0	CA1-005 Objective	Details	CA1-005
1	Governance, Risk, and Compliance		1.0
3	Given a set of organizational security requirements, implement the appropriate governance components		1.1
4		Security program documentation	1.1
5		Policies	1.1
6		Procedures	1.1
7		Standards	1.1
8		Guidelines	1.1
9		Security program management	1.1
10		Awareness and training	1.1
11		Phishing (training)	1.1
12		Security (training)	1.1
13		Social engineering (training)	1.1
14		Privacy (training)	1.1
15		Operational security (training)	1.1
16		Situational awareness (training)	1.1
17		Communication	1.1
18		Reporting	1.1
19		Management commitment	1.1
20		Responsible, accountable, consulted, and informed (RACI) matrix	1.1
21		Governance frameworks	1.1
22		Control Objectives for Information and Related Technologies (COBIT)	1.1
23		Information Technology Infrastructure Library (ITIL)	1.1
24		Change/configuration management	1.1
25		Asset management life cycle	1.1
26		Configuration management database (CMDB)	1.1
27		Inventory	1.1
28		Governance risk and compliance (GRC) tools	1.1
29		Mapping (GRC tools)	1.1
30		Automation (GRC tools)	1.1
31		Compliance tracking (GRC tools)	1.1
32		Documentation (GRC tools)	1.1
33		Continuous monitoring (GRC tools)	1.1
34		Data governance in staging environments	1.1
35		Production	1.1
36		Development	1.1
37		Testing	1.1
38		Quality assurance (QA)	1.1
39		Data life cycle management	1.1
41	Given a set of organizational security requirements, perform risk management activities		1.2
42		Impact analysis	1.2
43		Extreme but plausible scenarios	1.2
44		Risk assessment and management	1.2
45		Quantitative vs. qualitative analysis	1.2
46		Risk assessment frameworks	1.2
47		Appetite/tolerance	1.2
48		Risk prioritization	1.2
49		Severity impact	1.2
50		Remediation	1.2
51		Validation	1.2

52		Third-party risk management	1.2
53		Supply chain risk	1.2
54		Vendor risk	1.2
55		Subprocessor risk	1.2
56		Availability risk considerations	1.2
57		Business continuity/disaster recovery	1.2
59		Backups	1.2
62		Confidentiality risk considerations	1.2
63		Data leak response	1.2
64		Sensitive/privileged data breach	1.2
65		Incident response testing	1.2
66		Reporting	1.2
67		Encryption	1.2
68		Integrity risk considerations	1.2
69		Remote journaling	1.2
70		Hashing	1.2
71		Interference	1.2
72		Antitampering	1.2
73		Privacy risk considerations	1.2
74		Data subject rights	1.2
75		Data sovereignty	1.2
76		Biometrics	1.2
77		Crisis management	1.2
78		Breach response	1.2
80	Explain how compliance affects information security strategies.		1.3
81		Awareness of industry-specific compliance	1.3
82		Healthcare	1.3
83		Financial	1.3
84		Government	1.3
85		Utilities	1.3
86		Industry standards	1.3
87		Payment Card Industry Data Security Standard (PCI DSS)	1.3
88		International Organization for Standardization/International Electrotechnical Commission (ISO/ IEC) 27000 series	1.3
89		Digital Markets Act (DMA)	1.3
90		Security and reporting frameworks	1.3
91		Benchmarks	1.3
92		Foundational best practices	1.3
93		Security Organization Control Type 2(SOC 2)	1.3
94		National Institute of Standards andTechnology Cybersecurity Framework (NIST CSF)	1.3
95		Center for Internet Security (CIS)	1.3
96		Cloud Security Alliance (CSA)	1.3
97		Audits vs. assessments vs. certifications	1.3
98		External audit	1.3
99		Internal audit	1.3
100		Privacy regulations	1.3
101		General Data Protection Regulation (GDPR)	1.3
102		California Consumer Privacy Act (CCPA)	1.3
103		General Data Protection Law (LGPD)	1.3
104		Children’s Online Privacy Act (COPPA)	1.3
105		Awareness of cross-jurisdictional compliance requirements	1.3

106		e-discovery	1.3
107		Legal holds	1.3
108		Due diligence	1.3
109		Due care	1.3
110		Export controls	1.3
111		Contractual obligations	1.3
114	Given a scenario, perform threat modeling activities.		1.4
115		Actor characteristics	1.4
116		Motivation	1.4
117		Financial	1.4
118		Geopolitical	1.4
119		Activism	1.4
120		Notoriety	1.4
121		Espionage	1.4
122		Resources	1.4
123		Time	1.4
124		Money	1.4
125		Capabilities	1.4
126		Supply chain access	1.4
127		Vulnerability creation	1.4
128		Knowledge	1.4
129		Exploit creation	1.4
130		Attack patterns	1.4
131		Frameworks	1.4
132		MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)	1.4
133		Common Attack Pattern Enumeration and Classification (CAPEC)	1.4
134		Cyber Kill Chain	1.4
135		Diamond Model of Intrusion Analysis	1.4
136		Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE)	1.4
137		Open Web Application Security Project (OWASP)	1.4
138		Attack surface determination	1.4
139		Architecture reviews	1.4
140		Data flows	1.4
141		Trust boundaries	1.4
142		Code reviews	1.4
143		User factors	1.4
144		Organizational change	1.4
145		Mergers	1.4
146		Acquisitions	1.4
147		Divestitures	1.4
148		Staffing changes	1.4
149		Enumeration/discovery	1.4
150		Internally and externally facing assets	1.4
151		Third-party connections	1.4
152		Unsanctioned assets/accounts	1.4
152		Cloud services discovery	1.4
153		Public digital presence	1.4
155		Abuse cases	1.4
156		Antipatterns	1.4
157		Attack trees/graphs	1.4

158		Modeling applicability of threats tthe organization/environment	1.4
159		With an existing system in place	1.4
161		Without an existing system in place	1.4
165	Summarize the information security challenges associated with artificial intelligence (AI) adoption		1.5
166		Legal and privacy implications	1.5
167		Potential misuse	1.5
168		Explainable vs. non-explainable models	1.5
169		Organizational policies on the use of AI	1.5
170		Ethical governance	1.5
171		Threats tthe model	1.5
172		Prompt injection	1.5
173		Unsecured output handling	1.5
174		Training data poisoning	1.5
175		Model denial of service (DoS)	1.5
176		Supply chain vulnerabilities	1.5
177		Model theft	1.5
178		Model inversion	1.5
179		AI-enabled attacks	1.5
180		Unsecure plugin design	1.5
181		Deep fake	1.5
182		Digital media	1.5
183		Interactivity	1.5
184		AI pipeline injections	1.5
185		Social engineering	1.5
186		Automated exploit generation	1.5
188		Risks of AI usage	1.5
189		Over-reliance	1.5
190		Sensitive information disclosure	1.5
191		Tthe model	1.5
192		From the model	1.5
193		Excessive agency of the AI	1.5
194		AI-enabled assistants/digital workers	1.5
195		Access/permissions	1.5
196		Guardrails	1.5
197		Data loss prevention (DLP)	1.5
198		Disclosure of AI usage	1.5
201	Security Architecture		2.0
202	Given a scenario, analyze requirements tdesign resilient systems.		2.1
203		Component placement and configuration	2.1
204		Firewall	2.1
205		Intrusion prevention system (IPS)	2.1
206		Intrusion detection system (IDS)	2.1
207		Vulnerability scanner	2.1
208		Virtual private network (VPN)	2.1
209		Network access control (NAC)	2.1
210		Web application firewall (WAF)	2.1
211		Proxy	2.1
212		Reverse proxy	2.1
213		Application programming interface (API) gateway	2.1
214		Taps	2.1

215		Collectors	2.1
216		Content delivery network (CDN)	2.1
217		Availability and integrity design considerations	2.1
218		Load balancing	2.1
219		Recoverability	2.1
220		Interoperability	2.1
221		Geographical considerations	2.1
222		Vertical vs. horizontal scaling	2.1
223		Persistence vs. non-persistence	2.1
226	Given a scenario, implement security in the early stages of the systems life cycle and throughout subsequent stages		2.2
227		Security requirements definition	2.2
228		Functional requirements	2.2
229		Non-functional requirements	2.2
230		Security vs. usability trade-off	2.2
231		Software assurance	2.2
232		Static application security testing (SAST)	2.2
233		Dynamic application security testing (DAST)	2.2
234		Interactive application security testing (IAST)	2.2
235		Runtime application self-protection (RASP)	2.2
236		Vulnerability analysis	2.2
237		Software composition analysis (SCA)	2.2
238		Software bill of materials (SBoM)	2.2
239		Formal methods	2.2
240		Continuous integration/continuous deployment (CI/CD)	2.2
241		Coding standards and linting	2.2
242		Branch protection	2.2
243		Continuous improvement	2.2
244		Testing activities	2.2
245		Canary	2.2
246		Regression	2.2
247		Integration	2.2
248		Automated test and retest	2.2
249		Unit	2.2
250		Supply chain risk management	2.2
251		Software	2.2
252		Hardware	2.2
253		Hardware assurance	2.2
254		Certification and validation process	2.2
255		End-of-life (EOL) considerations	2.2
257	Given a scenario, integrate appropriate controls in the design of a secure architecture		2.3
258		Attack surface management and reduction	2.3
259		Vulnerability management	2.3
260		Hardening	2.3
261		Defense-in-depth	2.3
262		Legacy components within an architecture	2.3
263		Detection and threat-hunting enablers	2.3
264		Centralized logging	2.3
265		Continuous monitoring	2.3
266		Alerting	2.3
267		Sensor placement	2.3

268		Information and data security design	2.3
269		Classification models	2.3
270		Data labeling	2.3
271		Tagging strategies	2.3
272		DLP	2.3
273		At rest	2.3
274		In transit	2.3
275		Data discovery	2.3
276		Hybrid infrastructures	2.3
277		Third-party integrations	2.3
278		Control effectiveness	2.3
279		Assessments	2.3
280		Scanning	2.3
281		Metrics	2.3
284	Given a scenario, apply security concepts tthe design of access, authentication, and authorization systems		2.4
285		Provisioning/deprovisioning	2.4
286		Credential issuance	2.4
287		Self-provisioning	2.4
288		Federation	2.4
289		Single sign-on (SSO)	2.4
290		Conditional access	2.4
291		Identity provider	2.4
292		Service provider	2.4
293		Attestations	2.4
294		Policy decision and enforcement points	2.4
295		Access control models	2.4
296		Role-based access control	2.4
297		Rule-based access control	2.4
298		Attribute-based access control (ABAC)	2.4
299		Mandatory access control (MAC)	2.4
300		Discretionary access control (DAC)	2.4
301		Logging and auditing	2.4
302		Public key infrastructure (PKI) architecture	2.4
303		Certificate extensions	2.4
304		Certificate types	2.4
305		Online Certificate Status Protocol (OCSP) stapling	2.4
306		Certificate authority/registration authority (CA/RA)	2.4
307		Templates	2.4
308		Deployment/integration approach	2.4
309		Access control systems	2.4
310		Physical	2.4
311		Logical	2.4
314	Given a scenario, securely implement cloud capabilities in an enterprise environment		2.5
315		Cloud access security broker (CASB)	2.5
316		API-based CASB	2.5
317		Proxy-based CASB	2.5
318		Shadow IT detection	2.5
319		Shared responsibility model	2.5
320		CI/CD pipeline	2.5
321		Terraform	2.5

322		Ansible	2.5
323		Package monitoring	2.5
324		Container security	2.5
325		Container orchestration	2.5
326		Serverless	2.5
327		Workloads	2.5
328		Functions	2.5
329		Resources	2.5
330		API security	2.5
331		Authorization	2.5
332		Logging	2.5
333		Rate limiting	2.5
334		Cloud vs. customer-managed	2.5
335		Encryption keys	2.5
336		Licenses	2.5
337		Cloud data security considerations	2.5
338		Data exposure	2.5
339		Data leakage	2.5
340		Data remanence	2.5
341		Unsecured storage resources	2.5
342		Cloud control strategies	2.5
343		Proactive	2.5
344		Detective	2.5
345		Preventative	2.5
346		Customer-to-cloud connectivity	2.5
347		Cloud service integration	2.5
348		Cloud service adoption	2.5
351	Given a scenario, integrate ZerTrust concepts intsystem architecture design		2.6
352		Continuous authorization	2.6
353		Context-based reauthentication	2.6
354		Network architecture (zertrust)	2.6
355		Segmentation	2.6
356		Microsegmentation	2.6
357		VPN	2.6
358		Always-on VPN	2.6
359		API integration and validation	2.6
360		Asset identification, management, and attestation	2.6
361		Security boundaries	2.6
362		Data perimeters	2.6
363		Secure zone	2.6
364		System components (zertrust)	2.6
365		Deperimeterization	2.6
366		Secure access service edge (SASE)	2.6
367		Software-defined wide area network (SD-WAN)	2.6
368		Software-defined networking	2.6
369		Defining subject-object relationships	2.6
372	Security Engineering		3.0
373	Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment		3.1
374		Subject access control	3.1
375		User (subject access control)	3.1

376		Process (subject access control)	3.1
377		Device (subject access control)	3.1
378		Service (subject access control)	3.1
379		Biometrics (subject access control)	3.1
380		Secrets management	3.1
381		Tokens (secret management)	3.1
382		Certificates (secret management)	3.1
383		Passwords (secret management)	3.1
384		Keys (secret management)	3.1
385		Rotation (secret management)	3.1
386		Deletion (secret management)	3.1
387		Conditional access	3.1
388		User-to-device binding	3.1
389		Geographic location	3.1
390		Time-based	3.1
392		Attestation	3.1
393		Cloud IAM access and trust policies	3.1
394		Logging and monitoring	3.1
395		Privilege identity management	3.1
396		Authentication and authorization	3.1
397		Security Assertions Markup Language (SAML)	3.1
398		OpenID	3.1
399		Multifactor authentication (MFA)	3.1
400		SSO	3.1
401		Kerberos	3.1
402		Simultaneous authentication of equals (SAE)	3.1
403		Privileged access management (PAM)	3.1
404		Open Authorization (OAuth)	3.1
405		Extensible Authentication Protocol (EAP)	3.1
406		Identity proofing	3.1
407		Institute for Electrical and Electronics Engineers (IEEE) 802.1X	3.1
408		Federation	3.1
411	Given a scenario, analyze requirements tenhance the security of endpoints and servers		3.2
412		Application control	3.2
413		Endpoint detection response (EDR)	3.2
414		Event logging and monitoring	3.2
415		Endpoint privilege management	3.2
416		Attack surface monitoring and reduction	3.2
417		Host-based intrusion protection system/ host-based detection system (HIPS/ HIDS)	3.2
418		Anti-malware	3.2
419		SELinux	3.2
420		Host-based firewall	3.2
421		Browser isolation	3.2
422		Configuration management	3.2
423		Mobile device management (MDM) technologies	3.2
424		Threat-actor tactics, techniques, and procedures (TTPs)	3.2
425		Injections	3.2
426		Privilege escalation	3.2
427		Credential dumping	3.2
428		Unauthorized execution	3.2

429		Lateral movement	3.2
430		Defensive evasion	3.2
432	Given a scenario, troubleshoot complex network infrastructure security issues		3.3
433		Network misconfigurations	3.3
434		Configuration drift	3.3
435		Routing errors	3.3
436		Switching errors	3.3
437		Unsecure routing	3.3
438		VPN/tunnel errors	3.3
439		IPS/IDS issues	3.3
440		Rule misconfigurations	3.3
441		Lack of rules	3.3
442		False positives/false negatives	3.3
443		Placement	3.3
444		Observability	3.3
445		Domain Name System (DNS) security	3.3
446		Domain Name System Security Extensions (DNSSEC)	3.3
447		DNS poisoning	3.3
448		Sinkholing	3.3
449		Zone transfers	3.3
450		Email security	3.3
451		Domain Keys Identified Mail (DKIM)	3.3
452		Sender Policy Framework (SPF)	3.3
453		Domain-based Message Authentication Reporting & Conformance (DMARC)	3.3
454		Secure/Multipurpose Internet Mail Extension (S/MIME)	3.3
455		Transport Layer Security (TLS) errors	3.3
456		Cipher mismatch	3.3
457		PKI issues	3.3
458		Issues with cryptographic implementations	3.3
459		DoS/distributed denial of service (DDoS)	3.3
460		Resource exhaustion	3.3
461		Network access control list (ACL) issues	3.3
464	Given a scenario, implement hardware security technologies and techniques		3.4
465		Roots of trust	3.4
466		Trusted Platform Module (TPM)	3.4
467		Hardware Security Module (HSM)	3.4
468		Virtual Trusted Platform Module (vTPM)	3.4
469		Security coprocessors	3.4
470		Central processing unit (CPU) security extensions	3.4
471		Secure enclave	3.4
472		Virtual hardware	3.4
473		Host-based encryption	3.4
474		Self-encrypting drive (SED)	3.4
475		Secure boot	3.4
476		Measured boot	3.4
477		Self-healing hardware	3.4
478		Tamper detection and countermeasures	3.4
479		Threat-actor TTPs	3.4
480		Firmware tampering	3.4
481		Shimming	3.4

482		Universal Serial Bus (USB)-based	3.4
483		Basic input/output system/Unified Extensible Firmware Interface (BIOS/UEFI)	3.4
484		Memory	3.4
485		Electromagnetic interference (EMI)	3.4
486		Electromagnetic pulse (EMP)	3.4
489	Given a set of requirements, secure specialized and legacy systems against threats.		3.5
490		Operational technology (OT)	3.5
491		Supervisory control and data acquisition (SCADA)	3.5
492		Industrial control system (ICS)	3.5
493		Heating ventilation and air conditioning (HVAC)/environmental	3.5
494		Internet of Things (IoT)	3.5
495		System-on-chip (SoC)	3.5
496		Embedded systems	3.5
497		Wireless technologies/radifrequency (RF)	3.5
498		Security and privacy considerations	3.5
499		Segmentation	3.5
500		Monitoring	3.5
501		Aggregation	3.5
502		Hardening	3.5
503		Data analytics	3.5
504		Environmental systems	3.5
505		Regulatory	3.5
506		Safety	3.5
507		Industry-specific challenges	3.5
508		Utilities	3.5
509		Transportation	3.5
510		Healthcare	3.5
511		Manufacturing	3.5
512		Financial	3.5
513		Government/defense	3.5
514		Characteristics of specialized/legacy systems	3.5
515		Unsecurable	3.5
516		Obsolete	3.5
517		Unsupported	3.5
518		Highly constrained	3.5
521	Given a scenario, use automation tsecure the enterprise.		3.6
522		Scripting	3.6
523		PowerShell	3.6
524		Bash	3.6
525		Python	3.6
526		Cron/scheduled tasks	3.6
527		Event-based triggers	3.6
528		Infrastructure as code (IaC)	3.6
529		Configuration files	3.6
530		Yet Another Markup Language (YAML)	3.6
531		Extensible Markup Language (XML)	3.6
532		JavaScript Object Notation (JSON)	3.6
533		Tom’s Obvious, Minimal Language (TOML)	3.6
534		Cloud APIs/software development kits (SDKs)	3.6
535		Web hooks	3.6

536		Generative AI	3.6
537		Code assist	3.6
538		Documentation	3.6
539		Containerization	3.6
540		Automated patching	3.6
541		Auto-containment	3.6
542		Security orchestration, automation, and response (SOAR)	3.6
543		Runbooks	3.6
544		Playbooks	3.6
545		Vulnerability scanning and reporting Security Content Automation Protocol (SCAP)	3.6
546		Open Vulnerability Assessment Language (OVAL)	3.6
547		Extensible Configuration Checklist Description Format (XCCDF)	3.6
548		Common Platform Enumeration (CPE)	3.6
549		Common vulnerabilities and exposures (CVE)	3.6
550		Common Vulnerability Scoring System (CVSS)	3.6
551		Workflow automation	3.6
554	Explain the importance of advanced cryptographic concepts.		3.7
555		Post-quantum cryptography (PQC)	3.7
556		Post-quantum vs. Diffie-Hellman and elliptic curve cryptography (ECC)	3.7
557		Resistance tquantum computing decryption attack	3.7
558		Emerging implementations	3.7
559		Key stretching	3.7
560		Key splitting	3.7
561		Homomorphic encryption	3.7
562		Forward secrecy	3.7
563		Hardware acceleration	3.7
564		Envelope encryption	3.7
565		Performance vs. security	3.7
566		Secure multiparty computation	3.7
567		Authenticated encryption with associated data (AEAD)	3.7
568		Mutual authentication	3.7
571	Given a scenario, apply the appropriate cryptographic use case and/or technique		3.8
572		Data at rest	3.8
573		Data in transit	3.8
574		Encrypted tunnels	3.8
575		Data in use/processing	3.8
576		Secure email	3.8
577		Immutable databases/blockchain	3.8
578		Non-repudiation	3.8
579		Privacy applications	3.8
580		Legal/regulatory considerations	3.8
581		Resource considerations	3.8
582		Data sanitization	3.8
583		Data anonymization	3.8
584		Certificate-based authentication	3.8
585		Passwordless authentication	3.8
586		Software provenance	3.8
587		Software/code integrity	3.8
588		Centralized vs. decentralized key management	3.8
589		Tokenization	3.8

590		Code signing	3.8
591		Cryptographic erase/obfuscation	3.8
592		Digital signatures	3.8
593		Obfuscation	3.8
594		Serialization	3.8
595		Hashing	3.8
596		One-time pad	3.8
597		Symmetric cryptography	3.8
598		Asymmetric cryptography	3.8
599		Lightweight cryptography	3.8
603	Security Operations		4.0
604	Given a scenario, analyze data tenable monitoring and response activities		4.1
605		Security information event management (SIEM)	4.1
606		Event parsing	4.1
607		Event duplication	4.1
608		Non-reporting devices	4.1
609		Retention	4.1
610		Event false positives/false negatives	4.1
611		Aggregate data analysis	4.1
612		Correlation	4.1
613		Audit log reduction	4.1
614		Prioritization	4.1
615		Trends	4.1
616		Behavior baselines and analytics	4.1
617		Network	4.1
618		Systems	4.1
619		Users	4.1
620		Applications/services	4.1
621		Incorporating diverse data sources	4.1
622		Third-party reports and logs	4.1
623		Threat intelligence feeds	4.1
624		Vulnerability scans	4.1
625		CVE details	4.1
626		Bounty programs	4.1
627		DLP data	4.1
628		Endpoint logs	4.1
629		Infrastructure device logs	4.1
630		Application logs	4.1
631		Cloud security posture management (CSPM) data	4.1
632		Alerting	4.1
633		False positives/false negatives	4.1
634		Alert failures	4.1
635		Prioritization factors	4.1
636		Impact	4.1
637		Asset type	4.1
638		Residual risk	4.1
639		Data classification	4.1
642		Reporting and metrics	4.1
643		Visualization	4.1
644		Dashboards	4.1

647	Given a scenario, analyze vulnerabilities and attacks, and recommend solutions treduce the attack surface		4.2
648		Vulnerabilities and attacks	4.2
649		Injection	4.2
650		Cross-site scripting (XSS)	4.2
651		Unsafe memory utilization	4.2
652		Race conditions	4.2
653		Cross-site request forgery	4.2
654		Server-side request forgery	4.2
655		Unsecure configuration	4.2
656		Embedded secrets	4.2
657		Outdated/unpatched software and libraries	4.2
658		End-of-life software	4.2
659		Poisoning	4.2
660		Directory service misconfiguration	4.2
661		Overflows	4.2
662		Deprecated functions	4.2
663		Vulnerable third parties	4.2
664		Time of check, time of use (TOCTOU)	4.2
665		Deserialization	4.2
666		Weak ciphers	4.2
667		Confused deputy	4.2
668		Implants	4.2
669		Mitigations	4.2
670		Input validation	4.2
671		Output encoding	4.2
672		Safe functions	4.2
673		Atomic functions	4.2
674		Memory-safe functions	4.2
675		Thread-safe functions	4.2
676		Security design patterns	4.2
677		Updating/patching	4.2
678		Operating system (OS)	4.2
679		Software	4.2
680		Hypervisor	4.2
681		Firmware	4.2
682		System images	4.2
683		Least privilege	4.2
684		Fail secure/fail safe	4.2
685		Secrets management	4.2
686		Key rotation	4.2
687		Least function/functionality	4.2
688		Defense-in-depth	4.2
689		Dependency management	4.2
690		Code signing	4.2
691		Encryption	4.2
692		Indexing	4.2
693		Allow listing	4.2
696	Given a scenario, apply threat-hunting and threat intelligence concepts.		4.3
697		Internal intelligence sources	4.3
698		Adversary emulation engagements	4.3

699		Internal reconnaissance	4.3
700		Hypothesis-based searches	4.3
701		Honeypots security	4.3
702		Honeynets	4.3
703		User behavior analytics (UBA)	4.3
704		External intelligence sources	4.3
705		Open-source intelligence (OSINT)	4.3
706		Dark web monitoring	4.3
707		Information sharing and analysis centers (ISACs)	4.3
708		Reliability factors	4.3
709		Counterintelligence and operational	4.3
710		Threat intelligence platforms (TIPs)	4.3
711		Third-party vendors	4.3
712		Indicator of compromise (IoC) sharing	4.3
713		Structured Threat Information eXchange (STIX)	4.3
714		Trusted automated exchange of indicator information (TAXII)	4.3
715		Rule-based languages	4.3
716		-Sigma	4.3
717		Yet Another Recursive Acronym (YARA)	4.3
718		Rita	4.3
719		Snort	4.3
720		Indicators of attack (threat intel)	4.3
721		TTPs (threat intel)	4.3
724	Given a scenario, analyze data and artifacts in support of incident response activities		4.4
725		Malware analysis	4.4
726		Detonation	4.4
727		IoC extractions	4.4
728		Sandboxing	4.4
729		Code stylometry	4.4
730		Variant matching	4.4
731		Code similarity	4.4
732		Malware attribution	4.4
733		Reverse engineering	4.4
734		Disassembly and decompilation	4.4
735		Binary	4.4
736		Byte code	4.4
737		Volatile/non-volatile storage analysis	4.4
738		Network analysis	4.4
739		Host analysis	4.4
740		Metadata analysis	4.4
741		Email header	4.4
742		Images	4.4
743		Audio/video	4.4
744		Files/filesystem	4.4
745		Hardware analysis	4.4
746		Joint test action group (JTAG)	4.4
747		Data recovery and extraction	4.4
748		Threat response	4.4
749		Preparedness exercises	4.4
750		Timeline reconstruction	4.4

751		Root cause analysis	4.4
752		Cloud workload protection platform (CWPP)	4.4
753		Insider threat	4.4
755		Netflow	x
756		SNMP	x
757		jumpbox	x
758		screened subnet	x
759		guest environment	x
760		staging environment	x
761		peer-to-peer	x
762		airgap	x
763		Customer relationship management (CRM)	x
764		Enterprise resource planning (ERP)	x
765		Content management system (CMS)	x
766		Enterprise service bus (ESB)	x
767		Development approaches	x
768		Agile	x
769		Waterfall	x
770		Spiral	x
771		Versioning	x
772		SecDevOps	x
773		Data loss prevention	x
774		DLP - Blocking use of external media - Print blocking	x
775		DLP - Remote Desktop	x
776		DLP - Protocol (RDP) blocking	x
777		DLP - Clipboard privacy controls	x
778		DLP - infrastructure (VDI) implementation	x
779		DLP - Restricted virtual desktop	x
780		DLP - Data classification blocking	x
781		DLP - Watermarking	x
782		DLP - Digital rights management (DRM)	x
783		DLP - deep packet inspection	x
784		DLP - Network traffic decryption/	x
785		Password policies	x
786		RADIUS	x
787		TACACS	x
788		HMAC-based one-time password (HOTP)	x
789		lime-based one-time password (TOTP)	x
790		cloud service models	x
791		SaaS	x
792		PaaS	x
793		IaaS	x
794		Object storage/file-based storage - Database storage	x
795		Block storage	x
796		Blob storage	x
797		Key-value pairs	x
798		Nano technology	x
799		Virtual reality / augmented reality	x
800		3D printing	x
801		Unsafe browser extensions	x

802		Flash plugins	x
803		ActiveX plugins	x
804		Asynchronous JavaScript and XML (AJAX)	x
805		Simple Object Access Protocol (SOAP)	x
806		Forensics process	x
807		Evidence collection	x
808		Chain of custody	x
809		Order of volatility	x
810		Evidence preservation	x
811		Forensics tools	x
812		Integrity preservation of evidence	x
813		File carving tools	x
814		Foremost	x
815		Strings	x
816		Binary analysis tools	x
817		Hex dump	x
818		Binwalk	x
819		Ghidra	x
820		GNU Project debugger (GDB) OllyDbg	x
821		readelf	x
822		objdump strace	x
823		ldd	x
824		file	x
825		Analysis tools	x
826		ExifTool	x
827		Nmap	x
828		Aircrack-ng	x
829		Volatility	x
830		The Sleuth Kit	x
831		Dynamically vs. statically linked	x
832		Imaging tools	x
833		Forensic Toolkit (FTK) Imager	x
834		dd	x
835		Hashing utilities	x
836		sha256sum ssdeep	x
837		Live collection vs. post-mortem tools	x
838		netstat -ps	x
839		vmstat ldd	x
840		lsof	x
841		netcat	x
842		tcpdump conntrack Wireshark	x
843		Given a scenario, apply secure configurations to enterprise mobility	x
844		Managed configurations	x
845		Application control Password	x
846		MFA requirements Token-based access Patch repository	x
847		Firmware Over-the-Air Remote wipe	x
848		WiFi	x
849		WiFi Protected Access (WPA2/3)	x
850		Device certificates Profiles	x
851		Bluetooth	x

852		Near-field communication (NFC) Peripherals	x
853		Geofencing	x
854		VPN settings	x
855		Geotagging	x
856		Certificate management Full device encryption	x
857		Tethering	x
858		Airplane mode	x
859		Location services	x
860		DNS over HTTPS (DoH)	x
861		Custom DNS	x
862		Deployment scenarios	x
863		Bring your own device (BYOD) Corporate-owned	x
864		Corporate owned,	x
865		personally enabled (COPE)	x
866		Choose your own device (CYOD)	x
867		Unauthorized remote activation/ deactivation of devices or features	x
868		Encrypted and unencrypted communication concerns	x
869		Physical reconnaissance	x
870		Personal data theft	x
871		Health privacy	x
872		Implications of wearable devices Digital forensics of collected data Unauthorized application stores Jailbreaking/rooting	x
873		Side loading	x
874		Containerization	x
875		Original equipment manufacturer	x
876		(OEM) and carrier differences Supply chain issues	x
877		eFuse	x
878		Secure Hashing Algorithm (SHA) Hash-based message	x
879		authentication code (HMAC) Message digest (MD)	x
880		RACE integrity primitives	x
881		evaluation message digest (RIPEMD) Poly1305	x
882		Galois/Counter Mode (GCM) Electronic codebook (ECB)	x
883		Cipher block chaining (CBC) Counter (CTR)	x
884		Output feedback (OFB)	x
885		Stream and block	x
886		Advanced Encryption	x
887		Standard (AES)	x
888		Triple digital encryption standard (3DES)	x
889		ChaCha	x
890		Salsa20	x
891		Diffie-Hellman	x
892		Elliptic-curve Diffie-Hellman	x
893		(ECDH) Signing	x
894		Digital signature algorithm (DSA) Rivest, Shamir, and Adleman (RSA)	x
895		Elliptic-curve signature algorithm (ECDSA)	x
896		Elliptic curve cryptography	x
897		P256	x
898		P384	x
899		Password-based key derivation function 2 (PBKDF2)	x
900		Bcrypt	x
901		- Total cost of ownership (TCO)	x

902		- Return on investment (ROI)	x
903		- Mean time to recovery (MTTR)	x
904		- Mean time between failure (MTBF)	x
905		- Annualized loss expectancy (ALE)	x
906		- Annualized rate of occurrence (ARO)	x
907		- Single loss expectancy (SLE)	x

CAS-004
4.1
4.1
4.1
x
x
x
4.1
x
x
x
x
x
x
x
x
x
4.3
x
x
4.2
2.4
1.3
2.4
x
x
x
x
x
x
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1
4.1

4.2
4.2
4.2
4.2
4.4
4.4
3.4
multi
multi
multi
2.7
multi
multi
multi
x
multi
multi
multi
multi
multi
4.3
multi
multi
multi
4.3
3.3
3.3
3.3
3.3
4.3
4.3
x
x
4.3
x
x
1.3
x
4.3
x
4.3
x
x
x
4.3
4.3
x
x
4.3
4.3

4.3
4.3
4.3
4.3
4.3
4.3
2.1
2.1
2.1
2.1
2.1
2.1
2.1
2.1
2.1
2.1
2.1
2.1
2.1
x
2.1
2.1
x
x
x
x
x
x
x
x
x
1.1
1.1
x
x
x
x
x
x
x
x
x
x
x

x
x
x
1.8
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
1.1
1.1
1.1
1.1
1.1
1.1
1.1
1.1
1.1
1.1
1.1
1.1

1.1
1.1
1.3
1.1
1.3
1.3
1.3
1.2
1.2
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
multi
2.4
x
x
1.3
1.3
x
x
1.3
x
1.3
1.3
1.3
1.3
x
x
x
x
x
x
2.5
3.2
3.2
3.2
x
x
3.2
3.2
3.2
3.2
1.1

multi
1.4
1.4
1.4
1.1
1.7
1.7
1.7
1.6
x
x
x
x
x
1.5
x
x
x
x
x
x
1.5
1.5
1.5
1.5
1.5
1.5
1.5
1.5
3.2
3.5
3.5
3.5
3.5
3.5
3.5
3.5
3.5
3.5
3.5
1.5
2.5
1.5
3.4
x
x
x
4.2
1.3
x

x
x
x
3.4
3.4
3.4
3.4
3.4
x
x
x
x
3.4
3.4
2.6
x
x
x
x
x
x
x
1.6
x
x
1.1
x
x
x
1.1
1.1
1.1
1.1
1.1
2.4
x
1.1
x
x
1.1
x
x
1.1
x
x
x

x
x
x
x
1.5
x
x
1.5
1.5
1.5
x
x
x
3.1
x
1.5
x
1.5
1.5
1.5
1.5
1.5
1.5
1.5
1.5
x
1.5
1.5
1.5
1.5
1.5
1.5
3.2
3.2
3.2
x
3.2
3.2
3.2
3.2
3.2
x
x
3.1
2.1
2.5
x
x
x

x
x
2.5
2.5
2.5
x
x
x
x
x
x
x
x
x
1.3
1.1
x
x
x
x
x
x
x
3.6
x
2.5
2.5
2.5
2.5
2.5
x
3.2
3.2
3.2
3.2
3.2
x
x
3.2
1.6
3.2
3.2
3.2
3.2
3.2
x
2.5
x
x

x
3.2
3.2
x
x
3.3
3.3
3.3
3.3
3.3
3.3
3.3
1.1
multi
1.1
1.1
3.2
x
2.6
2.6
x
3.3
3.3
3.3
3.3
3.3
3.3
3.3
3.3
x
x
x
x
x
2.6
2.6
2.6
2.6
2.6
2.7
x
x
x
x
x
x
x
x

x
x
x
x
x
2.7
2.7
2.7
2.7
x
2.3
2.3
2.3
2.3
2.3
2.7
2.7
x
x
x
x
3.6
x
1.8
3.6
x
x
3.7
1.8
x
x
1.7
1.7
multi
1.7
1.7
1.8
1.7
1.7
3.6
x
4.3
1.4
1.7
1.8
1.7
1.7
x
1.4

1.7
x
3.5
1.4
x
3.6
x
3.6
3.6
3.6
2.2
2.7
2.7
x
x
x
2.7
x
x
x
2.2
2.2
2.2
2.7
2.7
2.7
2.7
x
x
2.1
2.3
2.3
x
2.2
2.2
2.2
2.2
2.2
x
2.7
2.7
2.7
2.7
4.1
4.1
4.1
1.4
x
x
x

2.5
2.5
2.5
2.5
2.5
2.5
x
2.5
2.5
2.5
2.5
2.5
2.5
2.5
2.5
2.5
2.5
2.5
x
2.5
x
x
2.5
x
x
x
2.6
x
x
1.3
3.2
2.3
2.3
2.3
3.2
2.3
2.3
4.1
x
x
3.7
x
x
2.4
1.3
x
2.6
2.6
2.6
2.6

2.6
2.6
2.6
2.6
x
x
2.1
2.1
2.3
x
x
x
x
x
x
x
x
x
x
x
x
x
x
x
2.6
x
1.3
x
x
x
x
2.4
2.4
2.4
2.4
2.8
2.8
2.8
2.8
2.8
2.8
2.8
2.8
2.8
2.8
x
2.7
2.7
2.7
x

x
x
2.1
1.1
1.1
1.1
1.1
1.1
1.1
1.1
1.1
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.3
1.5
1.5
1.5
1.5
1.5
1.6
1.6
1.6
1.6
1.6
1.6
1.6
1.6
1.8
1.8
1.8
2.5

2.5
2.5
2.5
2.5
2.8
2.8
2.8
2.8
2.8
2.8
2.8
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
2.9
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1

3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.1
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
3.6
4.1

4.1
4.1
4.1
4.1
4.1
4.1