Certified Information
Systems Security Professional

ISC2 Certification

Study Pack

As you prepare to take the next step in your cybersecurity career, let this CISSP Study Pack be your guide to showing up on exam day informed, prepared, and ready to succeed.

The **Certified Information Systems Security Professional (CISSP)** credential is one of the most sought-after certifications in job listings and a great way for experienced practitioners to move up to managing security teams. With increased autonomy, decision-making, and an average **US salary** of $147, 757 per year, it is easy to see why.

Not only is the CISSP ISC2's flagship certification but it is recognized as one of the top, if not the top, vendor independent certification for cybersecurity professionals. Drawing from National Institute of Standards and Technology (NIST) and International Standards Organization (ISO) requirements, the CISSP has become the "de facto standard" for security practitioners looking to expand their careers and take on a more managerial role.

This Study Pack will help you understand what to expect on the big day, the best study resources and strategies, how to avoid pitfalls, and what to do once you pass. With this Guide in hand, you'll be nothing if not prepared.

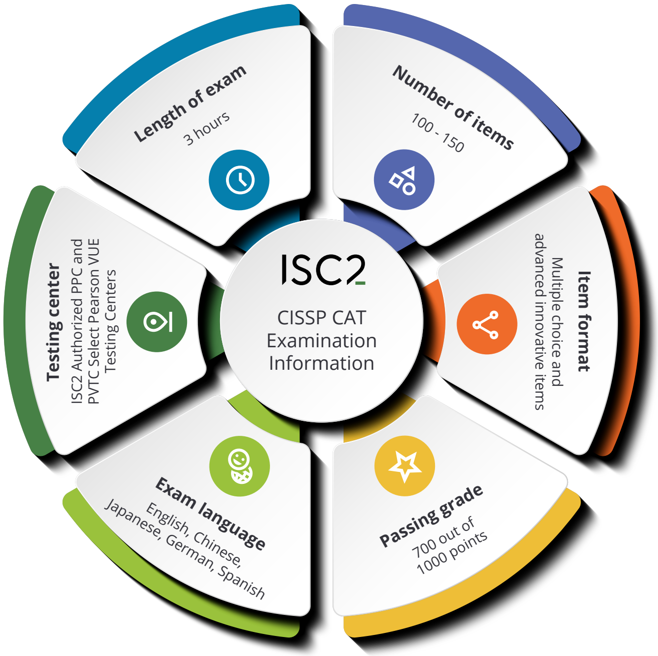
Index

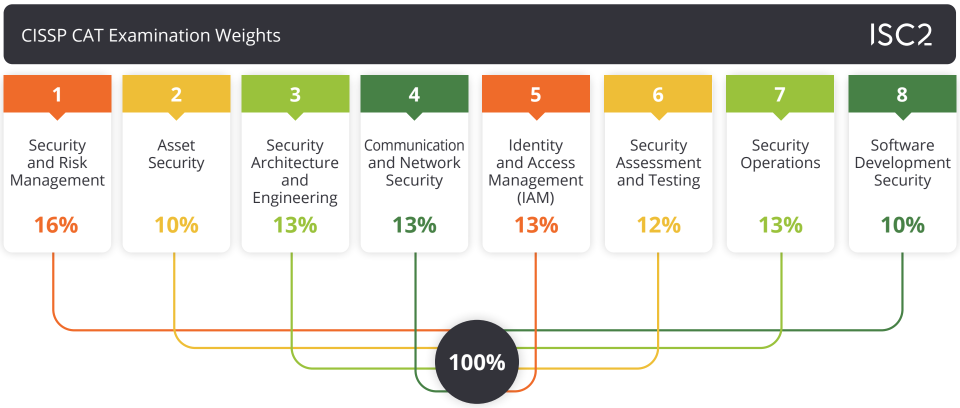
What to Expect

The CISSP Exam contains 100 - 150 multiple-choice and advanced innovative items related to eight different domains:

1. **Domain 1:** Security and Risk Management (16%)
2. **Domain 2:** Asset Security (10%)
3. **Domain 3:** Security Architecture and Engineering (13%)
4. **Domain 4:** Communication and Network Security (13%)
5. **Domain 5:** Identity and Access Management (IAM) (13%)
6. **Domain 6:** Security Assessment and Testing (12%)
7. **Domain 7:** Security Operations (13%)
8. **Domain 8:** Software Development Security (10%)

You will have three hours to complete the exam and will need at least a 70% passing score. 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
CISSP CAT Examination Information
Length of exam
3 hours
Number of items
100 - 150
Item format
Multiple choice and advanced innovative items
Passing grade
700 out of 1000 points
Exam language
English, Chinese, Japanese, German, Spanish
Testing center
ISC2 Authorized PPC and PVTC Select Pearson VUE Testing Centers


CISSP CAT Examination Weights ISC2

1	2	3	4	5	6	7	8
Security and Risk Management	Asset Security	Security Architecture and Engineering	Communication and Network Security	Identity and Access Management (IAM)	Security Assessment and Testing	Security Operations	Software Development Security
16%	10%	13%	13%	13%	12%	13%	10%

ISC2 Dedicated Resources

Know the official material *before* you see it on the CISSP. ISC2 has dedicated resources proven to help you succeed on exam day.

1. **Leverage official eTextbooks** | Take advantage of a range of **Official ISC2 CISSP textbooks** as your go-to resources for study. Get a comprehensive review of the exam topics as you build your confidence in the various domains.

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

3. **Use the ISC2 Community** | If you struggle, don't struggle alone. Never underestimate 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. **Your CISSP Self-Study Tools** | ISC2's Self-Study Tools for the CISSP Exam include:

    - **Official CISSP Online Self-Paced Training**
    - **Official CISSP Flashcards**
    - **Official CISSP Practice Quiz**
    - **Official CISSP Study App**
    - **Official CISSP Online Study Groups (as mentioned above)**
    - **Official ISC2 CISSP Textbooks**

And remember, you can always ask questions on the community board! Additionally, ISC2 Official Training Partners can provide more convenient access to official ISC2 training to fit your individual needs.

Study Tips

While your optimum study methods will be unique, here are some practical solutions that can help boost your curated routine. 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."

- And don't forget to use your fellow learners as resources. Check out the **individual CISSP study plans** other security professionals share on forums like LinkedIn and lean on **community** support! Remember, many cybersecurity experts have passed this milestone for themselves and are more than willing to help.

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.

Domain 1: Security and Risk Management

Overall, security professionals reviewing CISSP Domain 1 must develop a comprehensive understanding of the principles, concepts, and best practices related to information security management. This includes not only technical skills but also an understanding of legal and regulatory requirements, risk management, and security governance.

Essential takeaways include:

- Security governance is the foundation for effective information security management. Security policies, standards, and procedures must be established and maintained to guide the implementation of security controls and ensure resources are allocated appropriately.
- Risk management is critical to the success of any information security program. The process involves identifying, assessing, and mitigating risks, as well as selecting and implementing appropriate security controls to manage those risks.
- Security controls are the technical and administrative measures used to protect information and systems from unauthorized access, disclosure, or destruction. Technology professionals should be familiar with the different types of security controls and know how to select and implement them appropriately.
- Compliance with legal and regulatory requirements is essential for organizations operating in any industry. Technology professionals need to be familiar with the relevant laws and regulations and understand how to comply with them.
- Core security principles, such as confidentiality, integrity, and availability, are the foundation of information security. Technology professionals must understand how these principles apply to different types of information and systems and know how to implement security controls to protect them.

Key topics include:

- Professional Ethics
- Legal, Regulatory, and Compliance Concerns
- Standards, Procedures, and Guidelines
- Risk Management Concepts
- Security Concepts
- Investigation Types
- Business Continuity Requirements
- Threat Modeling Concepts and Methodologies
- Security Awareness, Education, and Training Programs
- Security Governance Principles
- Security Policy
- Personnel Security Policies and Procedures
- Supply Chain Risk Management Concepts

Additional Resources

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

Domain 2: Asset Security

Security professionals reviewing CISSP Domain 2 need to understand the importance of asset security and the measures that can be used to protect assets throughout their life cycle. This includes not only technical controls but also physical security measures, disaster recovery planning, and privacy considerations. Additionally, third-party relationships must be carefully managed to ensure assets are properly protected.

Essential takeaways include:

- Information and assets must be protected throughout their life cycle. This includes the creation, use, storage, and destruction of information.
- Identification and classification of assets is crucial for effective asset security management. This involves understanding the value, sensitivity, and criticality of different types of information and assets.
- Physical security measures are essential to protect assets from theft, destruction, or damage. This includes access controls, locks, and environmental controls.
- Logical security measures are necessary to protect assets from unauthorized access, disclosure, or modification. This includes controls such as authentication, authorization, and encryption.
- Data backups and disaster recovery planning are critical to ensure that assets can be recovered in the event of a disaster or system failure.
- Third-party relationships, such as outsourcing or cloud services, require special attention to ensure assets are properly protected. This includes the use of contracts and agreements to define roles and responsibilities.
- Privacy considerations are important for protecting personal and sensitive information. This includes complying with relevant laws and regulations and implementing appropriate security controls.

Key topics include:

- Identify and classify information and assets
- Establish information and asset handling requirements
- Provision of information and assets securely
- Manage the data life cycle
- Ensure appropriate asset retention
- Determine data security controls and compliance requirements

Additional Resources

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

Domain 3: Security Architecture and Engineering

Security professionals reviewing CISSP Domain 3 must understand the principles of secure system design and the various tools and techniques that can be used to protect information and systems. This includes technical controls, such as cryptography and access controls, security models, and testing methodologies. Additionally, physical security measures are necessary to protect systems and equipment from physical threats.

Essential takeaways include:

- Security architecture and engineering involves designing and implementing security controls to protect information and systems. All major frameworks are risk-based and encourage control design to reflect the outcomes of the risk management process.
- Secure design principles should be integrated into every aspect of system development, from the initial design to the final implementation. Undertaking control design at an early stage is usually more effective, straightforward, and cost-effective.
- Cryptography is an important tool for protecting information from unauthorized access or modification. Technology professionals should be familiar with the advantages and disadvantages of both symmetric and asymmetric encryption, as well as some common encryption algorithms and how to use them effectively.
- Access controls are necessary to prevent unauthorized access to information and systems. This includes controls such as authentication, authorization, and accounting.
- Security models can be used to define and enforce security policies. This includes models such as Bell-LaPadula, Biba, and Clark-Wilson.
- Security testing is essential to ensure security controls are working effectively. This includes testing for vulnerabilities, penetration testing, and security audits.
- Physical security measures, such as access controls and environmental controls, are necessary to protect systems and equipment from theft, damage, or destruction.

Key topics include:

- Secure Design Principles
- Security Models
- Controls & Systems Security Requirements
- Security Capabilities -
- Vulnerabilities of Security Architectures & Designs
- Cryptographic Solutions
- Cryptanalytic Attacks
- Secure Site & Facility Design
- Site & Facility Security Controls
- Information System Life Cycle

Additional Resources

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

Domain 4: Communication and Network Security

Security professionals reviewing CISSP Domain 4 must understand the principles of communication and network security and the tools and techniques used to protect information as it is transmitted over networks. This includes securing network protocols and services, using network security devices, implementing secure transmission protocols, securing wireless networks, and mitigating internet-related security risks. Additionally, special security considerations are required for real-time communication technologies.

Essential takeaways include:

- Communication and network security involves protecting the confidentiality, integrity, and availability of information as it is transmitted over networks.
- Network protocols and services, such as TCP/IP, DNS, and DHCP, are fundamental to network communication and must be secured to prevent attacks.
- Network security devices, such as firewalls and intrusion detection/prevention systems, can be used to protect networks from unauthorized access and attacks.
- Secure transmission protocols, such as SSL/TLS and VPNs, can be used to protect information as it is transmitted over networks.
- Wireless networks present unique security challenges, including the need to secure access points and encrypt data transmissions.
- The internet presents significant security risks, including malware, phishing attacks, and denial-of-service attacks. Network security measures must be implemented to mitigate these risks.
- Voice over IP (VoIP) and other real-time communication technologies require special security considerations, such as ensuring the confidentiality of conversations and protecting against eavesdropping.

Key topics include:

- Secure Design in Network Architectures
- Secure Network Components
- Secure Communication Channels

Additional Resources

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

Domain 5: Identity Access Management

Security professionals reviewing CISSP Domain 5 must understand the principles of identity and access management and the various tools and techniques for managing user accounts and controlling access to information and systems. This includes understanding user authentication and authorization mechanisms, managing privileged accounts, and implementing single sign-on (SSO) and federated identity management (FIM). Additionally, access control monitoring and logging are critical for detecting and preventing unauthorized access and providing an audit trail for forensic analysis.

Essential takeaways include:

- Identity and access management involves managing the life cycle of user accounts from creation to deletion.
- Identification, authentication, and authorization are the three key components of access control.
- User authentication mechanisms include passwords, tokens, biometrics, and multifactor authentication.
- Authorization mechanisms include access control lists, role-based access control, and mandatory access control.
- Identity and access management also involves managing privileged accounts, such as administrator accounts, which require special attention to ensure they are not misused.
- Single sign-on (SSO) and federated identity management (FIM) can be used to simplify access control and reduce the number of accounts and passwords users must manage.
- Access control monitoring and logging are essential to detect and prevent unauthorized access and to provide an audit trail for forensic analysis.

Key topics include:

- Physical and Logical Access Controls
- Identification and Authentication Strategy
- Federated Identities
- Authorization Mechanisms
- IAM Life Cycle
- Authentication Systems

Additional Resources

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

Domain 6: Security Assessment and Testing

Regarding CISSP Domain 6, it is crucial for security professionals to grasp the foundational principles of security assessment and testing, along with the diverse tools and techniques utilized for uncovering vulnerabilities and assessing security controls.

Essential takeaways include:

- Security assessment and testing involves evaluating the effectiveness of security controls and pinpointing vulnerabilities in information systems.
- This process encompasses a variety of techniques, including vulnerability scanning, penetration testing, and social engineering.
- Vulnerability scanning is characterized by the automated use of tools aimed at identifying known vulnerabilities in information systems.
- Penetration testing ventures into exploiting vulnerabilities within a controlled environment to gauge the effectiveness of security controls.
- Social engineering uses psychological tactics to deceive users, prompting them to disclose confidential information or take actions that compromise security.
- Regular security assessment and testing are imperative as they ensure the identification of new vulnerabilities and ongoing effectiveness of security controls.
- Utilize the outcomes of security assessment and testing to strategically prioritize remediation efforts and enhance security controls.

Key topics include:

- Assessment, Test, & Audit Strategies
- Security Controls Testing
- Security Process Data
- Test Output & Reporting
- Security Audits

Additional Resources

- **Click here for Domain 6 Chapter Terms and Definitions.**
- **Click here for Domain 6 Flashcards.**

Domain 7: Security Operations

Security professionals reviewing CISSP Domain 7 must understand the principles of security operations, the different tools and techniques used to manage security controls, and how concepts are applied to produce high-fidelity security data to inform the overall security program. This includes understanding the importance of ongoing monitoring, regular review of security controls, following regularly updated policies and procedures, and continuously refining sources of security data.

Essential takeaways include:

- Security operations involve the day-to-day management and implementation of security controls, including incident management, vulnerability management, logging, disaster recovery, business continuity planning, and ongoing monitoring of security controls and systems.
- Incident management involves responding to security incidents, including identifying and containing the incident, conducting forensic analysis, and restoring normal operations.
- Vulnerability management involves the entire life cycle of a vulnerability, including identification, discovery, evaluation, reporting, remediation, and continuous monitoring.
- Adequate logging is crucial to security operations and has a significant impact on multiple aspects of security operations and the overall security program. Small changes to logging can be used to improve and refine security data in your environment.
- Disaster recovery involves preparing for and responding to natural disasters and other catastrophic events that could disrupt normal operations.
- Business continuity planning involves developing and implementing plans to ensure that critical business functions can continue in the event of a disruption.
- Security operations should be guided by policies and procedures and should be reviewed and updated on a regular basis to ensure that they remain effective.
- Collaboration and communication with other departments, such as legal, human resources, and IT, is essential to ensure effective security operations.

Key topics include:

- Comply with Investigations
- Security Operations Concepts
- Incident management
- Change Management
- Business Continuity Planning and Exercises
- Logging and Monitoring Activities
- Security Operations Concepts
- Detection and Preventative Measures
- Recovery Strategies
- Physical Security
- Configuration Management
- Resource Protection
- Patch and Vulnerability Management
- Implement and Test Disaster Recovery
- Personnel Safety and Security

Additional Resources

- **Click here for Domain 7 Chapter Terms and Definitions.**
- **Click here for Domain 7 Flashcards**.

Domain 8: Software Development Security

Overall, security professionals reviewing CISSP Domain 8 should understand the principles of software development security and the different tools and techniques that can be used to incorporate security into the SDLC. This includes understanding secure coding practices, code reviews and testing, and incorporating security into the design, deployment, and maintenance of software.

Essential takeaways include:

- Software development security involves incorporating security into the software development life cycle (SDLC) to prevent security vulnerabilities and ensure that software is secure by design.
- The SDLC consists of several phases, including planning, design, implementation, testing, and deployment.
- Secure coding practices, such as input validation and error handling, can help prevent common vulnerabilities, such as buffer overflows and SQL injection.
- Code reviews and testing, such as static code analysis and dynamic testing, can help identify security vulnerabilities in software.
- Security should be incorporated into the design and architecture of software, including the use of secure protocols and encryption.
- Security should also be incorporated into the deployment and maintenance of software, including the use of secure configuration management and patch management.
- Security awareness and training for developers and other stakeholders is important to ensure that security is incorporated throughout the SDLC.

Key topics include:

- Security in the SDLC
- Security Controls in Software Development
- Effectiveness of Software Security
- Security Impact of Acquired Software
- Secure Coding Guidelines and Standards

Additional Resources

- **Click here for Domain 8 Chapter Terms and Definitions.**
- **Click here for Domain 8 Flashcards.**

One common roadblock to certification success is the inevitable fatigue, anxiety, and burnout that often results from working single-mindedly towards a goal – especially a large one. While it is nice to pass the CISSP exam on your first try, remember that your CISSP certification journey will wait until you are ready. Maintaining a firm and healthy hold on the rest of your life is a key skill to taking on additional responsibilities now and in your professional career.

That said, here are some proactive tips to pass your CISSP without overextending yourself.

5 Steps to Avoiding Burnout

As we covered in-depth in our blog, **Beat the Burnout: Tips for Staying Motivated on Your CISSP Journey** , having a manageable plan in place is key to going the distance.
That plan includes:

1. **Establish a Schedule and Stick to It** | "Be realistic. You might be tempted to work ridiculous hours and finish your study period as quickly as possible, but this approach rarely works."
2. **Manage a Healthy Work-Life-Study Balance** | "The most important part of maintaining a healthy work-life-study balance is knowing when to switch off."
3. **Use a Variety of Resources** | "Studying can be monotonous, especially if you're relying on a single study method."
4. **Look After Yourself** | "Make sure you hang out with friends, exercise, and keep up with your other activities to feel fresh when you return to your desk. "
5. **Think About What You're Working Towards** | "When you're struggling... check out a cybersecurity job board and look at the listings for CISSP certification holders; this will remind you what you're working towards and keep you motivated."

Advice from Past Test-Takers

As you apply these practices, keep in mind the advice of those who have passed the CISSP before (and lived to tell the tale). Carlos A. Agrelo, CISSP and CCSK certified cybersecurity professional, emphasizes that the following method helped him stay sane during months of preparation.

- **Set a clear goal:** Set a date for your exam and use it as your timeline for preparation.
- **Have a proper study plan:** Set specific goals for your study, alloting time for each CISSP domain. Maintain weekly and daily objectives.
- **Seek emotional support from your inner circle:** Those close to you will be sacrificing time with you to accommodate your study routine, so it is crucial to have their support and understanding upfront.

Regarding staying positive, **Manuel Benet**, ISC2 community member, shares, ***"Don't be discouraged by what you read on the Internet.*** *The CISSP is a passable exam with a reasonable degree of effort, which in general will be inversely proportional to the professional experience you have in the eight domains of the CISSP."* And **CEO Christopher M.** advises, ***"Engaging with a community of others*** *who are also preparing for the CISSP can provide additional insights, clarify doubts, and offer moral support."*

Pro Tips for Anxiety

Need more advice for showing up ready on game day? Try these creative takes on CISSP preparation and how to take your test in the right frame of mind.

Avoid anxiety: Take your test sooner| Though it may seem counterintuitive, scheduling your test sooner , rather than later, can have unseen benefits and lead to less stress overall. You are more likely to retain information when the deadline doesn't loom too far ahead, and a truncated study period (of a few weeks rather than a few months) will mean you are in "stress mode" for a shorter amount of time. Additionally, the urgency of an upcoming exam can heighten brain alertness and enable you to learn better in the time you have. The key is to still avoid long cram sessions and still opt for a consistent study routine with plenty of fun and rest in between.

Intersperse Stress with Fun | It is **proven** that "fun" chemicals in the brain (oxytocin, dopamine, norepinephrine) improve memory and learning, so be just as disciplined about your "study stop times" as your times to buckle down. Remove yourself completely from your study environment, engage in a completely different (and enjoyable) activity, and come back when you feel ready. Again, the point is to completely "reset" between sessions.

Putting Your Test Foot Forward | To be your calmest, **most prepared self** when you show up for your CISSP exam, consider the following:

- Drive the route to your Pearson VUE testing center a few days before your exam to work out the kinks and get familiar with parking. The fewer surprises, the better.
- Lay out your clothes and belongings the night before.
- Stop studying around six and take time to unwind before a natural bedtime.

Grab your favorite power snack or breakfast before arriving at the testing center and drink plenty of water – it **helps you focus**.

Still anxious? As one contributor empathized, "Some people need multiple times to pass." You don't need to get it on your first attempt, or waste money doing it. For the freedom to take the test multiple times without spending additional cash, try ISC2's **Peace of Mind Protection** for two tries at the exam.

5 Testimonials

As you can see, studying for the CISSP is a lot of work. But it's worth it. It proves you have what it takes to effectively design, implement, and manage a best-in-class cybersecurity program, advance your career, and validate your hard-earned knowledge. But don't just take it from us: here's what some of our CISSP graduates had to say.

Parul Khanna is the Director of Information Security at Manulife, an accomplished industry speaker, and a CISSP-certified cybersecurity professional. Earning the CISSP gave her the confidence and broad expertise she needed to take her career to the next level.

"The CISSP credential helped me approach the job with improved confidence and with much more understanding, and better technical expertise. ***It gave me exposure to all the different domains and allowed me to be able to speak up confidently*** *when it comes to either approaching the interviews or approaching the different jobs. The power of this certification is that it opens numerous other options in which you can step into within the realm of cybersecurity, and it equips you with the right mindset as well as knowledge,"* she said.

Kieran Masters, OT Cyber Security Consultant at PWC, has a similar opinion of the CISSP. *"Passing the exam and becoming an ISC2 member has reassured me of my competence in this field. The course offers a comprehensive learning experience across all spectrums of cybersecurity.* ***It allows individuals with a specific specialization to expand their knowledge into other areas of cybersecurity where they may lack experience****,"* he said.

For **Matt Lee**, Senior Director of Security Compliance at Pax8, however, the CISSP is a springboard for continuous learning, arguing that *"the benefits are what you get out of actually learning and continuing your education and building upon that. I would encourage anybody to pursue the CISSP credential. Then, also after you do so, look for more.* ***Don't stop learning. Our field is not static; it is ever-changing.****"*

Sudesh Kannan, PhD, also known as Dr K, is Principal Engineer at Info Security Innovation and an ISC2 instructor. He says that *"****having the CISSP credential is very important. It looks great on your resume. It makes the difference when you're being interviewed and when you get your job****."* But it's not only that: he believes the biggest benefit of the CISSP is that it helps his students understand their roles better and work more effectively with their colleagues.

Want to have your bases covered? Here are a few useful exam tips you *won't* have to memorize.

Where do I register for the CISSP?
For instructions on how to register for your ISC2 exam, visit
Register for Your Certification Exam.

Where can I take the CISSP exam?
All ISC2 exams are offered exclusively at **Pearson VUE testing centers** worldwide. Register for the most convenient location. ISC2 has not adopted an at-home proctoring policy.

How much does the exam cost?
Exam pricing varies by region.

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

What happens after the exam?
After the exam, you are escorted to the front of the testing room where you will receive your final score. When you pass, you are required to have an ISC2 credential holder endorse your experience. If you do not have one, ISC2 can assign one. It takes 4-6 weeks for the application to be processed and your official CISSP certification to arrive.

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

Can I accelerate my learning?
ISC2 offers the Cybersecurity Leadership Skill Builders to build CISO skills for the CISSP exam.

Good Luck! Bookmark this for reference.

You're on your way. Once you pass your CISSP exam, you will be uniquely qualified to enter a managerial role in cybersecurity, and employers in the industry will know it. Bookmark this Study Pack for reference and use it as a roadmap to CISSP success.

We'd wish you best of luck, but with these comprehensive resources in tow, we know you won't need it!

Domain 1: Security and Risk Management

Audit/auditing: The tools, processes, and activities used to perform compliance reviews.

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

Business continuity (BC): Actions, processes, and tools for ensuring an organization can continue critical operations during a contingency.

Business continuity and disaster recovery (BCDR): A term used to jointly describe business continuity and disaster recovery efforts.

Business impact analysis (BIA): A list of the organization's assets, annotated to reflect the criticality of each asset to the organization.

Compliance: Adherence to a mandate; both the actions demonstrating adherence and the tools, processes, and documentation that are used in adherence.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Data custodian: The person/role within the organization who usually manages the data on a day-to-day basis on behalf of the data owner/controller.

Data owner/ controller: An entity that collects or creates PII.

Data subject: The individual human related to a set of personal data.

Disaster recovery (DR): Those tasks and activities required to bring an organization back from contingency operations and reinstate regular operations.

Due care: A legal concept pertaining to the duty owed by a provider to a customer.

Due diligence: Actions taken by a vendor to demonstrate/ provide due care.

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.

Governance committee: A formal body of personnel who determine how decisions will be made within the organization and the entity that can approve changes and exceptions to current relevant governance.

Guidelines: Suggested practices and expectations of activity to best accomplish tasks and attain goals.

Integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Intellectual property: Intangible assets (notably includes software and data).

Maximum allowable downtime (MAD): The measure of how long an organization can survive an interruption of critical functions. [also known as maximum tolerable downtime (MTD)]

Personally identifiable information (PII): Any data about a human being that could be used to identify that person.

Policy: Documents published and promulgated by senior management dictating and describing the organization's strategic goals.

Privacy: The right of a human individual to control the distribution of information about him- or herself.

Procedures: Explicit, repeatable activities to accomplish a specific task. Procedures can address one-time or infrequent actions or common, regular occurrences.

Recovery point objective (RPO): A measure of how much data the organization can lose before the organization is no longer viable.

Recovery time objective (RTO): The target time set for recovering from any interruption.

Residual risk: The risk remaining after security controls have been put in place as a means of risk mitigation.

Risk: The possibility of damage or harm and the likelihood that damage or harm will be realized.

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 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 mitigation: Putting security controls in place to attenuate the possible impact and/or likelihood of a specific risk.

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

Security control framework: A notional construct outlining the organization's approach to security, including a list of specific security processes, procedures, and solutions used by the organization.

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

Standards: Specific mandates explicitly stating expectations of performance or conformance

Domain 2: Asset Security

Accountability: Accountability ensures that account management has assurance that only authorized users are accessing the system and using it properly.

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.

Asset Lifecycle: The phases that an asset goes through from creation (collection) to destruction.

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

Categorization: The process of grouping sets of data, information or knowledge that have comparable sensitivities (impact or loss ratings), and have similar security needs mandated by law, contracts or other compliance regimes.

Classification: The process of recognizing the impacts to the organization if its information suffers any security compromise—to its confidentiality-, integrity-, availability-, non-repudiation-, authenticity-, privacy- or safety-related characteristics. Classifications are derived from the compliance mandates the organization must operate within, whether these be law, regulation, contract-specified standards or other business expectations.

Clearing: The removal of sensitive data from storage devices in such a way that there is assurance the data may not be reconstructed using normal system functions or software recovery utilities.

Data Custodian: The individual who manages permissions and access on a day-to-day basis based on instructions from the data owner. Responsible for protecting an asset that has value, while in the custodian's possession.

Defensible Destruction Inventory: Eliminating data using a controlled, legally defensible and regulatory compliant way.

Inventory: Complete list of items.

Purging: The removal of sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique.

Qualitative: Measuring something without using numbers, using adjectives, scales or grades.

Quantitative: Using numbers to measure something, usually monetary values.

Recovery: The process of jointly addressing business resiliency and restoration of critical infrastructure and functionality after a disruption.

Responsibility: Obligation for doing something. Can be delegated.

Scoping: Limiting the general baseline recommendations by removing those that do not apply.

Tailoring: The process by which a security control baseline is modified based on (i) the application of scoping guidance, (ii) the specification of compensating security controls, if needed and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

Domain 3: Security Architecture and Engineering

Algorithm: A mathematical function that is used in the encryption and decryption processes. It may be quite simple or extremely complex. Also defined as the set of instructions by which encryption and decryption is done.

Asymmetric Encryption: Process that uses different keys for encryption than it does for decryption, and in which the decryption key is computationally infeasible to determine given the encryption key itself, from plaintext and corresponding ciphertext, or from knowledge of the key generation or encryption algorithm.

Block Mode Encryption: Using fixed-length sequences of input plaintext symbols as the unit of encryption.

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

Collision: This occurs when a hash function generates the same output for different inputs. In other words, two different messages produce the same message digest.

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.

Cryptanalysis: The study of techniques for attempting to defeat cryptographic techniques and, more generally, information security services.

Cryptographic Hash, Cryptographic Hash Function: A process or function that transforms an input plaintext into a unique value called a hash (or hash value). These do not use cryptographic algorithms; the term "cryptographic" refers to the assertion that strong hash algorithms are one-way functions, that is, it is computationally infeasible to example of the use of a cryptographic hash. determine the input plaintext from the hash value and knowledge of the algorithm alone. Message digests are an example of the use of a cryptographic hash.

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.

Cryptosystem: The complete set of hardware, software, communications elements and procedures that allows parties to communicate, store information or use information that is protected by cryptographic means. The system includes the algorithm, key and key management functions, together with other services that can be provided through cryptography.

Cryptovariable(s): One or more parameters that are inherent to a particular cryptographic algorithm and its implementation in a cryptosystem. Block size, key length and number of iterations (or rounds) are examples of cryptovariables.

Decoding: The reverse process from encoding, converting the encoded message back into its plaintext format.

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 “deciphering.”

Encoding: The action of changing a message or other set of information into another format through the use of a code. Unlike encryption, which obscures or hides the meaning, encoded information can still be read by anyone with knowledge of the encoding process.

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.

Frequency Analysis: A form of cryptanalysis that uses the frequency of occurrence of letters, words or symbols in the plaintext alphabet as a way of reducing the search space.

Hybrid Encryption System: A system that uses both symmetric and asymmetric encryption processes.

In Band: Refers to transmitting or sharing control information, such as encryption keys and cryptovariables, over the same communications path, channel or system controlled or protected by that information.

Key: The input that controls the operation of the cryptographic algorithm. It determines the behavior of the algorithm and permits the reliable encryption and decryption of the message.

Key Escrow: A process by which keys (asymmetric or symmetric) are placed in a trusted storage agent’s custody, for later retrieval. The trustworthiness of the encryption system(s) being used is thus completely placed in the escrow agent’s control.

Key Generation: The process of creating a new encryption (or decryption) key.

Key Management: All processes used to create, store, distribute and provide expiration and revocation of encryption and decryption keys, for all users of a particular encryption system.

Key Pair (Asymmetric Encryption): A matching set of one public and one private key, generally associated with only one person, organization or identity.

Key Recovery: A process of reconstructing an encryption key from the ciphertext alone, such as when the original key has been corrupted, lost or forgotten. Requires a known way of reverse-engineering the algorithm (i.e., a successful means of conducting a ciphertext-based attack). By definition, a workable key recovery process for an algorithm means that the algorithm is not secure.

Key Space: Represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password.

Message Digest: A small representation of a message, file or other data, usually generated by a cryptographic hash. Message digests are used to ensure the authentication and integrity of information, not the confidentiality.

Modulo, Modular Arithmetic, Modulus: A system of arithmetic in which a number can range from 0 up to a certain value called the modulus; this is done by integer division of the number by the modulus, with the remainder being the result used in subsequent operations. For example, 15 modulo 4 is 3. Programming and logic languages will represent this as an operator (15 modulo 4, for example) or as a function: f(x) = mod(15,4).

Non-repudiation: The inability to deny. In cryptography, it is a security service by which evidence is maintained so that the sender and the recipient of data cannot deny having participated in the communication. There are two kinds of non-repudiation: “non- repudiation of origin” means the sender cannot deny having sent a particular message, and “non-repudiation of delivery” is when the receiver cannot say that they have received a different message than the one that they actually did receive.

One-time Pad: A series of randomly generated symmetric encryption keys, each one to be used only once by sender and recipient.

Out-of-Band: Refers to transmitting or sharing control information, such as encryption keys and crypto variables, by means of a separate and distinct communications path, channel or system from which the control information is used to operate and keep secure.

Plaintext: The message or data in its natural format and in readable form. Plaintext is human readable and is extremely vulnerable from a confidentiality perspective. Plaintext is the message or data that has not been turned into a secret. Plaintext should not be confused with cleartext, which is data or to send the packets to or what to do with them upon receipt. a message in its natural format, but which its originator has no intention or need to protect via encryption. For example, SSH and TLS protect the contents of a packet by replacing their plaintext forms with ciphertext while leaving the packet headers, preambles and postambles in their unencrypted cleartext forms; if these fields were encrypted, the transport and network protocols wouldn’t know where to send the packets to or what to do with them upon receipt.

Private Key: One part of a matching key pair generated via asymmetric encryption processes, which is kept secret by its possessor. Secrecy and integrity of an asymmetric encryption process are entirely dependent upon protecting the value of the private key.

Public Key: One part of a matching key pair generated via asymmetric encryption processes, which can then be shared or published. Secrecy and integrity of a public-key encryption process does not depend upon protecting the value of a public key.

Random and Pseudorandom Number Generators: System elements that are used to provide a value chosen over a key space, such that on successive uses of the function the values returned will have as close to a near-perfect random distribution over that key space as possible. Truly random number generators do not exist in software; they need hardware to observe physical activities such as thermal noise to work properly. Pseudorandom number generators, quite common in software systems, generally demonstrate clumpiness or other exploitable weaknesses in their distribution of returned (generated) values.

Session Key: A symmetric encryption key generated for one-time use, such as during a specific internet connection session. Usually requires a key encapsulation approach to eliminate key management issues.

Stream Mode Encryption System: A system using a process that treats the input plaintext as a continuous flow of symbols and encrypts one symbol at a time. Most stream mode (or streaming) systems also use a streaming key, which uses part of the key as a one-time key for each symbol's encryption.

Substitution Cipher: An encryption or decryption process using substitution.

Symmetric Encryption: A process which uses the same key, or a simple transformation of it, for both encryption and decryption.

Transposition Cipher: An encryption or decryption process using transposition.

Very Early Smoke Detection Apparatus (VESDA): A brand name for an air sampling sensor device that continually breathes in a small amount of the air surrounding it, which can be placed anywhere in a room or its HVAC ducts and plenum spaces

Work Factor: The amount of effort necessary to break a cryptographic system, usually measured in total elapsed time.

Domain 4: Communication and Network Security

Acknowledgment (ACK): An acknowledgment of a signal being received.

Address Resolution Protocol (ARP): Used at the Media Access Control (MAC) layer to provide for direct communication between two devices within the same LAN segment.

Advanced Persistent Threat (APT): An adversary with sophisticated levels of expertise and significant resources who is able to use multiple different attack vectors (e.g., cyber, physical and deception) to achieve its objectives. Its objectives are typically to establish and extend footholds within the IT infrastructure of organizations in order to continually exfiltrate information and/or to undermine or impede critical aspects of a mission, program or organization, or place itself in a position to do so in the future. Moreover, the APT pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.

Application Programming Interface (API): Mobile code mechanisms that provide ways for applications to share data, methods or functions over a network. Usually implemented either in XML or JavaScript Object Notation (JSON). A reference to a software access point or library function with a well- defined syntax and well-defined functionality.

Bandwidth: The amount of information transmitted over a period of time. A process consisting of learning or education could necessitate higher bandwidth than a quick status update, which would require a lower bandwidth.

Bit: Most essential representation of data (zero or one) at layer 1 of the OSI 7-Layer Model.

Bluetooth (Wireless Personal Area Network IEEE 802.15): Bluetooth wireless technology is an open standard for short-range RF communication used primarily to establish wireless personal area networks (WPANs). It has been integrated into many types of business and consumer devices.

Bound Network(s): Network in which devices are connected at layer 1 by means of physical cables, wires or fiber. Often referred to as wired networks, Ethernet networks or by wiring or cable standard used, (e.g., fiber network, Cat 5 or Cat 6 network). See also Unbound (wireless) Network(s).

Boundary Routers: Primarily advertise routes that external hosts can use to reach internal ones.

Bridges: A device that creates a single aggregate network from separate network segments. Using the OSI model, this device aggregates networks at layer 2.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA): A method of flow control in a network. To prevent more than one station from accessing the network simultaneously, the sending station announces its intent to send, and other stations wait until the sending station announces its completion.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD): A method of flow control in a network. If more than one station accesses the network simultaneously, the other stations detect the event and subsequently attempt retransmission.

Cellular Network: A radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station.

Circuit-Switched Network: A network that establishes a dedicated circuit between endpoints.

Code-Division Multiple Access (CDMA): Every call's data is encoded with a unique key, then the calls are all transmitted at once.

Concentrators: Multiplex connected devices into one signal to be transmitted on a network.

Content Distribution Network (CDN): A large, distributed system of servers deployed in multiple data centers, which moves content to achieve QoS and availability requirements.

Control Plane: Control of network functionality and programmability is directly made to devices at this layer. OpenFlow was the original framework/protocol specified to interface with devices through southbound interfaces.

Converged Protocols: A protocol that combines (or converges) standard protocols (such as TCP/IP) with proprietary or other non-standard protocols. These can sometimes provide greatly enhanced functionality and security to meet the needs of specific situations or industries. Adopting them can also complicate enterprise-wide security engineering efforts by requiring additional specialist knowledge and skills to manage and secure.

Domain Name Service (DNS): This acronym can be applied to three interrelated elements: a service, a physical server and a network protocol.

Driver (Device Driver): Software layer that provides an interface for accessing the functions of hardware devices. Typically used by the OS.

Dynamic Host Configuration Protocol (DHCP): An industry standard protocol used to dynamically assign IP addresses to network devices.

Dynamic or Private Ports: Ports 49152–65535. Whenever a service is requested that is associated with well- known or registered ports, those services will respond with a dynamic port.

East-West Data Flow (or Traffic): Network data traffic that flows laterally across a set of internal systems, networks or subnetworks within an IT architecture. These can be flows within a data center or between geographically disperse locations. Contrast with north-south data flows, in which northbound data is leaving the Within SDNs, east-west data flow is within a data plane, control plane or application plane. North-south data flows, in SDN terms, is data flowing up and down the stack of data/ control/application planes. organization and southbound is entering it.

Fiber Distributed Data Interface (FDDI): A LAN standard, defined by ANSI X3T9.5, specifying a 100Mbps token- passing network using fiber-optic cable, with transmission distances of up to two kilometers.

Fibre Channel over Ethernet (FCoE): A lightweight encapsulation protocol that lacks the reliable data transport of the TCP layer.

File Transfer Protocol (FTP): The internet protocol (and program) used to transfer files between hosts.

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

Firmware: Computer programs and data stored in hardware typically in read-only memory (ROM) or programmable read-only memory (PROM)—such that the programs and data cannot be dynamically written or modified during execution of the programs.

Frame: Data represented at layer 2 of the OSI 7-Layer Model.

Gateway Device: A firewall or other device sitting at the edge of a network to regulate traffic and enforce rules.

Hypertext Transfer Protocol (HTTP): A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client browser. The protocol used to transport hypertext files across the internet.

Internet Control Message Protocol (ICMP): An IP network protocol standardized by the IETF through RFC 792 to determine if a particular service or host is available.

Internet Group Management Protocol (IGMP): Used to manage multicasting groups that are a set of hosts anywhere on a network that are listening for a transmission.

Internet of Things (IoT): A virtual network made up of small, dedicated-use devices that are typically designed as small form factor, embedded hardware with a limited functionality OS. They may interface with the physical world and tend to be pervasively deployed where they exist.

Internet Protocol (IPv4): The dominant protocol that operates at layer 3 of the OSI) 7-Layer Model. IP is responsible for addressing packets so that they can be transmitted from the source to the destination hosts.

Internet Protocol (IPv6): A modernization of IPv4 that includes a much larger address field: IPv6 addresses are 128 bits that support 2128 hosts.

Internetworking: Two different sets of servers and communications elements using network protocol stacks to communicate with each other and coordinate their activities with each other.

Intrusion Detection System (IDS): A security service that monitors and analyzes network or system events for the purpose of finding and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Intrusion Prevention Systems (IPS): Uses available information to determine if an attack is underway and sends alerts but also blocks the attack from reaching its intended target.

Kill Chain, Cyber Kill Chain: A generalized attack model consisting of actions on the objective and six broad, overlapping sets of operational activities: reconnaissance, weaponization, delivery, exploitation, installation, command and control. APT actors often combine these operations in complex ways to achieve their goals; such attacks may span over many months. For defenders, the kill chain model highlights the temporary gain in security that can result by improved systems and organizational hardening across any or all of these areas.

Lightweight Directory Access Protocol (LDAP): Authentication is specified as simple (basic), simple using SSL/TLS, or Simple Authentication and Security Layer (SASL).

Logical Link Control (LLC): One of two sublayers that together make up the data link layer in the OSI.

Man-in-the- Middle (MITM): A form of active attack in which the attacker inserts themselves into the physical or logical communications flow between two parties and masquerades to each as the other, falsifying or altering the data exchanged as the attacker chooses to. Also known as MITM. Man (machine)-in-the-browser (MITB) attacks focus on layer 7 vulnerabilities to masquerade as client to the server and as server to the client.

Media Access Control (MAC): The 48-bit hex number assigned to all network cards. The first 24 bits are assigned to the card manufacturer with the send being a unique value (address) for that card.

Microsegmented Networks, 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 a firewall at every connection point.

Modem: Provides modulation and demodulation of binary data into analog signals for transmission through telephone, cable, fiber, or other signaling systems.

Multiprotocol Label Switching (MPLS): A WAN protocol that operates at both layer 2 and layer 3 and does label switching.

Network Function Virtualization (NFV): Alternately referred to as virtual network function. The objective of NFV is to decouple functions, such as firewall management, intrusion detection, NAT and name service resolution, away from specific hardware implementation and move them into software solutions. NFV's focus is to optimize distinct network services.

Network Management: Monitors network performance and identifies attacks and failures. Mechanisms include components that enable network administrators to monitor and restrict resource access.

North-South Network Data Flow (or Traffic): Data flowing either from the organization to external destinations (northbound) or into the organization from external sources (southbound). In SDN terms, data flowing up (northbound) or down (southbound) the stack of data/control/applications planes.

Open Shortest Path First (OSPF): An interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm.

- **OSI Layer 1:** Physical Layer
- **OSI Layer 2:** Data Link Layer
- **OSI Layer 3:** Network Layer
- **OSI Layer 4:** Transport Layer
- **OSI Layer 5:** Session Layer
- **OSI Layer 6:** Presentation Layer
- **OSI Layer 7:** Application Layer

Packet: Representation of data at layer 3 of the OSI 7-Layer Model.

Packet Loss: Degradation of VoIP or other streaming data caused by lost packets. A technique called packet loss concealment (PLC) is used in VoIP communications to mask the effect of dropped packets.

Packet-Switched Networks: Networks that do not use a dedicated connection between endpoints.

Point-to-Point Protocol (PPP): Provides a standard method for transporting multiprotocol datagrams over point-to-point links.

Port Address Translation (PAT): An extension to network address translation (NAT) to translate all addresses to one routable IP address and translate the source port number in the packet to a unique value.

Quality of Service (QoS): Refers to the capability of a network to provide better service to selected network traffic over various technologies, including frame relay, ATM, Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

Registered Ports: Ports 1024–49151. These ports typically accompany non-system applications associated with vendors and developers.

Remote Procedure Call (RPC): A protocol that enables one system to execute instructions on other hosts across a network infrastructure.

Root of Trust (RoT): Hardware-based mechanisms that guarantee the integrity of the hardware prior to loading the OS of a computer.

Segment: Data representation (or datagram name) at Layer 4 of the OSI 7-Layer Model. A portion of a larger network, usually isolated by firewalls or routers at either end from other portions of the network. See also Microsegmented Networks, Microsegmentation.

Simple Network Management Protocol (SNMP): An IP protocol for collecting and organizing information about managed devices on IP networks. It can be used to determine the “health” of networking devices including routers, switches, servers, workstations, printers, and modem racks.

Smurf: ICMP echo request sent to the network broadcast address of a spoofed victim causing all nodes to respond to the victim with an echo reply.

Software-Defined Networking (SDN): Any of a broad range of techniques that enable network management, routing, forwarding and control functions to be directed by software. This is generally done by abstracting the control and management planes from the data plane and its forwarding functions.

Software-Defined Wide Area Network (SD-WAN): An extension of the SDN practices to connect to entities spread across the internet to support WAN architecture especially related to cloud migration.

Teardrop Attack: Exploits the reassembly of fragmented IP packets in the fragment offset field that indicates the starting position, or offset, of the data contained in a fragmented packet relative to the data of the original unfragmented packet.

Terminal Emulation Protocol (Telnet): A command-line protocol designed to give command-line access from one host to another.

Transmission Control Protocol (TCP): The major transport protocol in the internet suite of protocols providing reliable, connection-oriented, full-duplex streams.

Transmission Control Protocol over Internet Protocol (TCP/IP): The name of the IETF's four-layer networking model, and its protocol stack.

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.

Trusted Platform Module (TPM): A tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation) and protect small amounts of sensitive information, such as passwords and cryptographic keys.

Unbound (Wireless) Network(s): Network in which physical layer interconnections are done using radio, light or other means not confined to wires, cables or fibers. Devices on unbound networks may or may not be mobile. See also Bound Network(s).

Virtual Local Area Networks (VLANs): Allow network administrators to use switches to create software-based LAN segments that can be defined based on factors other than physical location.

Voice over Internet Protocol (VoIP): A set of technologies that enables voice to be sent over a packet network.

Web Application Firewall (WAF): A software-based firewall, which monitors and filters exchanges between an applications program and a host. WAFs usually involve inspection and filtering of HTTP and HTTPS conversations.

Wi-Fi (Wireless LAN IEEE 802.11x): Primarily associated with computer networking, Wi-Fi uses the IEEE 802.11x specification to create a wireless LAN either public or private.

WiMAX (Broadband Wireless Access IEEE 802.16): A well-known example of wireless broadband. WiMAX can potentially deliver data rates of more than 30 Mbps.

Zero Trust Model / Architecture: Replaces *trust, but verify* as security design principle by asserting that all activities attempted, by all users or entities, must be subject to control, authentication, authorization, and management at the most granular level possible. NIST and others have proposed zero trust architectures as guidance frameworks for organizations to use as they combine microsegmentation, access control, behavior modeling, and threat intelligence (among other techniques) in moving toward a zero-trust implementation.

Domain 5: Identity and Access Management (IAM)

Access Control System: Means to ensure that access to assets is authorized and restricted based on business and security requirements related to logical and physical systems.

Access Control Tokens: The system decides if access is to be granted or denied based upon the validity of the token for the point where it is read based on time, date, day, holiday or other condition used for controlling validation.

Accounting: Access control process which records information about all attempts by all identities to access any resources of the system. See also authentication, authorization.

Attribute- based Access Control (ABAC): This is an access control paradigm whereby access rights are granted to users with policies that combine attributes together.

Authentication: Access control process that validates the identity being claimed by a user or entity is known to the system, by comparing one or more factors of identification. Factors typically include something the user is, something they have and something they know (such as a fingerprint, a hardware questions). Single-factor (SFA) authenticates with only one of these; multi-factor (MFA) uses two or more. security token and answers to challenge.

Authorization: The process of defining the specific resources a user needs and determining the type of access to those resources the user may have.

Crossover Error Rate (CER): This is the point at which the false acceptance (or Type 2) error rate equals the false rejection (Type 1) error rate, for a given sensor used in a given system and context. This is only the optimal point of operation if the potential impacts of both types of errors are equivalent.

Data Custodian, Custodian: The individual who manages permissions and access on a day-to-day basis based on instructions from the data owner. Responsible for protecting an asset that has value, while in the custodian’s possession.

Data Owner/ Data Controller: The individual or entity who is responsible to classify, categorize and permit access to the data. The data owner is the one who is best familiar with the importance of the data to the business.

Data Processor: Any entity, working on behalf or at the direction of the data controller, that processes personally identifiable information (PII).

Discretionary Access Control (DAC): Access control in which the system owner decides who gets access.

Ethical Wall: The separation of information, assets or job functions to establish and enforce need to know boundaries or prevent conflict of interest situations from arising. The use of administrative, physical and/ or logical controls to establish, maintain and monitor such separations. Also known as a compartment.

False Acceptance Rate (FAR or Type 2): Incorrectly authenticating a claimed identity as legitimate and recognized and granting access on that basis.

False Rejection Rate (FRR or Type 1): Incorrectly denying authentication to a legitimate identity and thus denying it access.

Granularity of Controls: Level of abstraction or detail at which a security function can be configured or tuned for performance and sensitivity purposes.

Identity as-a- Service (IDaaS): Cloud-based services that broker IAM functions to target systems on customers' premises and/or in the cloud.

Identity Proofing: The process of collecting and verifying information about a person for the purpose of proving that a person who has requested an account, a credential or other special privilege is indeed who they claim to be and establishing a reliable relationship that can be trusted electronically between the individual and said credential for purposes of electronic authentication.

Logical Access Control System: Automated systems that authorize or deny access to and use of an information system and its assets to an individual user, based on verification that the identity presented matches that which was previously approved.

Mandatory Access Controls (MAC): Access control that requires the system itself to manage access controls in accordance with the organization's security policies.

Multi-factor Authentication (MFA): Ensures that a user is who they claim to be. The more factors used to determine a person's identity, the greater the trust of authenticity.

Open Authorization (OAuth): The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

Privilege Creep: The unnecessary accumulation of access privileges by a user, typically due to failing to remove privileges when they are no longer needed.

Self-Service Identity Management: Elements of the identity management lifecycle and provisioning process, which the end user (the identity in question) can initiate or perform with little or no interaction or assistance from administrators. Examples include password resets, postal address updates or changes to challenge questions and answers.

Single-Factor Authentication (SFA): Involves the use of simply one of the three available factors solely to carry out the authentication process being requested.

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.

Domain 6: Security Assessment and Testing

Artifact: A piece of evidence, such as text or a reference to a resource, that is submitted to support a response to a question.

Assessment: The testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization.

Audit/Auditing: The process of reviewing a system for compliance against a standard or baseline. Examples include audits of security controls, configuration baselines and financial records. Can be formal and independent, or informal using internal staff.

Chaos Engineering: The discipline of experimenting on a software system in production in order to build confidence in the system's capability to withstand turbulent and unexpected conditions.

Compliance Calendar: A calendar that tracks an organization's audits, assessment, required filings, their due dates and related details.

Compliance Tests: An evaluation that provides assurance an organization's controls are being applied in accordance with management policies and procedures.

Ethical Penetration Testing, Penetration Testing: A security testing and assessment method in which testers actively attempt to circumvent or defeat the security features of a system. Ethical penetration testing is constrained, typically by contracts, to stay within specified rules of engagement (RoE).

Examination: The process of reviewing, inspecting, observing, studying or analyzing one or more assessment objects (i.e., specifications, mechanisms or activities). The purpose of the examine method is to facilitate assessor understanding, achieve clarification or obtain evidence.

Finding(s): Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective.

Interview(s): As a systems assessment technique, the process of holding discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification or obtain evidence.

Judgmental Sampling: Also called purposive sampling or authoritative sampling, it is a non- probability sampling technique in which the sample members are chosen only on the basis of the researcher's knowledge and judgment.

Misuse Case Testing: Testing strategy and technique from the point of view of an actor hostile to the system, using deliberately chosen sets of actions, which could lead to systems integrity failures, malfunctions or other security or safety compromises.

Plan of Action and Milestones (POA&M): A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for meeting the tasks and scheduled milestone completion dates.

Rules of Engagement (RoE): A set of rules, constraints, boundaries or conditions that establish limits on what participants in an activity may or may not do. Ethical penetration testing, for example, uses RoE to define the scope of the testing to be done and to establish liability limitations for both the testers and the sponsoring organization or systems owners.

Statistical Sampling: Statistical sampling is the process of selecting subsets of examples from a population with the objective of estimating properties of the total population.

Substantive Test: The testing technique used by an auditor to obtain the audit evidence in order to support auditor opinion.

Testing: The process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior.

Trust Services Criteria (TSC): The criteria used by an auditor when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the entity.

Domain 7: Security Operations

Allowed Listing (software, identities, addresses): These systems also alert designated IT security personnel if the attempt involves a resource not on a pre-approved list. Standalone security tools and integrated systems which provide these capabilities are now starting to incorporate anti-malware processes as part of their offerings; similarly, In this course, ”blocked list” and ”allowed list” replace ”blacklist” and ”whitelist.” Anti-malware products have begun to incorporate these blocked listing /allowed listing management and use capabilities.

Alternate Site: A general term for a contingency or continuity of operations (COOP) site used to assume system or organizational operations in the event that the primary site is not usable for a period of time.

Backup: A copy of files and programs made to facilitate recovery, if necessary.

Baseline: The total inventory of all of a system’s components, including hardware, software, data, administrative controls, documentation or user instructions. Types of baselines include enumerated baselines, which are inventory lists generated by systems cataloging, discovery and enumeration. Build Security baselines associate the minimum acceptable set of security controls for each CI within a configuration baseline. Modification, update or patch baselines, which are subsets of a total system baseline. These would contain only those CIs which have been modified. or deployment baselines, which are configuration baselines for instances of a system being built for a specific purpose (such as security assessment) or environment (such as production or delivery to end users). tools. Configuration baselines, which have a revision or version identifier associated with each configuration item (CI).

Baselining: Creating a total inventory of a system, component by component, part by part.

Blocked Listing and Allowed Listing (software, identities, addresses): Use of lists of blocked or allowed identities, whether as users, URLs, URIs, web addresses, IP addresses, geographic regions, hardware addresses, files or programs, as a means of controlling (prohibiting or permitting) their access, use or attempt to load and execute.

Change Management: The formal process an organization uses to transition from the current state to a future state. This typically includes mechanisms to request, evaluate, approve, implement, verify and learn from the change.

Configuration Item: An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process. Item or aggregation of hardware, software, or both, which is designated for configuration management and treated as a single entity in the configuration management process.

Configuration Management (CM): A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing and monitoring the configurations of those products and systems throughout the system development lifecycle.

Cyber Forensics: The practice of gathering, retaining and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Disaster Recovery (DR): The ability to provide IT services following an interruption, often at an alternate location.

Disruption: An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network or equipment or facility damage or destruction).

Egress Monitoring: Monitoring the flow of information out of an organization's control boundaries.

Entity: Any form of user, such as a hardware device, software daemon, task, processing thread or human, which is attempting to use or access systems resources. Endpoint devices, for example, are entities that human (or nonhuman) users make use of in accessing a system. Should be subject to access control and accounting. See also User and Entity Behavior Analysis.

Eradication: In incident response, the activities which remove the cause of the incident from the environment. This often requires the use of a formal root cause analysis process.

Event: Any observable occurrence in a network or system.

False Positive: Incorrectly classifying a benign activity, system state or configuration as malicious or vulnerable.

Forensics, Cyber Forensics: The examination of evidence related to suspected criminal activity. Cyber forensics refers to investigations of such activities involving information systems.

Full Backup: Copies the entire system to backup media.

Hackback: Actions taken by a victim of hacking to compromise the systems of the alleged attacker.

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. Hardening is normally performed based on industry guidelines and benchmarks such as those provided by the Center for Internet Security (CIS).

Heuristics: A method of machine learning, which identifies patterns of acceptable activity so that deviations from the patterns will be identified.

Honeypots/ Honeynets: Machines that exist on the network, but do not contain sensitive or valuable data; they are meant to distract and occupy malicious attackers or unauthorized intruders, as a means of delaying their attempts to access production data/assets. A number of machines of this kind, linked together a network or subnet, are referred to as a honeynet.

Hot Site: A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.

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

Incident Response: The mitigation of violations of security policies and recommended practices.

Indicator: A technical artifact or observable occurrence that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred.

Indicators of Compromise (IoC): A signal that an intrusion, malware or other predefined hostile or hazardous set of events is occurring or has occurred.

Information Security Continuous Monitoring (ISCM): Maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions. [Note: The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed and analyzed at a frequency to systems, networks and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance, and within a reporting structure designed to make real-time, data-driven risk management decisions. sufficient to support risk-based security decisions to adequately protect organization information.] Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related.

Information Sharing and Analysis Center (ISAC): Any entity or collaboration created or employed by public- or private-sector organizations, for purposes of gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, to ensure their availability, integrity and reliability.

Intrusion: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Intrusion Detection System (IDS): A security service that monitors and analyzes network or system events for the purpose of finding and providing real time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Prevention Systems (IPS): A security service that uses available information to determine if an attack is underway; it then sends alerts, but also blocks the attack from reaching its intended target.

Log: A record of actions and events that have taken place on a computer system.

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.

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.

Precursor(s): Signals from events that suggest a possible change of conditions (internal or external to the organization) may alter the current threat landscape. An increase in tensions in the local political or social environment, or complaints or grievances by employees or customers going viral in social media, are examples of precursors.

Provisioning: Taking a particular configuration baseline, making additional or modified copies of it, then taking steps as necessary to properly place those copies into the environments they should belong in.

Ransom Attack: Any form of attack, which threatens the destruction, denial or unauthorized public release or remarketing of private information assets. Usually involves encrypting these assets and withholding the decryption key until the ransom is paid by the victim.

Ransomware: Malware used for the purpose of facilitating a ransom attack.

Recovery: The process of jointly addressing business resiliency and restoration of critical infrastructure and functionality after a disruption.

Regression Testing: Testing of a system to ascertain whether recently approved modifications have changed its performance of other approved functions or has introduced other unauthorized behaviors.

Remediation: Changes to a system's configuration to immediately limit or reduce the chance of reoccurrence of an incident. This might include updating the sensitivities, thresholds or alarm settings on any number of security controls, or instituting a rapid reset of access controls information such as passwords and security challenge responses.

Request for Change (RFC): The documentation of a proposed change in support of change management activities.

Root Cause Analysis: A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks or incidents.

Sandbox: A testing environment that is logically, physically or virtually isolated from other environments, and in which applications or systems can be evaluated. Sandboxes can be used as part of development, integration or acceptance testing (so as to not interact with the production environments), as part of malware screening, or as part of a honeynet.

Threat Intelligence: Threat information that has been aggregated, transformed, analyzed, interpreted or enriched to provide the necessary context for decision-making processes.

User and Entity Behavior Analytics (UEBA): Analysis of behaviors and activities of human and nonhuman users, and of the software and hardware entities associated with those users and activities, as a way of detecting inappropriate or unauthorized activity, including fraud detection, malware and insider attacks.

Vulnerability Management: The activities necessary to identify, assess, prioritize and remediate information system weaknesses.

Domain 8: Software Development Security

Acceptance: A formal, structured hand-over of the finished software system to the customer organization; typically involves test, analysis and assessment activities.

Accreditation (also Security Accreditation): Formal declaration by a designated accrediting authority (DAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial and procedural safeguards.

ACID Test: Data integrity provided by means of enforcing atomicity, consistency, isolation and durability policies.

Advanced Persistent Threats (APTs): An agent or organization of agents that plans, organizes and carries out a highly sophisticated attack against a target person, organization or industry over a period of months or possibly even years (thus “persistent”). APTs usually have a strategic goal in mind, which requires many steps in a concerted attack plan to achieve. The term APT may refer to the organization conducting the attack, to specific steps in such an attack as observed by a target or the entire attack sequence. An APT usually involves a phased set of activities, each of which may use dozens of different attack vectors in sequence or in tandem.

Aggregation: The ability to combine non-sensitive data from separate sources to create sensitive information.

Agile Development: Agile development focuses on small team environments and focuses on collaborative, iterative learning, building, testing and deployment of capabilities to operational use. Agile is used to address the need for rapid software development and deployment cycles, perhaps many cycles per day. Agile development follows patterns of activities such as “scrum,” “sprint” or “safe” to manage change and develop and deploy working, reliable and verifiable function.

Application Programming Interfaces (APIs): Mobile code mechanisms that provide ways for applications to share data, methods or functions over a network. Usually implemented either in XML or JavaScript Object Notation (JSON). A reference to a software access point or library function with a well-defined syntax and well-defined functionality.

Arbitrary Code: Alternate sets of instructions and data that an attacker attempts to trick a processor into executing.

Blocked and Allowed Lists (software, identities, addresses): Use of lists of blocked or allowed identities—whether as users, URLs, URIs, web addresses, IP addresses, geographic regions, hardware addresses, files or programs—as a means of controlling (prohibiting or permitting) personnel if the attempt involves a resource not on a pre-approved list. Stand-alone security tools and integrated systems that provide these capabilities are now starting to incorporate anti-malware processes as part of their offerings; similarly, anti- malware products have begun to incorporate these blocked/allowed list management and use capabilities. their access, use or attempt to load and execute. These systems also alert designated IT security. In this course, the term “blocked list” replaces “blacklist” and the term “allowed list” replaces “whitelist.”

Botnets: A network of automated systems or processes (robots, or for short, bots) performing a specific function together, usually malicious. Botnets have greatly magnified the power and speed of malicious operations because they all work together toward achieving a malicious goal, and they have allowed for tuning and directing of operations in a way that was not possible with malicious programs in the past.

Bots: An emerging and special class of mobile code. These employ limited machine- learning capabilities to assist with user requests for help or assistance, automation of or assistance with workflows, data input quality validation and other similar tasks.

Buffer Overflow: A source code vulnerability, which allows attempts to access data locations outside of the storage space to be allocated to the buffer. It can be triggered by attempting to input data that is larger than the input buffer being used.

Bypass Attack: Users may attempt to bypass controls at the front end of the database application to access information.

Certification: The comprehensive technical security analysis of the system to ensure that it meets all applicable security requirements.

Citizen Programmers: Members of the organization who codify work-related knowledge, insights and ideas into varying degrees of reusable software- like forms, often using extensibility features found in most commercial software apps. The very ad hoc nature of these pieces of functionality is extremely difficult to manage, control, verify or assess. In almost all cases, these are beyond the reach and visibility of the organization’s software quality, configuration management or security assessment processes. Such “citizen programming” is often done with little regard to security requirements and can pose a significant risk to some organizations.

Code Protection or Logic Hiding: Prevents one software unit from reading or altering the source, intermediate or executable code of another software unit.

Code Reuse: When programmers reuse, rather than reinvent, units of software (procedures or objects) that have already been demonstrated to be correct, complete, safe and secure.

Commercial Off- the-Shelf (COTS): Software elements, usually applications, that are provided as finished products not intended for alteration by the end user. Most COTS applications are available as host-based, endpoint-based or platform- based services, and support user extensibility by means of non-programming tools, scripts, macros and configuration parameters. COTS can also include firmware and hardware elements.

Common Object Request Broker Architecture (CORBA): A set of standards that addresses the need for interoperability between hardware and software products residing on different machines across a network. CORBA provides for object location and use across a network.

Configuration Control (CC): Process of controlling modifications to hardware, firmware, software and documentation to protect the information system against improper modifications prior to, during and after system implementation.

Configuration Management (CM): A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing and monitoring the configurations of those products and systems throughout the system development lifecycle.

Continuous Integration and Continuous Delivery (CI/CD): Workflow automation processes and tools that attempt to reduce, if not eliminate, the need for manual communication and coordination between the steps of a software development process.

Covert Channel or Covert Path: A communications pathway between two or more processes that transfers information in ways that violate some security policy or requirement. These can be created deliberately (wittingly) by the process designer(s), or unwittingly by the hostile process exploiting hitherto unrecognized exposures of information, resources or other characteristics by the target system.

Data Contamination: Attackers can attempt to use malformed inputs—at the field, record, transaction or file level—in an attempt to disrupt the proper functioning of the system.

Data Lake: A data warehouse incorporating multiple types or streams of unstructured or semi- structured data.

Data Mining: An analysis and decision-making technique that relies on extracting deeper meanings from many different instances and types of data; often applied to data warehouse content.

Data Modeling: A design process that identifies all data elements that the system will need to input, create, store, modify, output and destroy during its operational use. Arguably, data modeling should be one of the first steps in systems analysis and design, regardless of whether procedural or OOP approaches will be used to implement it.

Data Protection or Data Hiding: Restricts or prevents one software unit from reading or altering the private data of another software unit.

Due diligence: Actions taken by a vendor to demonstrate/ provide due care.

Data Type Enforcement: How well (or how poorly) a language protects the programmer from trying to perform operations on dissimilar types of data, or in ways that would lead to erroneous results.

Data Warehouse: A collection of data sources such as separate internal databases to provide a broader base of information for analysis, trending and reference. May also involve databases from outside of the organization, either by importing a copy or by reference.

Data-centric Threat Modeling: A methodology and framework for focusing on the authorized movement, locations, execution, input and output of data within, from and into a system. These correspond with the security concepts of protecting data in transit, at rest (or in storage) and in use, and it provides a focus for carrying out the security decisions already made as the organization classifies and categorizes its data.

Database Management System (DBMS): A suite of application programs that typically manages databases and their environments. The heart of the DBMS is the database engine, a core application that performs and manages the basic functions of create, read, update and delete (CRUD) of data to and from the database, while also making data available for display or export to users, endpoints and other systems. The DBMS provides the structure for the data and some type of language and architecture for accessing and manipulating the data. The primary objective is to store data and allow users to interact with the data, but of course, in a secure way from a confidentiality, integrity and availability perspective.

Database Model: The underlying software design concepts that a DBMS implements; it identifies the specific organization, structure and architecture that the DBMS can provide to users, as they build specific databases to meet business needs.

Defensive Programming: The style of program design and coding that translates the business logic about acceptable and harmful input into code, which allows processing of acceptable inputs, but safely blocks attempts to input (or inject) harmful inputs. The lack of adequate defensive programming measures can result in an arbitrary code execution, a misdirection of the program to other resources or locations or otherwise reveal more information useful to an attacker.

DevOps: A systems development approach based on lean and agile principles in which business owners and the development, operations and quality assurance departments collaborate and work together to deliver software in a continuous manner that enables the business to more quickly react to market opportunities and reduce the time to include customer feedback into products that need to be developed.

DevSecOps: Provides for a merger of phased review (as in the waterfall SDLC) with the DevOps method, so as to incorporate the needs for security, safety, resilience or other emerging properties in the final system, at each turn of the cycle of development.

Dynamic Application Security Testing (DAST): Tools that execute the software unit, application or system under test, in ways that attempt to drive it to reveal a potentially exploitable vulnerability.

Emerging Properties: An alternate and perhaps more powerful way of looking at systems-level behavior characteristics such as safety and security. This perspective also helps provide a more testable, measurable answer to questions such as "how secure is our system?"

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 or revealing. 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.

Executable Code, Object Code: The binary representation of the machine language instruction set that the CPU and other hardware of the target computer directly execute.

Extensible Markup Language (XML): A set of extensions to HTML that provide for data storage and transport in networked environments. XML is frequently used to interface web pages at the front end of a system (as they are displayed and used on client endpoint devices) with databases on back-end servers. XML is often embedded in the HTML files that make up the elements of web pages.

Functional Requirements: Describes a finite task or process the system must perform. These are often directly traceable to specific elements in the final system's design and construction; formal configuration item audits should, for example, be able to identify a given unit of software with the specific functional requirements that dictated it be written and included into the product build.

Hierarchical Database Model: Database model in which data elements and records are arranged in parent-child structures such as trees.

Independent Verification and Validation (IV&V): A comprehensive review, analysis and test (software and/or hardware) performed by an objective third party to confirm (i.e., verify) that the requirements are correctly defined, and to confirm (i.e., validate) that the system correctly implements the required functionality and security requirements.

Inheritance: Provides mechanisms by which objects that are members of a class (a higher level grouping of like objects) can make use of specific characteristics of the class. Files in a read-only folder, for example, generally will also inherit the folder's read-only attribute.

Integrated Development Environments (IDEs): A set of software applications, their control procedures, supporting databases, libraries and toolsets that provide a programmer or a team of programmers what they need to specify designs; translate designs into source code; and then compile, test and integrate that code into a finished software product. Many IDEs support multiple programming languages and facilitate their use on the same project.

Integrated Product and Process Development (IPPD): A management technique that simultaneously integrates all essential acquisition activities through the use of multidisciplinary teams to optimize the design, manufacturing and supportability processes.

Integrated Product Team (IPT): A team of stakeholders and individuals that possess various different skills and who work together to achieve a defined process or product.

Interactive Application Security Testing (IAST): Testing that combines or integrates SAST and DAST to improve testing and provide behavioral analysis capabilities to pinpoint the source of vulnerabilities.

Intermediate Code: Expressing a program's required function in a form that is somewhere between human- readable source code and binary sets of values that can be loaded into memory and executed by a CPU. The most common use of intermediate code is to provide machine independence or portability for a program, such as Java does.

Knowledge Discovery in Database (KDD): A mathematical, statistical and visualization method of identifying valid and useful patterns in data.

Knowledge Management: The efficient and effective management of information and associated resources in an enterprise to drive business intelligence and decision-making. It may include workflow management, business process modeling, document management, databases and information systems and knowledge-based systems.

Level of Abstraction: How close the description (in source code, design documents or any other form) represents one-to-one the details of the underlying object, system or component. Lower-level abstractions generally have far more fine-grain detail than higher level ones.

"Living-Off- the-Land" Non-malware based Ransom Attack: An attack on a system in which illicit access to a system is then used to misuse systems capabilities in the pursuit of the attacker's agenda. The attacker does not use malware in such attacks, hence anti-malware defenses will not detect and prevent it.

Logic Bombs: Malware inserted into a program which will activate and perform functions that suit an attacker's needs at some later date or when certain conditions are met.

Malformed Input Attack: Many of the common source code errors in software can lead to that software failing to correctly handle input data, singly or in combination, that exceeds logical range checks, is contradictory or inconsistent, or is unauthorized. This can result in an arbitrary code execution, a misdirection of the program to other resources or locations or otherwise reveal additional information useful to an attacker.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system or of otherwise annoying or disrupting the victim.

Markup Languages: Non-programming languages used to express formatting or arrangement of data on a page or screen. Markup languages are extensible, which allows users to define other operations to be performed. These extend the language into a programming language, such as the way that JavaScript extends HTML.

Memory or Object Reuse: All systems must allocate memory or other resources as objects to requesting processes, which involves one process reusing such resources after the first using process has finished with them. Any data remaining in the object when it is reused is a potential security violation (i.e., a data remanence issue).

Metadata: Information that describes the format or meaning of other data, which can be used to provide a systematic method for describing resources and improving the retrieval of information.

Mobile Code (Executable Content): A file or a set of files sent by one system to one or more other target or client systems, which, when opened by software already installed on that client, will either control the execution of systems and applications software on that client or be directly executed by that client's CPU.

Modified Prototype Model: An approach to designing and building a system, which starts by building a simplified version of the entire application; this is released for review, with the feedback from the stakeholders used to improve the design of a second, much better version. This is repeated until the owner and stakeholders are satisfied with the final product.

Network Database Model: Database model in which data elements and records are arranged in arbitrary linked fashion, such as lists, clusters or other network forms.

Nonfunctional Requirements: Identifies broad characteristics of the system as a whole. These usually do not align with a clearly identified subset of systems elements. Typically, many safety, security, privacy and resiliency needs have been deemed nonfunctional by their systems' analysts and engineers, and as such, configuration audits cannot identify whether any given software unit contributes to such nonfunctional requirements, or indeed if any of them do.

Object: An encapsulation of a set of data and the methods that can be used to manipulate that data.

Object-oriented (OO) Database Model: A database model that uses object-oriented programming concepts of classes, instances and objects to organize, structure and store both data and methods. Schemas define the structure of the data (in terms of tables, records and attributes or fields); views establish specific selections of tables, rows and columns to meet user or security needs.

Object-oriented Programming (OOP): Defines an object to be a set of software that offers one or more methods, internal to the object, that software external to that object can request be performed. Each method may require specific inputs and resources and may produce a specified set of outputs.

Object-oriented Security: Systems security designs that make use of object-oriented programming characteristics such as encapsulation, inheritance, polymorphism and polyinstantiation.

Open-Source Software: Software whose source code and other design information is made publicly available for inspection, testing, assessment and use. In many cases, open-source licenses allow modification and refactoring. While many commercial software products protect their source code as proprietary, others include or are licensed, supported reuse of open-source software.

Polyinstantiation: Creates a new instance (or version copy) of a data item, with the same identifier or key, allowing for each using process to have its own version of that data. Useful for enforcing and protecting different security levels for a shared resource.

Polymorphism: Allowing an object to “take many forms” based on how it is used means that changes to an object do not have to ripple out into every application’s program that uses that object.

Procedural Programming: Emphasizes the logical sequence or flow of steps to be performed. A “procedure” is a set of software that performs a particular function, requires specific input data (and possibly other resources) and produces a specific set of outputs. Outputs may include error signals when appropriate. Procedures can invoke (“call”) other procedures.

Query Attack: Use of query tools to access data not normally allowed by the trusted front end, including the views controlled by the query application. Malformed queries using SQL to bypass security controls may be possible as well. There are many other examples of where improper or incomplete checks on queries can be used in a similar way to bypass access controls.

Ransom Attack: Any form of attack that threatens the destruction, denial or unauthorized public release or remarketing of private information assets. Usually involves encrypting these assets and withholding the decryption key until the ransom is paid by the victim.

Ransomware: Malware used for the purpose of facilitating a ransom attack.

Rapid Application Development (RAD): A development methodology that creates an application more quickly by employing techniques such as the use of fewer formal methodologies and reuse of software components.

Refactoring: A partial or complete rewrite of a set of software to perform the same functions, but in a more straightforward, more efficient, or more maintainable form.

Regression Testing: Testing of a system to ascertain whether recently approved modifications have changed its performance of other approved functions or has introduced other unauthorized behaviors.

Relational Database Model: Database model in which data elements and records arranged in tables, and tables, are related (linked) to each other to implement a business logic needed to use data records of different structures or types together in the same activity.

Representational State Transfer (REST): A software architectural style for synchronizing the activities of two (or more) applications running on different systems on a network. REST facilitates these processes exchanging state information, usually via HTTP or HTTPS.

Reputation Monitoring: Defensive tactic that uses the trust reputation of a website or IP address as a means of blocking an organization’s users, processes or systems from connecting to a possible source of malware or exploitations. Possibly one’s only effective defense against zero-day exploits. This involves monitoring URLs, domains, IP addresses or other similar information in an attempt to separate the trustworthy sites from the less-than-trustworthy. Dark web addresses, for example, would almost invariably be non-trustworthy.

Runtime Application Security Protection (RASP): Security agents (small code units) built into an application by the developer, which can detect a given set of security violations; upon such detection, the RASP agents can cause the application to terminate, or take other protective actions.

Sandbox: A testing environment which is logically, physically or virtually isolated from other environments, and in which applications or systems can be evaluated. Sandboxes can be used as part of development, integration or acceptance testing (so as to not interact with the production environments), as part of malware screening or as part of a honeynet.

Scanners (Anti- malware): Software that examines a suspected file or set of files for the presence of malware, by signature analysis, activity monitors, heuristics and machine-learning techniques or change analysis.

Secure Coding Guidelines and Standards: Best practices identified by a variety of software and security professionals, that when used correctly can dramatically reduce the number of exploitable vulnerabilities introduced during development that remain in the operationally deployed system.

Security Assessment: Testing, inspection and analysis to determine the degree to which a system meets or exceeds the required security posture. This may assess whether an as- built system meets the requirements in its specifications, or whether an in-use system meets the current perception of the real-world security threats the system may be facing.

Software (Quality) Assurance: A variety of formal and informal processes that attempt to determine whether a software application or system meets all of its intended functions, does not perform unwanted functions, is free from known security vulnerabilities and is free from insertion of other errors in its design, code, form, function and data.

Software Capability Maturity Modeling (SW-CMM) and Assessment: A management process to foster the ongoing and continuous improvement of an organization's processes and workflows for developing, maintaining and using software.

Software Development Lifecycle (SDLC): A framework and a systematic process with associated tasks that are performed in a series of steps for building, deploying and supporting software applications. The lifecycle begins with planning and requirements gathering and ends with decommissioning and sunsetting the software. There are many different SDLCs— such as agile, DevSecOps, rapid prototyping—offering different approaches to defining and managing the software lifecycle.

Software Libraries: A repository of pre-written code, classes, procedures, scripts and other programming elements. These may be provided by systems or applications vendors, from trustworthy third-party developers, developed in-house by the organization's programmers or available from various open-source sites.

Source Code: Program statements written in human- readable form using a formal programming language's rules for syntax and semantics.

Spiral Method: Improved waterfall development process, which provides for a cycle of Plan, Do, Check and Act (PDCA) sub-stages at each phase of the SDLC.

Spyware and Adware: Software that performs a variety of monitoring and data gathering functions. Also known as potentially unwanted programs or applications (PUPs or PUAs), these may be used in monitoring employee activities or their use of systems resources (spyware); adware facilitates advertising efforts. Both may be legitimate and authorized by systems owners to be in use or may be unwanted intruders in these systems.

Static Application Security Testing (SAST): Also known as static source code analysis, these are tools which examine the source code for a variety of errors such as data type errors, loop and structure bounds violations and unreachable code. Since SAST tools do not attempt to execute or simulate the execution of the code being analyzed, it is a bit of a misnomer to call them "testing" tools.

Strong Data Typing: A feature of a programming language that prevents data type mismatch errors (such as trying to add amounts of money to dates or times). Strongly typed languages will generate errors at compile time, forcing the programmer to correct a type mismatch or include additional code that performs the correct data type conversion at run time.

Threat Surface: The total set of penetrations of a boundary or perimeter that surrounds or contains systems elements.

Time of Check vs. Time of Use (TOCTOU) Attacks: Takes advantage of the time delay between a security check (such as authentication or authorization) being performed and actual use of the asset.

Trapdoor or Backdoor: A hidden mechanism that bypasses access control measures. It is an entry point into an architecture or system that is inserted in software by developers, during the program's development to provide a method of gaining access into the program for modification and support reasons. It can also be inserted by an attacker, bypassing access control measures designed to prevent unauthorized software changes.

Trojans: Malware that inserts backdoors or trapdoors into other programs or systems. The malware may or may not be disguised as some useful or entertaining application.

Trusted Computing Base (TCB): The collection of all the hardware, software and firmware components within an architecture that is specifically responsible for security and the isolation of objects. TCB is a term that is usually associated with security kernels and the reference monitor.

View-Based Access Controls: An access control process that allows the database to be logically divided into pieces (individual records, fields or groups of items) that allow certain sensitive data to be hidden from users that are not authorized to see it or manipulate it. Administrators can set up a view for each type of user and then each user can only access the view assigned to them. Some database views will allow the restrictions to be very granular, for example, of both rows and columns, while others allow for views that can write and update data as well as the capability to only read.

Virus: A software program written with the intent and capability to copy and disperse itself without the knowledge and cooperation of the owner or user of the particular system. Researchers of malicious software disagree on a perfect definition of a virus; however, a common definition may be a program that modifies other programs to contain a possibly altered version of itself.

Waterfall Software Development Lifecycle (SDLC): Traditional or classic software development lifecycle model with clearly defined boundaries between each phase. There are many variations on this model, with phases such as concept or mission; needs identification; requirements definition; systems design; software and data systems coding; unit, subsystem and systems testing; acceptance testing; and deployment to operational use. There are many other SDLCs as models and business processes, all different, which are not "waterfall" in concept or use.

Worm: A software program written with the intent and capability to copy and disperse itself without the knowledge and cooperation of the owner or user of the particular system, but without needing to modify other programs to contain copies of itself.

Zero-day, Zero-hour Exploit: Exploit of a hitherto unreported vulnerability in a system, which can potentially be exploited without risk of detection or prevention until the system's owners or developers first detect such an exploit in action. It gets its name from the "zero time" being the time at which the exploit or the vulnerability is first identified by the systems' owners or builders. Also known as zero-hour exploit, zero-day attacks.

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**

Domain 6: **Security Assessment and Testing**

- **Domain 6: Flashcards**

Domain 7: **Security Operations**

- **Domain 7: Flashcards**

Domain 8: **Software Development Security**

- **Domain 8: 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