements
  [revised 2018 1.3, and "Determine compliance requirements" removed from 2018 1.2.6]
- 1.5 Understand legal and regulatory issues that pertain to information security in a holistic context
  [changed from 2018 1.4 "global context"]
- 1.6 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
  [this was topic 2018 7.2, 7.2.1-7.2.5]
- 1.10.6 Control assessments (security and privacy)
  [renamed from 2018 1.9.6 "Security Control Assessment (SCA)"]
- 1.12 Apply Supply Chain Risk Management (SCRM) concepts
  [renamed from 2018 1.11 "Apply risk-based management concepts to the supply chain"]

Domain 2: Asset Security

- 2.2 Establish information and asset handling requirements
  [moved from 2018 2.6]
- 2.3.1 Information and asset ownership
  [renamed from 2018 2.2 "Determine and maintain information and asset ownership"]
- 2.3.2 Asset inventory (e.g., tangible, intangible)
  [moved from 2018 7.4.2]
- 2.3.3 Asset Management
  [moved from 2018 7.4.2]
- 2.4.1 Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
  [renamed from 2018 2.3.1 Data owners and 2.3.2 Data processors]
- 2.4.2 Data collection
  [renamed from 2018 2.3.4 Collection limitation]
- 2.6 Determine data security controls and compliance requirements
  [renamed from 2018 2.5 Determine data security controls]
- 2.6.1 Data states (e.g., in use, in transit, at rest)
  [renamed from 2018 2.5.1 Understand data states]
- 2.6.4 Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))

[DRM moved from 2018 3.9.9, this item is also renamed from 2018 2.5.4]

Domain 3: Security Architecture and Engineering

- 3.1 Research, implement and manage engineering processes using secure design principles
  [renamed from 2018 3.1]
- 3.1.1 Threat modeling
  [renamed and moved from 2018 1.10, 1.10.1, and 1.10.2]
- 3.1.6 Separation of Duties (SoD)
  [also included in 7.4.2]
- 3.5.12 Embedded systems
  [renamed from 2018 3.8 Assess and mitigate vulnerabilities in embedded devices]
- 3.6 Select and determine cryptographic solutions
  [renamed from 2018 3.9 Apply cryptography]
- 3.7 Understand methods of cryptanalytic attacks
  [moved from 2018 3.9.8]

Domain 4: Communication and Network Security

- 4.1.9 Content Distribution Networks (CDN)
  [moved and renamed from 2018 4.2.5]
- 4.1.6 Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
  [SDN moved and renamed from 2018 4.1.5]

Domain 5: Identity and Access Management (IAM)

- 5.3 Federated identity with a third-party service
  [renamed from 2018 5.3.3]
- 5.5.1 Account access review (e.g., user, system, service)
  [renamed from 2018 5.5.1 and 5.5.2]

Domain 6: Security Assessment and Testing

- None

Domain 7: Security Operations

- 7.5.2 Media protection techniques
  [renamed from 2018 7.6.2 Hardware and software asset management]

Domain 8: Software Development Security

- 8.2.8 Software Configuration Management (SCM)
  [renamed from 2018 8.2.2]
- 8.2.9 Code repositories
  [renamed from 2018 8.2.3]

REMOVED ITEMS

There are several items that were removed or at least not retained in the 2021 version of the CISSP exam. While these items are removed from the 2021 CISSP Certification Exam Outline, that does not typically mean the topic is not on the 2021 exam. Most of the dropped items were removed because the topics are included in other topics already and their removal is resolving unnecessary repetition. Also, all number references in this list are from the 2018 Exam Outline since these items are not present in the 2021 CISSP Certification Exam Outline.

Domain 1: Security and Risk Management

1.9.8 Asset valuation

[Removed from 2021, but still relevant to overall topic]

1.10.1 Threat modeling methodologies

[This sub-sub-topic was removed for 2021, but it is still contained in the 1.11 Understand and apply threat modeling concepts and methodologies sub-domain.]

1.10.2 Threat modeling concepts

[This sub-sub-topic was removed for 2021, but it is still contained in the 1.11 Understand and apply threat modeling concepts and methodologies sub-domain.]

Domain 2: Asset Security

- 2.3 Protect privacy

[This sub-topic was removed for 2021, but it is contained in other 2021 topics, including 1.4.2, 1.5.5, 1.9.6, 1.10.6, and 3.1.9]

Domain 3: Security Architecture and Engineering

- 3.6 Assess and mitigate vulnerabilities in web-based systems

[This sub-topic was removed for 2021, but likely still relevant to the exam]

- 3.7 Assess and mitigate vulnerabilities in mobile systems

[This sub-topic was removed for 2021, but likely still relevant to the exam]

Domain 4: Communication and Network Security

None

Domain 5: Identity and Access Management (IAM)

None

Domain 6: Security Assessment and Testing

None

Domain 7: Security Operations

None

Domain 8: Software Development Security

8.2.1 Security of the software environments, [Removed in 2021, but still relevant to 2021- ***8.2 Identify and apply security controls in software development ecosystems***]

WHAT TO KNOW ABOUT THE CISSP-CAT PROCESS?

The legacy original CISSP exam was a paper-based, bubble-sheet test consisting of 250 questions to be completed in a six-hour time window. With the 2015 revision, the CISSP exam was available as a computer-based testing (CBT) option through Pearson VUE testing locations, but it retained the question count and time limit of its predecessor. With the 2018 revision, (ISC)2 adopted the current CISSP-CAT mode of exam delivery.

The CISSP-CAT is the current mode or method of exam delivery employed by (ISC)2 for the English version of the exam. CAT stands for Computer Adaptive Test. The CISSP-CAT only applies to the English version of the exam. For non-English versions, the linear 250-question, six-hour version is still used.

In the CISSP-CAT format, the student will view a minimum of 100 questions and a maximum of 150 with a three-hour time limit. Of the first 100 questions, only 75 are graded and count towards your score. The 25 ungraded questions are not marked, and are interspersed throughout the first 100 questions. These questions are used to evaluate questions for future tests. Rather than working towards accumulating points to cross a line to pass, (ISC)2 evaluates your ability to demonstrate knowledge in relation to a concept called the passing standard. (ISC)2 does not publicly define what the level of achievement is to surpass the passing standard. However, it is most likely scoring 70% or greater within each of the eight domains.

At question 100, the system evaluates your potential to achieve the passing standard. If the system estimates your pass potential is 95% or higher, the test will end with a pass. If the system estimates your failure potential is 95% or higher, the test will end with a fail result. If a 95%+ pass/fail determination cannot be made at question 100, then it is evaluated again after each question until you reach question 150. You are only assessed on the last 75 graded questions. This means that as you answer question 101, the first graded question is discarded and replaced with question 101. Then as you answer question 102, the second originally graded question is discarded and replaced with question 102, and so forth. As a question is “dropped” from being considered towards your pass/fail potential, it is replaced by a question of the same domain. This is how the exam maintains the domain coverage percentages.

Don’t skip questions

You get one chance to view a question and provide an answer. You cannot revisit previous questions. Although it is not stated, a skipped question is likely marked as incorrect. Therefore, guessing is still a better strategy than skipping. You should always attempt to eliminate question options from consideration, then select your answer from the remaining options.

In early 2021, (ISC)2 announced that they are performing a pilot test for performing the CISSP exam through an online remote proctoring system. (ISC)2 has remained one of last major certification entities that had not adopted a remote examination and online proctoring process for taking their certification exams. Based on the results of their preliminary pilot program which will occur in Feb 2021, (ISC)2 may elect to offer online remote proctored testing for CISSP and other (ISC)2 certs in the future. The statements released by (ISC)2 about the program indicate that the remote online exam will be a linear (i.e., not adaptive) 250 question six-hour exam, and you will not be able to revisit questions once an answer is submitted. For more information on this, visit the (ISC)2 blog and other relevant links:
https://blog.isc2.org/isc2_blog/
https://www.isc2.org/Exams/online-proctor-pilot-test-FAQ
https://www.isc2.org/News-and-Events/Press-Room?

Why the test revisions?

(ISC)2 references several factors that led to the deployment of the CISSP-CAT examination format, such as:

- A more precise evaluation
- Shorter test sessions
- Enhanced exam security

Additionally, there has been a significant increase in exam fraud worldwide over the last decade, including both tester impersonations as well as attempts to steal copies of the question bank. (ISC)2 and other test owners are using a wide range of techniques to reduce fraud while increasing certification value.

The CISSP-CAT is a reasonable defense against stolen test banks. This is also one of the primary reasons why (ISC)2 has not offered online testing in the past. But, with the COVID-19 pandemic changing how the world works and improvements in remote exam verification and monitoring processes, (ISC)2 is considering this more convenient mode of exam delivery.

CISSP exam tips

The 2021 CISSP exam questions seem to have the same level of depth and complexity as previous versions, with only a handful of new topics. The CISSP-CAT testing method or structure itself is often the most daunting part of achieving the certification for those who sit the exam.

(ISC)2 claims that the assessment of a candidate's knowledge and mastery of relevant topics is equivalent between the CISSP-CAT and the traditional flat version of the exam. However, I think there is an increased requirement to be knowledgeable across all eight domains rather than only needing to be proficient in six on the traditional flat or linear version.

On legacy linear versions, you needed to answer enough questions correct to accumulate a score above the minimum to pass. This seemed to allow a tester to score poorly in two domains, while scoring well in the other six and still achieving a passing score. The CISSP-CAT testing mode evaluates the tester in all eight domains and in order to pass you must achieve the "passing standard" in each domain.

Some training and exam preparation guidance for previous versions of the exam seem to indicate that you could overlook or ignore one or two domains that you found overly challenging and focus on the six domains that were more comfortable to the test taker. I don't think this is now a valid and responsible strategy for passing the CISSP exam. Therefore, you may need to spend additional time studying and preparing for the CISSP exam to ensure you are well-versed in most topics across all eight domains.