Certified in Cybersecurity

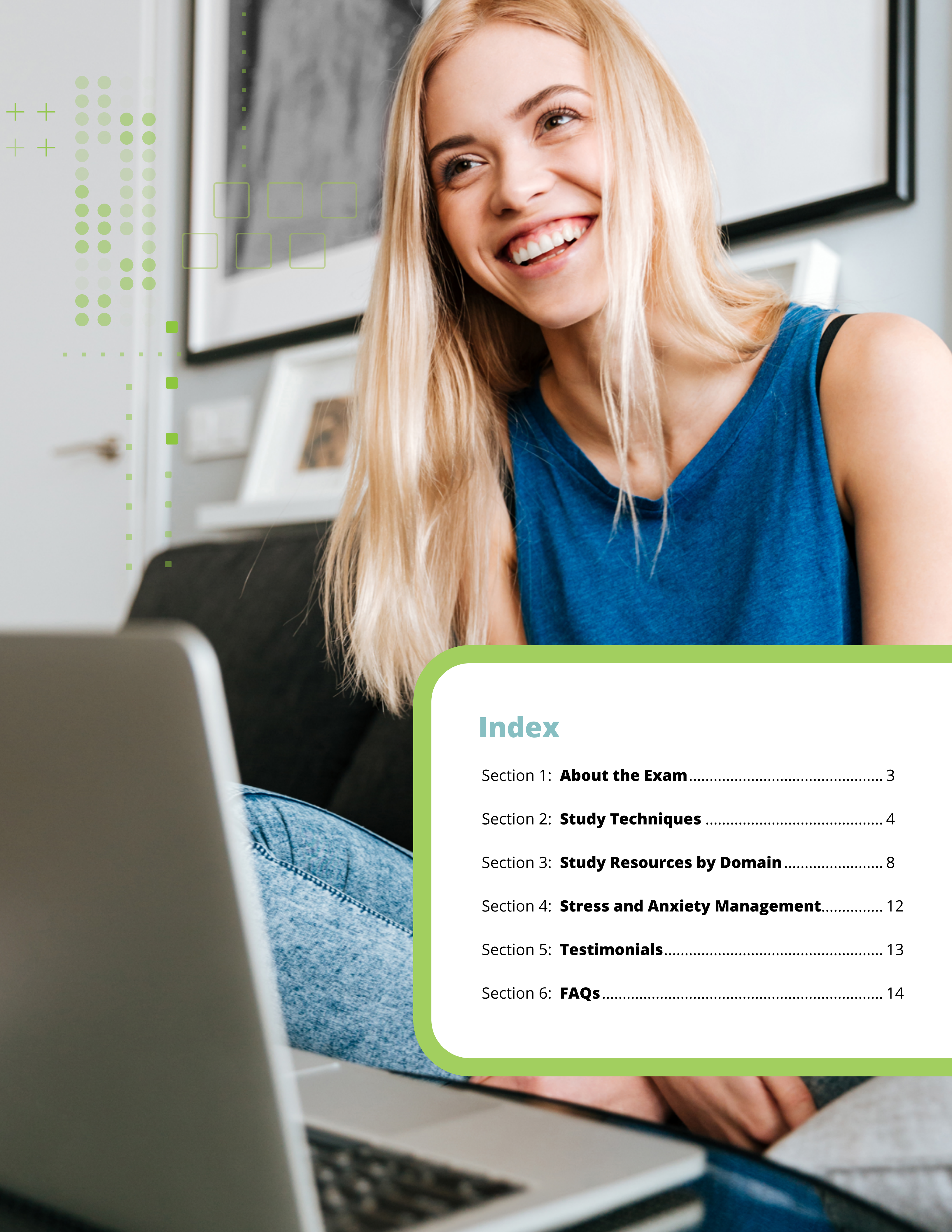
ISC2 Certification

Study Pack

As you study for the **Certified in Cybersecurity (CC) exam**, it helps to have a game plan for success. This CC Study Pack organizes the information you need to know prior to the exam and outlines the exam structure to help you build confidence for the big day.

Use this CC Study Pack to organize your time, study materials and state of mind to make test prep a reasonable reality instead of an unbearable load. Remember, cybersecurity is one of the most in-demand careers today, and those entering the field have their pick of professional opportunities around the globe. Currently, **4 million jobs** remain unfilled, with the gap predicted to widen to as many as **85 million workers by 2030**.

To help close the cybersecurity workforce gap, ISC2 is offering **FREE Certified in Cybersecurity (CC) Online Self-Paced Training and an exam** to 1 million people. Passing the CC exam could be your ticket to an exciting career in cybersecurity, and this CC Study Pack is here to help you succeed on exam day.



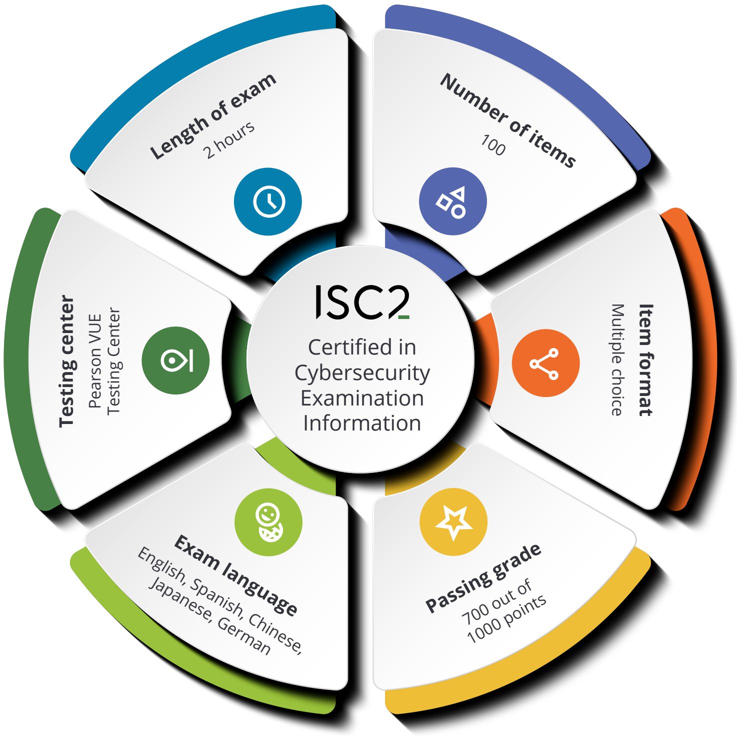
Index

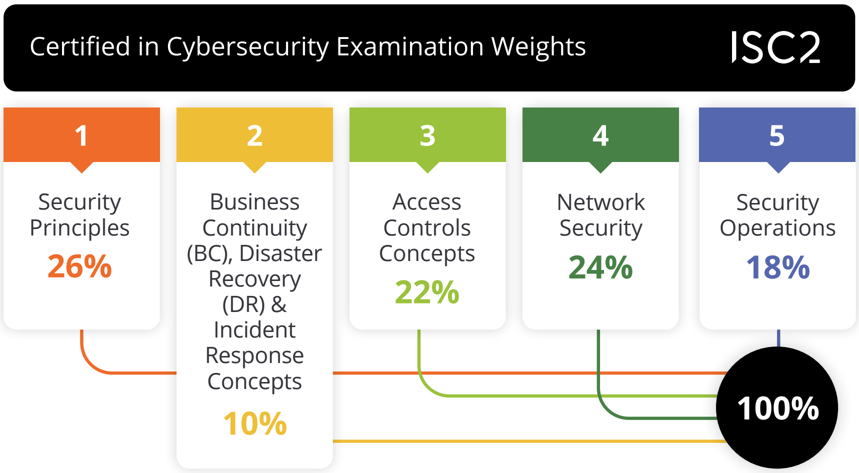
What to Expect

The CC Exam contains 100 total multiple-choice items related to five different domains:

1. **Domain 1:** Security Principles (26%)
2. **Domain 2:** Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts (10%)
3. **Domain 3:** Access Controls Concepts (22%)
4. **Domain 4:** Network Security (24%)
5. **Domain 5:** Security Operations (18%)

You'll have two hours to complete the exam and will need a minimum 70% accuracy to pass. The test is offered in English, Chinese, Japanese, German and Spanish and can be taken at **Pearson VUE testing centers** worldwide. Review the FAQs at the end of this Study Pack for pricing, registration and more.





ISC2 Dedicated Resources

Don’t go it alone. ISC2 has dedicated resources designed to help you succeed on exam day.

1. **Get the Official ISC2 CC eTextbook** | Leverage our **eTextbook** as your go-to resource and get a comprehensive review of the exam topics as you build confidence for exam day.

2. **Join the CC Study Group** | This open discussion forum for those studying for the CC Exam includes nearly 800 members. Post a question to the community or break off into small groups to study.

3. **Jump into the ISC2 Community** | If you struggle, don’t struggle alone. Tap into the value of a community of like-minded learners who have passed exams just like this one. Join the ISC2 community to ask, contribute, and establish connections that will serve you throughout your cybersecurity career.

4. **Leverage ISC2 Training Partners** | You’ll access to the most up-to-date course content from ISC2. Our Official ISC2 Training Partners around the globe are ready to provide convenient access to the ISC2 training that meets your needs.

5. **Your ISC2 Self-Study Tools** | Helpful exam prep resources include:

- **Official CC Flash Cards**
- **Official CC Practice Quiz**

A user of the ISC2 self-paced study tools herself, **Vickie Gray**, Owner of GrayMatter Governance Risk and Compliance Training and Consulting, Ltd., noted:

“I found the self-paced training very straightforward and very useful and very clear. One thing in particular that I liked was that the videos have transcripts, so I was able to read the transcript and watch the video, then review the content and take sample exams. I would highly recommend the ISC2 materials for that.”

Study Tips

While there is no one-size-fits-all solution for studying, below are some common practices that can help. Want more? Check out these **Study Tips and Tricks that Really Work**!

- **Identify your learning style** | If you don't already know it, find your unique learning style and work with it. Consider courses you've done well in. How did the professor teach, and what methods worked well for you? If you don't already know your learning style, online resources like the **VARK Questionnaire** (as cited in **scholarly research articles**) can help.

- **Auditory learner** | Use text-to-speech apps to listen as you read along or close your eyes and visualize as you listen to videos on current study topics. Talk out loud and pretend you are teaching the concept to others.

- **Visual learner** | Draw diagrams of technical topics and how they interrelate - and keep your eyes open for study videos. Re-copy textbook visuals and **even use AI** to generate helpful flowcharts.

- **Kinaesthetic learner** | Walk around the room as you review your notes, scroll through your eTextbook, or listen to videos and lectures. Explain concepts to yourself (or a patient friend) and use your hands to gesture as you do so. Throw a ball against the wall, or perform some other repetitive movement, while you ponder security principles and role-play when topics are tough.

- **Reading/writing learner** | Go to a quiet, uninterrupted space and curl up with your textbook. It may help to read and digest an entire section before breaking for notes. When you do write your flashcards, try to do them from memory. If you can't write the flashcard from memory, read the passage again.

Certified ISC2 members say that multimodal learning – hearing, seeing, taking notes, and engaging – works the best to cement learning. Lean on your learning style but use multiple inputs to maximize retention.

- **Repeat. Repeat. Repeat.** | Remember, repetition is the mother of all learning styles, so carve out a dedicated chunk of time to quiz yourself on what you learned the day before. The more you associate with the information, the more those synapses will fire, and the synapses that fire together, wire together.

- **Want to Learn? Teach.** | The "Protege Effect" suggests the best way to learn something is to teach it. If you want to make sure you know a topic forward and backward, join a study group and teach it to your peers. As the Roman philosopher Seneca stated, "When we teach, we learn."

Don’t Take Our Word for It: Study Tips from CC Veterans

One of the best sources of wisdom is other cybersecurity experts who have taken the CC course, taught it, or otherwise met this career milestone themselves. Here’s what some of them have to say.

*“**Don’t overload yourself just before the day of the exam**. Maybe have a few notes or a few topics that you want to just look at quickly the day before the exam. But at that point, you should be pretty well prepared and confident in your understanding of the concepts and the topics.”*

- **Dwayne Natwick**,
CEO/Principal Training Architect at
Captain Hyperscaler, LLC.

*“**The important thing is to know yourself**. Are you a morning person or an evening person? Do you like quiet, or do you prefer having headphones on with music? All those things contribute to how you make a plan for studying...*

*My advice is that **the more you can simulate the exam experience, the better you’ll get** at doing it. Embrace the anxiety in a controlled environment where you can just calm yourself. Anxiety comes from something in the future that is unknown. So whatever you can do to make the unknown into a known entity is going to help.”*

- **Vickie Gray**,
Owner of GrayMatter Governance Risk and Compliance
Training and Consulting, Ltd.

Tips for Neurodivergent Learners

Neurodivergent learners will fall under one or more of the unique learning styles mentioned above, so put all studying within the context that works for you. However, certain other elements will necessarily apply. Consider these learning techniques:

- **Honor the basics** | Sleep, hydration and a good meal: all are important to eliminate internal distractions. Taking prescribed medications is also key to priming your brain to focus. Now is not the time to get off track.

- **Know yourself** | When does your brain do its best work? If that's not 8 am, don't worry — time your study based on when your mind is most alert.

- **Remember your tolerance levels** | How much can your attention span handle before information starts to blur at the edges? Take breaks between sessions, even long ones. The point is to reset completely and eliminate mental stress.

The key for neurodivergent learners is adaptability. Work for your unique capabilities and allow yourself to be curious as to what those are. Knowing when and how you perform best will serve you for the rest of your life.

The **Certified in Cybersecurity (CC) Online Self-Paced Training** course reviews each domain in-depth and is FREE as part of our **One Million Certified in Cybersecurity** pledge. Below you will find an overview of the topics covered in each domain.

As **Vickie Gray**, fellow CC veteran notes, *"The ISC2 study materials are very accessible because of the way the content is structured with a case study that flows through the whole training. The variety of different learning styles and ways of being exposed to the content is really quite impressive."*

Domain 1: Security Principles

In Domain 1, learners will discover the foundational concepts of cybersecurity, including the CIA Triad: Confidentiality, Integrity, and Availability. They will review foundational concepts of information assurance and risk management, learn the different types of security controls, demonstrate the relationship among elements of governance and analyze appropriate outcomes per the ISC2 Code of Ethics.

After completing this domain, learners will be able to:

- Discuss the foundational concepts of cybersecurity principles.
- Recognize foundational security concepts of information assurance.
- Define risk management terminology and summarize the process.
- Relate risk management to personal or professional practices.
- Classify types of security controls.
- Distinguish between policies, procedures, standards, regulations and laws.
- Demonstrate the relationship among governance elements.
- Analyze appropriate outcomes according to the canons of the ISC2 Code of Ethics when given examples.
- Practice the terminology and review security principles.

Key topics include:

- Identity Assurance
- Privacy Control Mechanisms
- Safeguarding Data
- Strategic Risk Management

Additional Resources

- **Click here for Domain 1 Chapter Terms and Definitions**.
- **Click here for Domain 1 Flashcards**.

Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response

In Domain 2, students will learn about the Availability component of the CIA Triad. They will be taught the importance of incident response, disaster recovery, and business continuity in securing the availability of data and be encouraged to remember that:

Incident response helps navigate unexpected changes in operating conditions.

- Business continuity is the backup plan that enables the company to continue operating despite the changes.
- Disaster recovery is implemented when the above plans fail, and the organization must quickly resolve its state of crisis.

The important thing to remember is that cybersecurity is not only about ensuring data protection but the lives of those to whom that data belongs. Coworkers, customers and friends rely on cybersecurity experts to keep their information safe.

After completing this domain, learners will be able to:

- Explain how organizations respond to, recover from and continue to operate during unplanned disruptions.
- Recall the terms and components of incident response.
- Summarize the components of a business continuity plan.
- Identify the components of disaster recovery.
- Practice the terminology of and review incident response, business continuity and disaster recovery concepts.

Key topics include:

- Recovery Strategies
- Continuity Strategies
- Incident Management

Additional Resources

- **Click here for Domain 2 Chapter Terms and Definitions**.
- **Click here for Domain 2 Flashcards**.

Domain 3: Access Controls Concepts

In Domain 3, learners will be introduced to both physical and logical controls and their roles in strengthening overall security. They will learn not only how to assess different physical access controls and assign the proper control in a given situation, but understand why access control is necessary, how it is managed, and who gets access to what.

After completing this domain, learners will be able to:

- Select access controls that are appropriate in a given scenario.
- Relate access control concepts and processes to given scenarios.
- Compare various physical access controls.
- Describe logical access controls.
- Practice the terminology of access controls and review concepts of access controls.

Key topics include:

- Security Control Protocols
- Access Control Strategies
- User Privilege Administration

Additional Resources

- **Click here for Domain 3 Chapter Terms and Definitions**.
- **Click here for Domain 3 Flashcards**.

Domain 4: Network Security

In Domain 4, the principles of network security will be explained. Students will learn how computer networking can be used for good and ill, how cybercriminals exploit network protocols and vulnerabilities, and what can be done to ensure network protection. Essential network components will be reviewed, along with basic network attacks and popular methods of intervention. While network security can be its own specialized field, a working knowledge of the topic is integral for a well-rounded security professional.

After completing this domain, learners will be able to:

- Explain the concepts of network security.
- Recognize common networking terms and models.
- Identify common protocols and ports and their secure counterparts.
- Identify types of network threats and attacks.
- Discuss common tools used to identify and prevent threats.
- Identify common data center terminology.
- Recognize common cloud service terminology.

- Identify secure network design terminology.
- Practice the terminology of and review network security concepts.

Key topics include:

- Secure Infrastructure Strategies
- Cloud Computing Infrastructure
- Network Architecture
- Ports and Services Management

Additional Resources

- **Click here for Domain 4 Chapter Terms and Definitions**.
- **Click here for Domain 4 Flashcards**.

Domain 5: Security Operations

In Domain 5, learners will engage with the fundamentals of security operations. They will investigate the day-to-day use of risk mitigation strategies and security controls in use by organizations and explore strategies for securing data and the systems it is stored on. Finally, students will learn how to promote secure data practices among users.

After completing this domain, learners will be able to:

- Explain concepts of security operations.
- Discuss data handling best practices.
- Identify important concepts of logging and monitoring.
- Summarize the different types of encryption and their common uses.
- Describe the concepts of configuration management.
- Explain the application of common security policies.
- Discuss the importance of security awareness training.
- Practice the terminology of and review the concepts of network operations.

Key topics include:

- Data Governance
- Change Management
- Hashing and Encryption
- Password Security Awareness

Additional Resources

- Click here for Domain 5 Chapter Terms and Definitions.
- **Click here for Domain 5 Flashcards**.

It's understandable to have test-day jitters. What's important is that you also have the tools to put them in their place.

1. **Prepare, prepare, prepare** | The best way to be confident on test day is to know the material. Review your flashcards. Take your practice quizzes until you consistently earn passing scores. Play with the concepts and be able to explain them. The deeper our learning, the less chance we'll forget, even in times of stress.

2. **Eliminate non-test stressors** | Some facets of exam day are simply realities, such as the questions on the exam itself. Others we can move out of the way. Drive the route to your testing center the day before, figure out parking, and give yourself ample time to walk to the testing room. Uncertainty in all those areas could elevate stress hormones and decrease executive reasoning on the day of the exam.

3. **Pace your study leading up to the exam** | When you leave a large chunk of material to the last minute, stress levels rise and your ability to learn decreases. Pace yourself by setting aside a time every week, and don't binge. Study a reasonable amount of time, and give your mind time to retain and dwell on the information between sessions.

4. **Make smart sacrifices** | Sometimes test day is upon us and we have chapters left unread. At this point, you know 99% of what you're going to know, and stuffing in a few more facts won't compare to the boost of showing up mentally present. Skip last-minute review in favor of a good night's rest, time with friends to unwind, and a good meal. Even if your brain performs better under the pressure of cramming, the stress of learning new information will **impair your ability** to access information you already know on test day.

5. **Plan something fun after the exam** | Put yourself in a good mood for game day by planning something fun immediately following the exam. The positive anticipation will boost your dopamine levels (which helps you think) and reduce cortisol (which **impairs your memory**). Immediately taking your mind off the test will also help you avoid overthinking and prevent you from internalizing test-taking as a negative experience. Reducing fear around exams will in turn help you perform better on them in the future.

While the exam may be inevitable, our reaction to it is something you can control. Preparation eliminates fear, and leveraging the resources in this CC Study Pack can help you prepare to the fullest.

There is no replacement for firsthand experience. To help you see the light at the end of the tunnel, here are some insights from current cybersecurity experts who have taken the ISC2 course, received their CC certification, and launched into successful security careers.

*“**Having this knowledge has been absolutely pivotal** in my day-to-day work and has given me such an advantage in understanding client challenges and being able to speak the language of cybersecurity.”*

*“**Obtaining this certification has helped me stand out** from my peers and helped me be seen as a leader on my team. It has also contributed positively to my yearly compensation review, opportunities to network with other professionals, training resources, and discounts on other training programs!”*

*“I have gained a lot of benefits after being certified in the ISC2 CC program. I now have **access to continuous professional education resources**. I also have access to a global community of cybersecurity professionals who I can rely on when it comes to discussions about the industry.”*

- **Janet G.**,
Client Success Manager

*“**The knowledge from ISC2 will propel you** to that level where you can further develop your career in the cybersecurity field. I found the ISC2 CC program to be very relevant. Whether you have industry knowledge or are about to begin your journey, it will help you.”*

*“The CC program gave me a foundational knowledge and it really propelled my confidence to pursue the CISSP credential. When I attained the CC credential, I was given corporate recognition. **My employer sees me as a very valuable resource** in the company.”*

- **Ernest King Arthur**,
CC, CISSP, Solutions Architect

*“**That CC experience was a really good launch point for me**. I made contacts who helped me start my business, and they continue to be helpful contacts, connections, and friends. The CISSP credential opened doors that had been closed before.”*

- **Vickie Gray**,
Owner of GrayMatter Governance Risk and Compliance
Training and Consulting, Ltd.

Here's everything you need to know to get you through. Well, almost everything.

Where do I register?
Get instructions on how to register for your ISC2 exam **here**.

How much does the exam cost?
Exam pricing varies by region. You can participate in the **ISC2 One Million Certified in Cybersecurity** pledge and receive FREE Certified in Cybersecurity (CC) Online Self-Paced Training and an exam.

What languages are offered?
Available languages include Chinese Simplified, English, German, Japanese, and Spanish.

After passing the CC Exam, am I considered certified?
Passing your CC Exam is only one step to becoming ISC2 certified. **Click here** for everything you need to do to complete your certification process.

Should I become a member of ISC2?
While attaining your CC certification is a landmark step, its benefits can be augmented greatly by **becoming a member** of ISC2. All applicants must successfully pass an ISC2 credential exam and complete the **endorsement** to qualify. Here is what some of our experts had to say about becoming ISC2 members:

"***I decided to be a member of ISC2 because it is a reputable organization*** *and I realized that I would get the benefits of continuous professional education. I would also have access to a global community of cybersecurity professionals. Additionally, I would get benefits on resources, such as discounts on books that I need, to stay abreast of developments in the profession."*

- **Ernest King Arthur**,
CC, CISSP, Solutions Architect

"***ISC2 certifications are good to have***. *ISC2 is an important and valuable organization to be part of in the information security world. I really appreciate ISC2 as an organization."*

- **Vickie Gray**,
Owner of GrayMatter Governance Risk and Compliance
Training and Consulting, Ltd.

Good Luck! Bookmark this for reference.

The CC is offered by ISC2 as part of the **One Million Certified in Cybersecurity** pledge. Once obtained, the CC can open doors to your first opportunities in the cybersecurity industry. Bookmark this CC Study Pack and use it as a daily roadmap to plan out your **CC exam** success!

Domain 1: Security Principles

Adequate Security

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information. Source: OMB Circular A-130

Administrative Controls

Controls implemented through policy and procedures. Examples include access control processes and requiring multiple personnel to conduct a specific operation. Administrative controls in modern environments are often enforced in conjunction with physical and/or technical controls, such as an access-granting policy for new users that requires login and approval by the hiring manager.

Artificial Intelligence

The ability of computers and robots to simulate human intelligence and behavior.

Asset

Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property.

Authentication

Access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single-factor or SFA) or more (multi-factor authentication or MFA) factors of identification.

Authorization

The right or a permission that is granted to a system entity to access a system resource. Source: NIST 800-82 Rev. 2

Availability

Ensuring timely and reliable access to and use of information by authorized users.

Baseline

A documented, lowest level of security configuration allowed by a standard or organization.

Biometric

Biological characteristics of an individual, such as a fingerprint, hand geometry, voice, or iris patterns.

Bot

Malicious code that acts like a remotely controlled “robot” for an attacker, with other Trojan and worm capabilities.

Classified or Sensitive Information
Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status and classification level when in documentary form.

Confidentiality
The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes. Source: NIST 800-66

Criticality
A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.
Source: NIST SP 800-60 Vol. 1, Rev. 1

Data Integrity
The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing and while in transit. Source: NIST SP 800-27 Rev. A

Encryption
The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

General Data Protection Regulation (GDPR)
In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.

Governance
The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization, such as policies, roles and procedures the organization uses to make those decisions.

Health Insurance Portability and Accountability Act (HIPAA)
This U.S. federal law is the most important healthcare information regulation in the United States. It directs the adoption of national standards for electronic healthcare transactions while protecting the privacy of individuals' health information. Other provisions address fraud reduction, protections for individuals with health insurance, and a wide range of other healthcare-related activities. Est. 1996.

Impact
The magnitude of harm that could be caused by a threat's exercise of a vulnerability.

Information Security Risk

The potential adverse impacts to an organization's operations (including its mission, functions and image and reputation), assets, individuals, other organizations, and even the nation, which results from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.

Institute of Electrical and Electronics Engineers

IEEE is a professional organization that sets standards for telecommunications, computer engineering and similar disciplines.

Integrity

The property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose.

International Organization of Standards (ISO)

The ISO develops voluntary international standards in collaboration with its partners in international standardization, the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU), particularly in the field of information and communication technologies.

Internet Engineering Task Force (IETF)

The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards (e.g., IP, TCP, DNS) through a process of collaboration and consensus. Source: NIST SP 1800-16B

Likelihood

The probability that a potential vulnerability may be exercised within the construct of the associated threat environment.

Likelihood of Occurrence

A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities.

Multi-Factor Authentication (MFA)

Using two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification.

National Institutes of Standards and Technology (NIST)

The NIST is part of the U.S. Department of Commerce and addresses the measurement infrastructure within science and technology efforts within the U.S. federal government. NIST sets standards in a number of areas, including information security within the Computer Security Resource Center of the Computer Security Divisions.

Non-repudiation
The inability to deny taking an action such as creating information, approving information and sending or receiving a message.

Personally Identifiable Information (PII)
The National Institute of Standards and Technology, known as NIST, in its Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."

Physical Controls
Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

Privacy
The right of an individual to control the distribution of information about themselves.

Probability
The chances, or likelihood, that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Source: NIST SP 800-30 Rev. 1

Protected Health Information (PHI)
Information regarding health status, the provision of healthcare or payment for healthcare as defined in HIPAA (Health Insurance Portability and Accountability Act).

Qualitative Risk Analysis
A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high. Source: NISTIR 8286

Quantitative Risk Analysis
A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss or gain. Source: NISTIR 8286

Risk
A measure of the extent to which an entity is threatened by a potential circumstance or event.

Risk Acceptance
Determining that the potential benefits of a business function outweigh the possible risk impact/likelihood and performing that business function with no other action.

Risk Assessment
The process of identifying and analyzing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals and other organizations.
The analysis performed as part of risk management which incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.

Risk Avoidance
Determining that the impact and/or likelihood of a specific risk is too great to be offset by the potential benefits and not performing a certain business function because of that determination.

Risk Management
The process of identifying, evaluating and controlling threats, including all the phases of risk context (or frame), risk assessment, risk treatment and risk monitoring.

Risk Management Framework
A structured approach used to oversee and manage risk for an enterprise. Source: CNSSI 4009

Risk Mitigation
Putting security controls in place to reduce the possible impact and/or likelihood of a specific risk.

Risk Tolerance
The level of risk an entity is willing to assume in order to achieve a potential desired result. Source: NIST SP 800-32. Risk threshold, risk appetite and acceptable risk are also terms used synonymously with risk tolerance.

Risk Transference
Paying an external party to accept the financial impact of a given risk.

Risk Treatment
The determination of the best way to address an identified risk.

Security Controls
The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. Source: FIPS PUB 199

Sensitivity
A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. Source: NIST SP 800-60 Vol 1, Rev. 1

Single-Factor Authentication
Use of just one of the three available factors (something you know, something you have, something you are) to carry out the authentication process being requested.

State
The condition an entity is in at a point in time.

System Integrity
The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
Source: NIST SP 800-27 Rev. A

Technical Controls
Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service. Source: NIST SP 800-30 Rev. 1

Threat Actor
An individual or a group that attempts to exploit vulnerabilities to cause or force a t hreat to occur.

Threat Vector
The means by which a threat actor carries out their objectives.

Token
A physical object a user possesses and controls that is used to authenticate the user's identity.
Source: NISTIR 7711

Vulnerability
Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source. Source: NIST SP 800-30 Rev. 1

Domain 2: Incident Response, Business Continuity (BC) and Disaster Recovery (DR) Concepts

Adverse Events
Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.

Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose. Source: NIST SP 800-53 Rev. 5

Business Continuity (BC)

Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

Business Continuity Plan (BCP)

The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Business Impact Analysis (BIA)

An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. Source: NIST SP 800-34 Rev. 1

Disaster Recovery (DR)

In information systems terms, the activities necessary to restore IT and communications services to an organization during and after an outage, disruption or disturbance of any kind or scale.

Disaster Recovery Plan (DRP)

The processes, policies and procedures related to preparing for recovery or continuation of an organization's critical business functions, technology infrastructure, systems and applications after the organization experiences a disaster. A disaster is when an organization's critical business function(s) cannot be performed at an acceptable level within a predetermined period following a disruption.

Event

Any observable occurrence in a network or system. Source: NIST SP 800-61 Rev 2

Exploit

A particular attack. It is named this way because these attacks exploit system vulnerabilities.

Incident

An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.

Incident Handling

The mitigation of violations of security policies and recommended practices. Source: NIST SP 800-61 Rev 2

Incident Response (IR)
The mitigation of violations of security policies and recommended practices.
Source: NIST SP 800-61 Rev 2

Incident Response Plan (IRP)
The documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of a malicious cyberattack against an organization's information systems(s). Source: NIST SP 800-34 Rev 1

Intrusion
A security event, or combination of security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization. Source: IETF RFC 4949 Ver 2

Security Operations Center
A centralized organizational function fulfilled by an information security team that monitors, detects and analyzes events on the network or system to prevent and resolve issues before the result in business disruptions.

Vulnerability
Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source. Source: NIST SP 800-128.

Zero Day
A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods.

Domain 3: Access Controls Concepts

Audit
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
Source: NIST SP 1800-15B

Crime Prevention through Environmental Design (CPTED)
An architectural approach to the design of buildings and spaces which emphasizes passive features to reduce the likelihood of criminal activity.

Defense in Depth
Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Source: NIST SP 800-53 Rev 4

Discretionary Access Control (DAC)
A certain amount of access control is left to the discretion of the object's owner, or anyone else who is authorized to control the object's access. The owner can determine who should have access rights to an object and what those rights should be. Source: NIST SP 800-192

Encrypt
To protect private information by putting it into a form that can only be read by people who have permission to do so.

Firewalls
Devices that enforce administrative security policies by filtering incoming traffic based on a set of rules.

Insider Threat
An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. Source: NIST SP 800-32

iOS
An operating system manufactured by Apple Inc. Used for mobile devices.

Layered Defense
The use of multiple controls arranged in series to provide several consecutive controls to protect an asset; also called defense in depth.

Linux
An operating system that is open source, making its source code legally available to end users.

Log Anomaly
A system irregularity that is identified when studying log entries which could represent events of interest for further surveillance.

Logging
Collecting and storing user activities in a log, which is a record of the events occurring within an organization's systems and networks. Source: NIST SP 1800-25B.

Logical Access Control Systems
An automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application or database. A logical access control system requires the validation of an individual's identity through some mechanism, such as a PIN, card, biometric or other token. It has the capability to assign different access privileges to different individuals depending on their roles and responsibilities in an organization.
Source: NIST SP 800-53 Rev.5.

Mandatory Access Control
Access control that requires the system itself to manage access controls in accordance with the organization's security policies.

Mantrap
An entrance to a building or an area that requires people to pass through two doors with only one door opened at a time.

Object
Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See subject. Source: NIST SP 800-53 Rev 4

Physical Access Controls
Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

Principle of Least Privilege
The principle that users and programs should have only the minimum privileges necessary to complete their tasks. Source: NIST SP 800-179

Privileged Account
An information system account with approved authorizations of a privileged user.
Source: NIST SP 800-53 Rev. 4

Ransomware
A type of malicious software that locks the computer screen or files, thus preventing or limiting a user from accessing their system and data until money is paid.

Role-based access control (RBAC)
An access control system that sets up user permissions based on roles.

Rule
An instruction developed to allow or deny access to a system by comparing the validated identity of the subject to an access control list.

Segregation of Duties
The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats. Also commonly known as Separation of Duties.

Subject
Generally an individual, process or device causing information to flow among objects or change to the system state. Source: NIST SP800-53 R4

Technical Controls
The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

Turnstile
A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

Unix
An operating system used in software development.

User Provisioning
The process of creating, maintaining and deactivating user identities on a system.

Domain 4: Network Security

Application programming interface (API)
A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or web tool.

Bit
The most essential representation of data (zero or one) at Layer 1 of the Open Systems Interconnection (OSI) model.

Broadcast
Broadcast transmission is a one-to-many (one-to-everyone) form of sending internet traffic.

Byte
The byte is a unit of digital information that most commonly consists of eight bits.

Cloud computing
A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Source: NIST 800-145

Community cloud

A system in which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. Source: NIST 800-145

De-encapsulation

The opposite process of encapsulation, in which bundles of data are unpacked or revealed.

Denial-of-Service (DoS)

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) Source: NIST SP 800-27 Rev. A

Domain Name Service (DNS)

This acronym can be applied to three interrelated elements: a service, a physical server and a network protocol.

Encapsulation

Enforcement of data hiding and code hiding during all phases of software development and operational use. Bundling together data and methods is the process of encapsulation; its opposite process may be called unpacking, revealing, or using other terms. Also used to refer to taking any set of data and packaging it or hiding it in another data structure, as is common in network protocols and encryption.

Encryption

The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

File Transfer Protocol (FTP)

The internet protocol (and program) used to transfer files between hosts.

Fragment attack

In a fragment attack, an attacker fragments traffic in such a way that a system is unable to put data packets back together.

Hardware

The physical parts of a computer and related devices.

Hybrid Cloud

A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

Infrastructure as a Service (IaaS)

The provider of the core computing, storage and network hardware and software that is the foundation upon which organizations can build and then deploy applications. IaaS is popular in the data center where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resource is used.

Internet Control Message Protocol (ICMP)

An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.

Internet Protocol (IPv4)

Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. Source: CNSSI 4009-2015

Man-in-the-Middle

An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them. Source: NISTIR 7711

Microsegmentation

Part of a zero-trust strategy that breaks LANs into very small, highly localized zones using firewalls or similar technologies. At the limit, this places firewall at every connection point.

Oversized Packet Attack

Purposely sending a network packet that is larger than expected or larger than can be handled by the receiving system, causing the receiving system to fail unexpectedly.

Packet

Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.

Payload

The primary action of a malicious code attack.

Payment Card Industry Data Security Standard (PCI DSS)

Security standards that apply to merchants and service providers who process credit or debit card transactions.

Platform as a Service (PaaS)

The web-authoring or application development middleware environment that allows applications to be built in the cloud before they're deployed as SaaS assets.

Private Cloud
The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of cloud systems, but removes a number of objections to the cloud computing model, including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.

Protocols
A set of rules (formats and procedures) to implement and control some type of association (that is, communication) between systems. Source: NIST SP 800-82 Rev. 2

Public cloud
The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Source: NIST SP 800-145

Simple Mail Transport Protocol (SMTP)
The standard communication protocol for sending and receiving emails between senders and receivers.

Software
Computer programs and associated data that may be dynamically written or modified during execution. Source: NIST SP 80--37 Rev. 2

Software as a Service (SaaS)
The cloud customer uses the cloud provider's applications running within a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Derived from NIST 800-145

Spoofing
Faking the sending address of a transmission to gain illegal entry into a secure system.
CNSSI 4009-201515

Transport Control Protocol/Internet Protocol (TCP/IP) Model
Internetworking protocol model created by the IETF, which specifies four layers of functionality: Link layer (physical communications), Internet Layer (network-to-network communication), Transport Layer (basic channels for connections and connectionless exchange of data between hosts), and Application Layer, where other protocols and user applications programs make use of network services.

VLAN

A virtual local area network (VLAN) is a logical group of workstations, servers, and network device that appear to be on the same LAN despite their geographical distribution.

VPN

A virtual private network (VPN), built on top of existing networks, that can provide a secure communications mechanism for transmission between networks.

WLAN

A wireless area network (WLAN) is a group of computers and devices that are located in the same vicinity, forming a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN.

Zenmap

The graphical user interface (GUI) for the Nmap Security Scanner, an open-source application that scans networks to determine everything that is connected as well as other information.

Zero Trust

Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Microsegmentation of workloads is a tool of the model.

Domain 5: Security Operations

Application Server

A computer responsible for hosting applications to user workstations.
Source: NIST SP 800-82 Rev. 2

Asymmetric Encryption

An algorithm that uses one key to encrypt and a different key to decrypt the input plaintext.

Checksum

A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data.

Ciphertext

The altered form of a plaintext message so it is unreadable for anyone except the intended recipients. In other words, it has been turned into a secret.

Classification

Classification identifies the degree of harm to the organization, its stakeholders or others that might result if an information asset is divulged to an unauthorized person, process or organization. In short, classification is focused first and foremost on maintaining the confidentiality of the data, based on the data sensitivity.

Configuration Management

A process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated

Cryptanalyst

One who performs cryptanalysis which is the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

Cryptography

The study or applications of methods to secure or protect the meaning and content of messages, files, or other information, usually by disguise, obscuration, or other transformations of that content and meaning.

Data Loss Prevention (DLP)

System capabilities designed to detect and prevent the unauthorized use and transmission of information.

Decryption

The reverse process from encryption. It is the process of converting a ciphertext message back into plaintext through the use of the cryptographic algorithm and the appropriate key for decryption (which is the same for symmetric encryption, but different for asymmetric encryption). This term is also used interchangeably with the "deciphering."

Degaussing

A technique of erasing data on disk or tape (including video tapes) that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data.

Digital Signature

The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation. Source: NIST SP 800-12 Rev. 1

Egress Monitoring

Monitoring of outgoing network traffic.

Encryption

The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

Encryption System

The total set of algorithms, processes, hardware, software, and procedures that taken together provide an encryption and decryption capability.

Hardening
A reference to the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems, and software, including operating system, web server, application server, application, etc. Hardening is normally performed based on industry guidelines and benchmarks, such as those provided by the Center for Internet Security (CIS).

Hash Function
An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message. Source: NIST SP 800-15216

Hashing
The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. Source: CNSSI 4009-2015

Ingress Monitoring
Monitoring of incoming network traffic.

Message Digest
A digital signature that uniquely identifies data and has the property such that changing a single bit in the data will cause a completely different message digest to be generated. Source: NISTIR-8011 Vol.3

Operating System
The software “master control application” that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations. Source: NIST SP 800-44 Version 2

Patch
A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component. Source: ISO/IEC 19770-2

Patch Management
The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. Source: CNSSI 4009

Plaintext
A message or data in its natural format and in readable form; extremely vulnerable from a confidentiality perspective.

Records

The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Source: NIST SP 800-53 Rev. 4

Records Retention

A practice based on the records life cycle, according to which records are retained as long as necessary, and then are destroyed after the appropriate time interval has elapsed.

Remanence

Residual information remaining on storage media after clearing. Source: NIST SP 800-88 Rev. 1

Request for Change (RFC)

The first stage of change management, wherein a change in procedure or product is sought by a stakeholder.

Security Governance

The entirety of the policies, roles, and processes the organization uses to make security decisions in an organization.

Social Engineering

Tactics to infiltrate systems via email, phone, text, or social media, often impersonating a person or agency in authority or offering a gift. A low-tech method would be simply following someone into a secure building.

Symmetric Encryption

An algorithm that uses the same key in both the encryption and the decryption processes.

Web Server

A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an “intranet server.”
Source: NIST SP 800-44 Version 2

Whaling Attack

Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities.

Flashcards by Domain

Domain 1: **Security Principles**

- **Domain 1: Flashcards**

Domain 2: **Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts**

- **Domain 2: Flashcards**

Domain 3: **Access Controls Concepts**

- **Domain 3: Flashcards**

Domain 4: **Network Security**

- **Domain 4: Flashcards**

Domain 5: **Security Operations**

- **Domain 5: Flashcards**

About ISC2

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our more than 675,000 members, candidates and associates around the globe are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. ISC2 strengthens the influence, diversity and vitality of the cybersecurity profession through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in an interconnected world. Our charitable foundation, **The Center for Cyber Safety and Education**™, helps create more access to cyber careers and educate those most vulnerable. For more information on ISC2, visit **ISC2.org**, follow us on **X** or connect with us on **Facebook**, **LinkedIn** and **Youtube**.

CC SSCP CISSP CCSP CGRC CSSLP ISSAP ISSEP ISSMP

09/2024