* Access Control and Identity Management, 3rd Ed. by Mike Chapple. Publisher: Jones and Bartlett Learning. (Sep, 2020).
* Building an Information Security Awareness Program, 1st Ed. by Bill Gardner and Valerie Thomas. Publisher: Syngress. (Aug, 2014).
* Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syngress. (Sep, 2013).
* Cybersecurity Risk Management by Cynthia Brumfield, Brian Haugli. Publisher: Wiley. (Dec, 2021).
* Digital Forensics and Incident Response, 2nd Ed. by Gerard Johansen. Publisher: Packt Publishing. (Jan, 2020).
* Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference by Jamie Watters, Janet Watters. Publisher: Apress. (Dec, 2013).
* Distributed Denial of Service (DDoS) by Eric Chou, Rich Groves. Publisher: O’Reilly Media, Inc. (Apr, 2018).
* Foundations of Information Security: A Straightforward Introduction by Jason Andress. Publisher: William Pollock. (Oct, 2019).
* Fundamentals of Information Systems Security, 4th Ed. by David Kim, Michael G. Solomon. Publisher: Jones & Bartlett Publishers. (Nov, 2021).
* Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, 1st Ed. by Corey Schou and Steven Hernandez. Publisher: McGraw-Hill Education. (Sep, 2014).
* Information Security Policies, Procedures, and Standards: A Practitioner’s Reference by Dogulas J. Landoll. Publisher: Auerbach Publications. (Mar, 2017).
* [ISC2 Code of Ethics](https://www.isc2.org/ethics) by ISC2. (Dec, 2023).
* Mastering Windows Security and Hardening by Mark Dunkerley, Matt Tumbarello. Publisher: Packt Publishing. (Aug, 2022).
* Modern Cryptography for Security Professionals, 1st Ed. by Lisa Bock. Publisher: Packt Publishing. (Jun, 2021).
* Network Security, Firewalls, and VPNs, 3rd Edition by J. Michael Stewart, Denise Kinsey. Publisher: Jones & Bartlett Learning. (Oct, 2020).
* Networking Fundamentals, 1st Ed. by Gordon Davies. Publisher: Packt Publishing. (Dec, 2019).
* Network Security Strategies by Aditya Mukherjee. Publisher: Packt Publishing. (Nov, 2020).
* NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Force Transformation Initiative. (Sep, 2020).
* NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone. (Aug, 2012).
* Security Policies and Implementation Issues, 3rd Ed. by Robert Johnson and Chuck Easttom. Publisher: Bartlett Learning. (Oct, 2020).
* The Complete Guide to Physical Security by Paul R. Baker and Daniel J. Benny. Publisher: Auerbach Publications. (Apr, 2016).
* A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security by Will Arthur, David Challener. Publisher: Apress. (Jan, 2015).
* Access Control and Identity Management, 3rd Ed. by Mike Chapple. Publisher: Jones and Bartlett Learning. (Sep, 2020).
* A Technical Guide to IPSec Virtual Private Networks by James S. Tiller. Publisher: Auerbach Publications. (Jul, 2017).
* Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Ed. by Bruce Schneier. Publisher: Wiley. (Mar, 2015).
* Building an Information Security Awareness Program, 1st Ed. by Bill Gardner and Valerie Thomas. Publisher: Syngress. (Aug, 2014).
* Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syngress. (Sep, 2013).
* Cryptography and Network Security Principles and Practice, 6th Ed. by William Stallings. Publisher: Pearson. (Mar, 2013).
* Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents by Eric C. Thompson. Publisher: Apress. (Sep, 2018).
* Digital Forensics and Incident Response, 2nd Ed. by Gerard Johansen. Publisher: Packt Publishing. (Jan, 2020).
* Foundations of Information Security: A Straightforward Introduction by Jason Andress. Publisher: William Pollock. (Oct, 2019).
* Fundamentals of Information Systems Security, 4th Ed. by David Kim, Michael G. Solomon. Publisher: Jones & Bartlett Publishers. (Nov, 2021).
* Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution by Darran Rolls, Morey J. Haber. Publisher: Apress. (Dec, 2019).
* Identity and Access Management: Business Performance Through Connected Intelligence, 1st Ed. by Ertem Osmanoglu. Publisher: Syngress. (Nov, 2013).
* Information Risk Management: A Practitioner's Guide by David Sutton. Publisher: BCS, The Chartered Institute for IT. (Nov, 2014).
* Introduction to Computer Networks and Cybersecurity, 1st Ed. by J. Chwan-Hwa Wu, David Irwin. Publisher: CRC Press. (Apr, 2016).
* [ISC2 Code of Ethics](https://www.isc2.org/ethics) by ISC2. (Dec, 2023).
* Logging and Log Management by A. Chuvakin, K. Schmidt. Publisher: Syngress. (Dec, 2012).
* Network Security, Firewalls, and VPNs, 3rd Edition by J. Michael Stewart, Denise Kinsey. Publisher: Jones & Bartlett Learning. (Oct, 2020).
* Networking Fundamentals, 1st Ed. by Gordon Davies. Publisher: Packt Publishing. (Dec, 2019).
* NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone. (Aug, 2012).
* Official (ISC)² SSCP CBK Reference, 5th Ed. by Mike Wills. Publisher: Sybex. (Dec, 2019).
* Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Dotson. Publisher: O'Reilly Media. (Mar, 2019).
* A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security by Will Arthur, David Challener. Publisher: Apress. (Jan, 2015).
* Access Control, Authentication, and Public Key Infrastructure (Information Systems Security & Assurance), 1st Ed. by Bill Ballad, Tricia Ballad, Erin Banks. Publisher: Jones & Bartlett Learning. (Oct, 2010).
* Agile Application Security by Laura Bell, Rich Smith, Michael Brunton-Spall, Jim Bird. Publisher: O’Reilly Media, Inc. (Jun, 2017).
* Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS) by Michael Kavis. Publisher: Wiley. (Jan, 2014).
* Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations by Morey J. Haber, Brad Hibbert. Publisher: Apress. (Jun, 2018).
* Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syngress. (Sep, 2013).
* Computer and Information Security Handbook, 3rd Ed. by John Vacca. Publisher: Morgan Kaufmann. (May, 2017).
* Computer Security: Art and Science, 2nd Ed. by Matt Bishop. Publisher: Addison-Wesley Professional. (Nov, 2018).
* Core Software Security: Security at the Source by Anmol Misra, James F. Ransome. Publisher: Auerbach Publications. (Oct, 2018).
* Data Center Handbook, 2nd Ed. by Hwaiyu Geng. Publisher: Wiley. (May, 2021).
* Developing Cybersecurity Programs and Policies, 3rd Ed. by Omar Santos, Sari Greene. Publisher: Pearson IT Certification. (Aug, 2018).
* Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference by Jamie Watters, Janet Watters. Publisher: Apress. (Dec, 2013).
* Distributed Denial of Service (DDoS) by Eric Chou, Rich Groves. Publisher: O’Reilly Media, Inc. (Apr, 2018).
* DomainKeys Identified Mail (DKIM) Signature by Murray Kucherawy, Dave Crocker, Tony Hansen. Publisher: IETF. (Sep, 2011).
* Ethical Hacking and Penetration Testing Guide by Rafay Baloch. Publisher: Auerbach Publications. (Sep, 2017).
* Federated Identity Primer, 1st Ed. by Derrick Rountree. Publisher: Syngress. (Dec, 2012).
* Foundations of Information Security: A Straightforward Introduction by Jason Andress. Publisher: William Pollock. (Oct, 2019).
* Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle Program, 3rd Ed. by Toni Rice. Publisher: SAFECode. (Mar, 2018).
* Fundamentals of Information Systems Security, 4th Ed. by David Kim, Michael G. Solomon. Publisher: Jones & Bartlett Publishers. (Nov, 2021).
* EU General Data Protection Regulation (GDPR) by European Parliament. Publisher: European Parliament and Council of the European Union. (May, 2016).
* Identity and Access Management: Business Performance Through Connected Intelligence, 1st Ed. by Ertem Osmanoglu. Publisher: Syngress. (Nov, 2013).
* Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution by Darran Rolls, Morey J. Haber. Publisher: Apress. (Dec, 2019).
* Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, 1st Ed. by Corey Schou and Steven Hernandez. Publisher: McGraw-Hill Education. (Sep, 2014).
* Information Security Handbook by Darren Death. Publisher: Packt Publishing. (Dec, 2017).
* Information Security Policies, Procedures, and Standards: A Practitioner’s Reference by Dogulas J. Landoll. Publisher: Auerbach Publications. (Mar, 2017).
* Introduction to Computer Networks and Cybersecurity, 1st Ed. by J. Chwan-Hwa Wu, David Irwin. Publisher: CRC Press. (Apr, 2016).
* [ISC2 Code of Ethics](https://www.isc2.org/ethics) by ISC2. (Dec, 2023).
* IT Auditing Using Controls to Protect Information Assets, 3rd Edition by Mike Kegerreis, Mike Schiller, Chris Davis. Publisher: McGraw-Hill Education. (Oct, 2019).
* Network Security, Firewalls, and VPNs, 3rd Edition by J. Michael Stewart, Denise Kinsey. Publisher: Jones & Bartlett Learning. (Oct, 2020).
* Network Vulnerability Assessment: Identify Security Loopholes in Your Network's Infrastructure by Sagar Rahalkar. Publisher: Packt Publishing. (Aug, 2018).
* Networking Fundamentals, 3rd Ed. by Chuck Easttom, Richard M. Roberts. Publisher: Goodheart-Willcox. (Sep, 2018).
* NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments by Joint Task Force Transformation Initiative. (Sep, 2012).
* NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems by Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes. (May, 2010).
* NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy by Karen Scarfone, Paul Hoffman. (Sep, 2009).
* NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Force Transformation Initiative. (Sep, 2020).
* NIST SP 800-63-3, Digital Identity Guidelines: Enrollment and Identity Proofing by Paul A. Grassi, James L. Fenton, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, Mary F. Theofanos. (Jun, 2017).
* NIST SP 800-77, Revision 1, Guide to IPsec VPNs by Elaine Barker, Quynh Dang, Sheila Frankel, Karen Scarfone, Paul Wouters. Publisher: NIST. (Jun, 2020).
* NIST SP 800-88, Guidelines for Media Sanitization by Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine. (Dec, 2014).
* NIST SP 800-95, Guide to Secure Web Services by Anoop Singhal, Theodore Winograd, Karen Scarfone. (Aug, 2007).
* NIST SP 800-115, Technical Guide to Information Security Testing and Assessment by Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. (Sep, 2008).
* NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) by Erika McCallister, Tim Grance, Karen Scarfone. (Apr, 2010).
* NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems by Arnold Johnson, Kelley Dempsey, Ron Ross, Sarbari Gupta, Dennis Bailey. (Aug, 2011).
* NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations by Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, Kevin Stine. (Sep, 2011).
* NIST SP 800-160, Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems by Ron Ross, Michael McEvilley, Janet Carrier Oren. (Mar, 2018).
* Official (ISC)² Guide to the CISSP CBK, 5th Ed. by John Warsinske, Mark Graff, Kevin Henry, Christopher Hoover, Ben Malisow, Sean Murphy, C. Paul Oakes, George Pajari, Jeff T. Parker, David Seidl and Mike Vasquez. Publisher: Wiley. (May, 2019).
* OWASP Testing Guide, Release 4.0 by Matteo Meucci, Andrew Muller. Publisher: OWASP. (Dec, 2014).
* Physical Security and Safety by Jeffrey Dingle, Bobby E. Ricks, Truett A, Ricks. Publisher: CRC Press. (Oct, 2014).
* Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Dotson. Publisher: O'Reilly Media. (Mar, 2019).
* Practical Internet of Things Security, 2nd Ed. by Brian Russel, Drew Van Duren. Publisher: Packt Publisher. (Nov, 2018).
* Securing Open Source Libraries by Guy Podjarny. Publisher: O’Reilly Media, Inc. (Nov, 2017).
* Securing VoIP, 1st Ed. by Regis Bates. Publisher: Syngress. (Nov, 2014).
* Security Policies and Implementation Issues, 3rd Ed. by Robert Johnson and Chuck Easttom. Publisher: Bartlett Learning. (Oct, 2020).
* Security Risk Assessment: Managing Physical and Operational Security by John M. White. Publisher: Butterworth-Heinemann. (Jul, 2014).
* Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0 by Abhishek Hingnikar, Yvonne Wilson. Publisher: Apress. (Nov, 2022).
* The Complete Guide to Physical Security by Paul R. Baker and Daniel J. Benny. Publisher: Auerbach Publications. (Apr, 2016).
* The Disaster Recovery Handbook, 3rd Ed. by Michael Wallace, Lawrence Webber. Publisher: AMACOM. (Dec, 2017).
* Threat Modeling: Designing for Security, 1st Ed. by Adam Shostack. Publisher: Wiley. (Feb, 2014).
* Web Application Security: Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman. Publisher: O’Reilly Media, Inc. (Mar, 2020).
* Zero Trust Networks: Building Secure Systems in Untrusted Networks by Evan Gilman, Doug Barth. Publisher: O'Reilly. (Jul, 2017).
* Architecting Cloud Computing Solutions by Kevin L. Jackson and Scott Goessling. Publisher: Packt Publishing. (May, 2018).
* Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS) by Michael Kavis. Publisher: Wiley. (Jan, 2014).
* Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syngress. (Sep, 2013).
* Cloud Computing Design Patterns by Thomas Erl, Robert Cope, Amin Naserpour. Publisher: Prentice Hall. (Mar, 2017).
* Cloud Security Handbook by Eyal Estrin. Publisher: Packt Publishing. (Apr, 2022).
* Data Governance: The Definitive Guide by Evren Eryurek, Uri Gilad, Valliappa Lakshmanan, Anita Kibunguchy-Grant, Jessi Ashdown. Publisher: O'Reilly Media, Inc. (Mar, 2021).
* EU General Data Protection Regulation (GDPR) by European Parliament. Publisher: European Parliament and Council of the European Union. (May, 2016).
* Fundamental Practices for Secure Software Development. Publisher: SAFECode. (Mar, 2018).
* Guide to Privacy and Security of Electronic Health Information. Publisher: HealthIT.gov. (Apr, 2015).
* Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents by Erdal Ozkaya. Publisher: Packt Publishing. (Feb, 2021).
* Information Security Handbook by Darren Death. Publisher: Packt Publishing. (Dec, 2017).
* NIST SP 800-125, Guide to Security for Full Virtualization Technologies by Karen Scarfone, Murugiah Souppaya, Paul Hoffman. (Jan, 2011).
* Official (ISC)² Guide to the CCSP CBK, 3rd Ed. by Leslie Fife, Aaron Kraus, Bryan Lewis. Publisher: Sybex. (July, 2021).
* Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Dotson. Publisher: O'Reilly Media. (Mar, 2019).
* Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 by Rich Mogull, James Arlen, Adrian Lane, Gunnar Peterson, Mike Rothman, David Mortman. Publisher: Cloud Security Alliance. (Jul, 2017).
* Security, Privacy, and Digital Forensics in the Cloud by Lei Chen, Hassan Takabi, Nhien-An Le-Khac. Publisher: Wiley. (Apr, 2019).
* Information Security Risk Management for ISO 27001/ISO 27002, 3rd Ed. by Alan Calder, Steve Watkins. Publisher: IT Governance Publishing. (Aug, 2019).
* ISO 27001/ISO 27002, A Pocket Guide, 2nd Ed. By Alan Calder. Publisher: IT Governance Publishing. (Oct, 2013).
* NIST FIPS-199, Standards for Security Categorization of Federal Information and Information Systems by U.S. Dept. of Commerce. (Feb, 2004).
* NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems by Marianne Swanson, Joan Hash, Pauline Bowen. (Feb, 2006).
* NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments by Joint Task Force Transformation Initiative. (Sep, 2012).
* NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy by Joint Task Force Transformation Initiative. (Dec, 2018).
* NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View by Joint Task Force Transformation Initiative. (Mar, 2011).
* NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Force Transformation Initiative. (Sep, 2020).
* NIST SP 800-53A, Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations by Joint Task Force Transformation Initiative. (Jan, 2022).
* NIST SP 800-53B, Control Baselines for Information Systems and Organizations by Joint Task Force Transformation Initiative. (Sep, 2020).
* NIST SP 800-60, Vol. 1, Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories by Kevin Stine, Rich Kissel, William C. Barker, Jim Fahlsing, Jessica Gulick. (Aug, 2008).
* NIST SP 800-70, Rev. 4, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers by Stephen D. Quinn, Murugiah Souppaya, Melanie Cook, Karen Scarfone. (Feb, 2018).
* NIST SP 800-88, Guidelines for Media Sanitization by Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine. (Dec, 2014).
* NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations by Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, Kevin Stine. (Sep, 2011).
* A Guide to Building Secure Web Applications and Web Services 2.0 Black Hat Ed. by Abraham Kang, Adrian Wiesmann, et al. Publisher: OWASP. (Jul, 2005).
* A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security by Will Arthur, David Challener. Publisher: Apress. (Jan, 2015).
* Access Control, Authentication, and Public Key Infrastructure, 2nd Ed. by Mike Chapple, Bill Ballad, Tricia Ballad, Erin Banks. Publisher: Jones & Bartlett Learning. (Jul, 2013).
* Agile Application Security by Laura Bell, Rich Smith, Michael Brunton-Spall, Jim Bird. Publisher: O’Reilly Media, Inc. (Jun, 2017).
* Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Ed. by Bruce Schneier. Publisher: Wiley. (Mar, 2015).
* CMMI for Development: Implementation Guide by Mukund Chaudhary, Abhishek Chopra. Publisher: Apress. (Dec, 2016).
* Computer Security: Art and Science, 2nd Ed. by Matt Bishop. Publisher: Addison-Wesley Professional. (Nov, 2018).
* Core Software Security: Security at the Source by Anmol Misra, James F. Ransome. Publisher: Auerbach Publications. (Oct, 2018).
* Cybersecurity - Attack and Defense Strategies, 2nd Ed. by Erdal Ozkaya and Yuri Diogenes. Publisher: Packt Publishing. (Dec, 2019).
* Enterprise Software Security: A Confluence of Disciplines by Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley. Publisher: Addison-Wesley Professional. (Dec, 2014).
* Hacker Techniques, Tools, and Incident Handling, 2nd Ed. by Sean-Philip Oriyano. Publisher: Jones & Bartlett Learning. (Aug, 2013).
* Hands-On Security in DevOps by Tony Hsu. Publisher: Packt Publishing. (Jul, 2018).
* Improper Error Handling by Jeremy Ferragamo, Wichers, Jim Bird. Publisher: OWASP. (Dec, 2021).
* Information Security: Principles and Practices, 2nd Ed. by Mark S. Merkow, Jim Breithaupt. Publisher: Pearson IT Certification. (Jun, 2014).
* IT Release Management: A Hands-on Guide by Dave Howard. Publisher: CRC Press. (Apr, 2016).
* IT Security Risk Control Management: An Audit Preparation Plan by Raymond Pompon. Publisher: Apress. (Sep, 2016).
* Lessons Learned in Software Testing: A Context-Driven Approach by Bret Pettichord, Cem Kaner, James Marcus Bach. Publisher: Wiley. (Dec, 2001).
* Logging and Log Management by A. Chuvakin, K. Schmidt. Publisher: Syngress. (Dec, 2012).
* Mastering the Requirements Process: Getting Requirements Right v3.0 by S. Robertson, J. Robertson. Publisher: Addison-Wesley Professional. (Aug, 2012).
* NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy by Joint Task Force Transformation Initiative. (Dec, 2018).
* NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Force Transformation Initiative. (Sep, 2020).
* NIST SP 800-60, Vol. 1, Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories by Kevin Stine, Rich Kissel, William C. Barker, Jim Fahlsing, Jessica Gulick. (Aug, 2008).
* NIST SP 800-88, Guidelines for Media Sanitization by Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine. (Dec, 2014).
* NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems by Jon Boyens, Celia Paulsen, Nadya Bartol, Stephany A. Shankles, Rama Moorthy. (Oct, 2012).
* Official (ISC)² Guide to the CSSLP, 2nd Ed. by Mano Paul. Publisher: Auerbach Publications. (Aug, 2013).
* OWASP Testing Guide, Release 4.0 by Matteo Meucci, Andrew Muller. Publisher: OWASP. (Dec, 2014).
* Penetration Testing: A Survival Guide by W. Halton, B. Weaver, J. Ansari, S. Kotipalli, M. Imran. Publisher: Packt Publishing. (Jan, 2017).
* Security Risk Management by Evan Wheeler. Publisher: Syngress. (Apr, 2011).
* Software Testing Foundations: A Study Guide for the Certified Tester Exam, 4th Ed. by Andreas Spillner. Publisher: Rocky Nook. (Feb, 2014).
* Web Application Firewalls by Chad Russell. Publisher: O’Reilly Media, Inc. (Apr, 2018).
* Agile Application Lifecycle Management: Using DevOps to Drive Process Improvement, 1st Ed. by Bob Aiello, Leslie Sachs. Publisher: Addison-Wesley Professional. (Jun, 2016).
* Agile Application Security by Laura Bell, Rich Smith, Michael Brunton-Spall, Jim Bird. Publisher: O'Reilly Media, Inc. (Jun, 2017).
* Architecting Secure Software Systems, 1st Ed. by Asoke Talukder, Manish Chaitanya. Publisher: Auerbach Publications. (Sep, 2019).
* Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Ed. by Bruce Schneier. Publisher: Wiley. (Mar, 2015).
* Beginning Database Design Solutions by Rod Stephens. Publisher: Jossey-Bass. (Nov, 2008).
* Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syngress. (Sep, 2013).
* Cloud Storage Security: A Practical Guide by Aaron Wheeler, Michael Winburn. Publisher: Elsevier. (Jul, 2015).
* Common Criteria for Information Technology Security Evaluation, Version 3.1 Rev. 5 by Mead, N. Publisher: Carnegie. (Apr, 2017).
* Data Center Handbook, 2nd Ed. by Hwaiyu Geng. Publisher: Wiley. (May, 2021).
* Disaster Recovery and Business Continuity, 3rd Ed. by B.S. Thejandra. Publisher: IT Governance Publishing. (Jan, 2014).
* Enterprise Security Architecture: A Business-Driven Approach, 1st Ed. by John Sherwood. Publisher: CRC Press. (Nov, 2015).
* Identity and Access Management: Business Performance Through Connected Intelligence, 1st Ed. by Ertem Osmanoglu. Publisher: Syngress. (Nov, 2013).
* Information Security Management Handbook, Vol. 6, 6th Ed. by Harold F. Tipton and Micki Krause Nozaki. Publisher: Auerbach Publications. (Apr, 2016).
* Information Security Management Handbook, Vol. 7, 6th Ed. by Richard O'Hanley, James Tiller. Publisher: Auerbach Publications. (Aug, 2013).
* NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems by Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes. (May, 2010).
* NIST SP 800-57, Rev. 5, Recommendation for Key Management: Part 1 – General by Elaine Barker. Publisher: NIST. (May, 2020) .
* NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone. (Aug, 2012).
* NIST SP 800-63-3, Digital Identity Guidelines: Enrollment and Identity Proofing by Paul A. Grassi, James L. Fenton, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, Mary F. Theofanos. (Jun, 2017).
* NIST SP 800-115, Technical Guide to Information Security Testing and Assessment by Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. (Sep, 2008).
* ]NIST SP 800-125, Guide to Security for Full Virtualization Technologies by Karen Scarfone, Murugiah Souppaya, Paul Hoffman. (Jan, 2011).
* NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations by Vincent Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, Karen Scarfone. (Jan, 2014).
* Official (ISC)² Guide to the ISSAP CBK, 2nd Ed. by Adam Gordon. Publisher: Auerbach Publications. (Jan, 2017).
* Payment Card Industry Data Security Standards, Requirements and Security Assessment Procedures, Version 3.2.1 by PCI Security Standards Council. Publisher: PCI Security Standards Council, LLC. (May, 2018).
* Practical Internet of Things Security, 2nd Ed. by Brian Russel, Drew Van Duren. Publisher: Packt Publisher. (Nov, 2018).
* SABSA Executive Summary by SABSA. Publisher: The SABSA Institute. (Dec, 2021).
* Secure Coding in C and C++, 2nd Ed. by Robert Seacord. Publisher: Addison-Wesley Professional. (Apr, 2013).
* Security Patterns in Practice: Designing Secure Architectures Using Software Patterns by Eduardo Fernandez-Buglioni. Publisher: Wiley. (May, 2013).
* Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 by Rich Mogull, James Arlen, Adrian Lane, Gunnar Peterson, Mike Rothman, David Mortman. Publisher: Cloud Security Alliance. (Jul, 2017).
* A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7th Ed. by Project Management Institute. Publisher: Project Management Institute. (Aug, 2021).
* INCOSE Systems Engineering Handbook by Walden. Publisher: Wiley. (Jul, 2015).
* Information Assurance Technical Framework 3.1 by National Security Agency Information Assurance Solutions Technical Directors. (Sep, 2002).
* ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation by ISO/IEC. Publisher: National Information Assurance Partnership. (Dec, 2017).
* NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments by Joint Task Force Transformation Initiative. (Sep, 2012).
* NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy by Joint Task Force Transformation Initiative. (Dec, 2018).
* NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View by Joint Task Force Transformation Initiative. (Mar, 2011).
* NIST SP 800-40, Rev. 3, Guide to Enterprise Patch Management Technologies Murugiah Souppaya, Karen Scarfone. (Jul, 2013).
* NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Force Transformation Initiative. (Sep, 2020).
* NIST SP 800-88, Guidelines for Media Sanitization by Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine. (Dec, 2014).
* NIST SP 800-115, Technical Guide to Information Security Testing and Assessment by Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. (Sep, 2008).
* NIST SP 800-160, Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems by Ron Ross, Michael McEvilley, Janet Carrier Oren. (Mar, 2018).
* NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information System and Organizations by Jon Boyens, Celia Paulsen, Rama Moorthy, Nadya Bartol. (Apr, 2015).
* A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7th Ed. by Project Management Institute. Publisher: Project Management Institute. (Aug, 2021).
* Auditing IT Infrastructures for Compliance, 2nd Ed. by Martin Weiss. Publisher: Jones & Bartlett Publishers. (Jul, 2015).
* Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Ed. by Susan Snedaker. Publisher: Syngress. (Sep, 2013).
* Digital Forensics and Incident Response, 2nd Ed. by Gerard Johansen. Publisher: Packt Publishing. (Jan, 2020).
* Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference by Jamie Watters, Janet Watters. Publisher: Apress. (Dec, 2013).
* Disaster Recovery Planning: For Computers and Communication Resources by Jon Toigo. Publisher: Wiley. (Jan, 1996).
* Information Security Management Handbook, Vol. 6, 6th Ed. by Harold F. Tipton and Micki Krause Nozaki. Publisher: Auerbach Publications. (Apr, 2016).
* [ISC2 Code of Ethics](https://www.isc2.org/ethics) by ISC2. (Dec, 2023).
* Incident Response & Computer Forensics, 3rd Ed. by Jason Luttgens, Matthew Pepe, Kevin Mandia. Publisher: McGraw-Hill Osborne Media. (Aug, 2014).
* IT Auditing Using Controls to Protect Information Assets, 3rd Edition by Mike Kegerreis, Mike Schiller, Chris Davis. Publisher: McGraw-Hill Education. (Oct, 2019).
* NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments by Joint Task Force Transformation Initiative. (Sep, 2012).
* NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems by Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes. (May, 2010).
* NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy by Joint Task Force Transformation Initiative. (Dec, 2018).
* NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View by Joint Task Force Transformation Initiative. (Mar, 2011).
* NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations by Joint Task Force Transformation Initiative. (Sep, 2020).
* NIST SP 800-55, Rev. 1, Performance Measurement Guide for Information Security by Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, Will Robinson. (Jul, 2008).
* NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide by Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone. (Aug, 2012).
* NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems by Arnold Johnson, Kelley Dempsey, Ron Ross, Sarbari Gupta, Dennis Bailey. (Aug, 2011).
* NIST SP 800-160, Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems by Ron Ross, Michael McEvilley, Janet Carrier Oren. (Mar, 2018).
* Official (ISC)² Guide to the ISSMP CBK by Joseph Steinberg and Harold F. Tipton. Publisher: Auerbach Publications. (Apr, 2016).
* Security Operations Center: Building, Operating, and Maintaining your SOC by Gary McIntyre, Joseph Muniz, Nadhem AlFardan. Publisher: Cisco Press. (Nov, 2015).
* The Disaster Recovery Handbook, 3rd Ed. by Michael Wallace, Lawrence Webber. Publisher: AMACOM. (Dec, 2017).
* Threat Modeling: Designing for Security, 1st Ed. by Adam Shostack. Publisher: Wiley. (Feb, 2014).

**nline Training**

**Official ISC2 Certified in Cybersecurity (CC) eTextbook**

eTextbook Description

[< Return to Listing](https://enroll.isc2.org/product?catalog=CC-EPUB-DESC&utm_source=isc2&utm_medium=button&utm_campaign=GBL-CCetextbook&utm_term=cc-exam-outline&utm_content=training&_gl=1*1qi228n*_gcl_au*MTM5MDA3MTI1OS4xNzQxMDcyMzU2*_ga*MTYxNDY3OTAwLjE3MTQxMTcwODg.*_ga_7V1PGHSZT0*MTc0MTA3MjM1NS4zLjEuMTc0MTA3Mjg2MC41MC4wLjExMzg5NDczNjc.)



The Official ISC2 Certified in Cybersecurity (CC) eTextbook is your go-to learning resource as you prepare for the CC exam. It provides a comprehensive review of the topics covered in the Official ISC2 Training Course and will help you navigate key cybersecurity concepts as you build confidence for exam day.

**Price: $24.95**

**Language:**

English

Japanese

**Who Should Purchase:**

IT professionals, career-changers, college students, recent graduates and executives seeking foundational knowledge in cybersecurity. ISC2 is offering free Certified in Cybersecurity (CC) Online Self-Paced Training and an exam to 1 million people as part of our pledge to help close the cybersecurity workforce gap and diversify those working in the field. To meet every learner’s needs, we’re also offering two CC Training Bundles with special extras. Learn more.

**What to Expect:**

A comprehensive review of the Official ISC2 Training Course content related to the ISC2 Certified in Cybersecurity exam. Learning supports include:

 Chapter overviews, objectives and summaries

 Informative graphics

 Key terms and definitions

 Chapter quizzes and answer keys

**CPE Credits**

None

**Access Period:**

365 days from inital access

**This eTextbook covers the following:**

**Chapter 1: Security Principles**

* • 1: Understand the Security Concepts of Information Assurance
* • 2: Understand the Risk Management Process
* • 3: Understand Security Controls
* • 4: Understand Governance Elements and Processes
* • 5: Understand ISC2 Code of Ethics

**Chapter 2: Incident Response, Business Continuity and Disaster Recovery Concepts**

* • 1: Understand Incident Response
* • 2: Understand Business Continuity
* • 3: Understand Disaster Recovery

**Chapter 3: Access Controls Concepts**

* • 1: Understand Access Control Concepts
* • 2: Understand Physical Access Controls
* • 3: Understand Logical Access Controls

**Chapter 4: Network Security**

* • 1: Understand Computer Networking
* • 2: Understand Network (Cyber) Threats and Attacks
* • 3: Understand Network Security Infrastructure

**Chapter 5: Security Operations**

* • 1: Understand Data Security
* • 2: Understand System Hardening
* • 3: Understand Best Practice Security Policies
* • 4: Understand Security Awareness Training

**Technology Requirements:**

The CC eTextbook uses VitalSource eReader, which will allow you to view materials on multiple devices and platforms, online and offline.

The following may be among system requirements to access your eTextbook.

* A stable and continuous internet connection.

**Hardware Specifications**

* • Processor 2 GHz +
* • RAM 4 GB +
* • Monitor minimum resolution (1024 x 768)
* • Video Card
* • Keyboard and Mouse or other assistive technology

**Supported Operating Systems**

* • Macintosh OS X 10.10 to present
* • Windows 10 to present

**Supported Browsers**

* • Google Chrome
* • Microsoft Edge
* • Mozilla Firefox

**Application Software**

* VitalSource eReader
* Certification **Exam Outline**
* Effective Date: November 15, 20222
* ISSMP Certification Exam Outline
* **About CISSP-ISSMP**
* The Information Systems Security Management Professional (ISSMP) is a CISSP who specializes in establishing,
* presenting and governing information security programs and demonstrates management and leadership
* skills. CISSP-ISSMPs direct the alignment of security programs with the organization’s mission, goals and
* strategies in order to meet enterprise financial and operational requirements in support of its desired risk
* position.
* The broad spectrum of topics included in the CISSP-ISSMP Common Body of Knowledge (CBK®) ensure its
* relevancy across all disciplines in the field of information security management. Successful candidates are
* competent in the following six domains:
* • Leadership and Business Management
* • Systems Lifecycle Management
* • Risk Management
* • Threat Intelligence and Incident Management
* • Contingency Management
* • Law, Ethics and Security Compliance Management
* **Experience Requirements**
* Candidates must be a CISSP in good standing and have two years cumulative paid work experience
* in one or more of the six domains of the CISSP-ISSMP CBK. You can learn more about CISSP-ISSMP
* experience requirements and how to account for part-time work and internships at
* www.isc2.org/Certifications/CISSP-Concentrations#steps-to-certification.
* Accreditation
* CISSP-ISSMP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.
* Job Task Analysis (JTA)
* (ISC)² has an obligation to its membership to maintain the relevancy of the CISSP-ISSMP. Conducted at
* regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that
* are performed by security professionals who are engaged in the profession defined by the CISSP-ISSMP. The
* results of the JTA are used to update the examination. This process ensures that candidates are tested on the
* topic areas relevant to the roles and responsibilities of today’s practicing information security professionals.3
* ISSMP Certification Exam Outline
* **CISSP-ISSMP Examination Information**
* **CISSP-ISSMP Examination Weights**
* **Length of exam**
* **Number of items**
* **Item format**
* **Passing grade**
* **Exam availability**
* **Testing center**
* 3 hours
* 125
* Multiple choice
* 700 out of 1000 points
* English
* Pearson VUE Testing Center
* **Domains**
* **Weight**
* 1. Leadership and Business Management
* 20%
* 2. Systems Lifecycle Management
* 18%
* 3. Risk Management
* 19%
* 4. Threat Intelligence and Incident Management
* 17%
* 5. Contingency Management
* 15%
* 6. Law, Ethics and Security Compliance Management
* 11%
* **Total: 100%**4
* ISSMP Certification Exam Outline
* **Domain 1:**
* **Leadership and Business Management**
* 1.1 Establish security’s role in organizational culture, vision and mission
* » Define information security program vision and mission
* » Align security with organizational goals, objectives and values
* » Define security’s relationship to the overall business processes
* » Define the relationship between organizational culture and security
* 1.2 Align security program with organizational governance
* » Identify and navigate organizational governance structure
* » Validate roles of key stakeholders
* » Validate sources and boundaries of authorization
* » Advocate and obtain organizational support for security initiatives
* 1.3 Define and implement information security strategies
* » Identify security requirements from business initiatives
* » Evaluate capacity and capability to implement security strategies
* » Manage implementation of security strategies
* » Review and maintain security strategies
* » Prescribe security architecture and engineering theories, concepts and methods
* 1.4 Define and maintain security policy framework Determine applicable external standards
* » Determine applicable external standards
* » Determine data classification and protection requirements
* » Establish internal policies
* » Advocate and obtain organizational support for policies
* » Develop procedures, standards, guidelines and baselines
* » Ensure periodic review of security policy framework5
* ISSMP Certification Exam Outline
* » Define roles and responsibilities
* » Determine and manage team accountability
* » Build cross-functional relationships
* » Resolve conflicts between security and
* other stakeholders
* » Identify communication bottlenecks
* and barriers
* » Integrate security controls into human
* resources processes
* » Evaluate service management agreements
* (e.g., risk, financial)
* » Govern managed services
* (e.g., infrastructure, cloud services)
* » Manage impact of organizational change (e.g.,
* mergers and acquisitions, outsourcing)
* » Ensure that appropriate regulatory compliance
* statements and requirements are included in
* contractual agreements
* » Monitor and enforce compliance with
* contractual agreements
* 1.5 Manage security requirements in contracts and agreements
* 1.6 Manage security awareness and training programs
* » Promote security programs to key stakeholders
* » Identify needs and implement training programs by target segment
* » Monitor and report on effectiveness of security awareness and training programs
* 1.7 Define, measure and report security metrics
* » Identify Key Performance Indicators (KPI)
* » Associate Key Performance Indicators (KPI) to the risk posture of the organization
* » Use metrics to drive security program development and operations
* 1.8 Prepare, obtain and administer security budget
* » Prepare and secure annual budget
* » Adjust budget based on evolving risks and threat landscape
* » Manage and report financial responsibilities
* 1.9 Manage security programs
* 1.10 Apply product development and project management principles
* » Incorporate security into project lifecycle
* » Identify and apply appropriate project management methodology
* » Analyze project time, scope and cost relationship6
* ISSMP Certification Exam Outline
* 2.1 Manage integration of security into Systems Development Life Cycle (SDLC)
* » Integrate information security gates (decision points) and requirements into lifecycle
* » Implement security controls into system lifecycle
* » Oversee security configuration management (CM) processes
* 2.2 Integrate new business initiatives and emerging technologies into the
* security architecture
* » Integrate security into new business initiatives and emerging technologies
* » Address impact of new business initiatives on security posture
* 2.3 Define and oversee comprehensive vulnerability management programs
* (e.g., vulnerability scanning, penetration testing, threat analysis)
* » Identify, classify and prioritize assets, systems and services based on criticality to business
* » Prioritize threats and vulnerabilities
* » Manage security testing
* » Manage mitigation and/or remediation of vulnerabilities based on risk
* 2.4 Manage security aspects of change control
* » Integrate security requirements with change control process
* » Identify and coordinate with the stakeholders
* » Manage documentation and tracking
* » Ensure policy compliance (e.g., continuous monitoring)
* **Domain 2:**
* **Systems Lifecycle Management** 7
* ISSMP Certification Exam Outline
* **Domain 3:**
* **Risk Management**
* 3.1 Develop and manage a risk management program
* » Identify risk management program objectives
* » Communicate and agree on risk management objectives with risk owners and other stakeholders
* » Determine scope of organizational risk program
* » Identify organizational security risk tolerance/appetite
* » Obtain and verify organizational asset inventory
* » Analyze organizational risks
* » Determine countermeasures, compensating and mitigating controls
* » Perform cost-benefit analysis (CBA) of risk treatment options
* 3.2 Conduct risk assessments
* » Identify risk factors
* 3.3 Manage security risks within the supply chain (e.g., supplier, vendor, third-party risk)
* » Identify supply chain security risk requirements
* » Integrate supply chain security risks into organizational risk management
* » Validate security risk control within the supply chain
* » Monitor and review the supply chain security risks8
* ISSMP Certification Exam Outline
* 4.1 Establish and maintain threat intelligence program
* » Aggregate threat data from multiple threat intelligence sources
* » Conduct baseline analysis of network traffic, data and user behavior
* » Detect and analyze anomalous behavior patterns for potential concerns
* » Conduct threat modeling
* » Identify and categorize an attack
* » Correlate related security event and threat data
* » Create actionable alerting to appropriate resources
* 4.2 Establish and maintain incident handling and investigation program
* » Develop program documentation
* » Establish incident response case management process
* » Establish incident response team
* » Apply incident management methodologies
* » Establish and maintain incident handling process
* » Establish and maintain investigation process
* » Quantify and report financial and operational impact of incidents and investigations to stakeholders
* » Conduct root cause analysis (RCA)
* **Domain 4:**
* **Threat Intelligence and Incident**
* **Management** 9
* ISSMP Certification Exam Outline
* 5.1 Facilitate development of contingency plans
* » Identify and analyze factors related to the Continuity of Operations Plan (COOP)
* » Identify and analyze factors related to the business continuity plan (BCP) (e.g., time, resources, verification)
* » Identify and analyze factors related to the disaster recovery plan (DRP) (e.g., time, resources, verification)
* » Coordinate contingency management plans with key stakeholders
* » Define internal and external crisis communications plans
* » Define and communicate contingency roles and responsibilities
* » Identify and analyze contingency impact on business processes and priorities
* » Manage third-party contingency dependencies
* » Prepare security management succession plan
* 5.2 Develop recovery strategies
* » Identify and analyze alternatives
* » Recommend and coordinate recovery strategies
* » Assign recovery roles and responsibilities
* 5.3 Maintain contingency plan, Continuity of Operations Plan (COOP), business continuity
* plan (BCP) and disaster recovery plan (DRP)
* » Plan testing, evaluation and modification
* » Determine survivability and resiliency capabilities
* » Manage plan update process
* 5.4 Manage disaster response and recovery process
* » Declare disaster
* » Implement plan
* » Restore normal operations
* » Gather lessons learned
* » Update plan based on lessons learned
* **Domain 5:**
* **Contingency Management** 10
* ISSMP Certification Exam Outline
* 10
* 6.1 Identify the impact of laws and regulations that relate to information security
* 6.2 Adhere to the (ISC)
* 2
* Code of Ethics as related to management issues
* 6.3 Validate compliance in accordance with applicable laws, regulations and industry
* best practices
* 6.4 Coordinate with auditors and regulators in support of the internal and external
* audit processes
* 6.5 Document and manage compliance exceptions
* » Identify and document compensating controls and workarounds
* » Report and obtain authorized approval of risk waiver
* **Domain 6:**
* **Law, Ethics and Security Compliance**
* **Management**
* » Identify applicable privacy laws
* » Identify legal jurisdictions the organization and
* users operate within (e.g., trans-border data flow)
* » Identify export laws
* » Identify intellectual property (IP) laws
* » Identify applicable industry regulations
* » Identify and advise on non-compliance risks
* » Inform and advise senior management
* » Evaluate and select compliance framework(s)
* » Implement the compliance framework(s)
* » Define and monitor compliance metrics
* » Plan
* » Schedule
* » Coordinate audit activities
* » Evaluate and validate findings
* » Formulate response
* » Validate implemented mitigation and
* remediation actions11
* ISSMP Certification Exam Outline
* **Additional Examination Information**
* Supplementary References
* Candidates are encouraged to supplement their education and experience by reviewing
* relevant resources that pertain to the CBK and identifying areas of study that may need
* additional attention.
* View the full list of supplementary references at www.isc2.org/certifications/References.
* Examination Policies and Procedures
* (ISC)2 recommends that CISSP-ISSMP candidates review exam policies and procedures
* prior to registering for the examination. Read the comprehensive breakdown of this
* important information at www.isc2.org/Exams/Before-Your-Exam.
* Legal Info
* For any questions related to (ISC)
* 2
* ’s legal policies, please contact the (ISC)2 Legal
* Department at legal@isc2.org.
* Any Questions?
* (ISC)2 Americas
* Tel: +1.866.331.ISC2 (4722)
* Email: info@isc2.org
* (ISC)2 Asia-Pacific
* Tel: +(852) 28506951
* Email: isc2asia@isc2.org
* (ISC)2 EMEA
* Tel: +44 (0)203 300 1625
* Email: info-emea@isc2.org
* 11

v222[Register for exam](https://www.isc2.org/register-for-exam)

Effective Date: August 29, 2022

# Certified in Cybersecurity Certification Exam Outline

View and download the latest PDF version of the Certified in Cybersecurity Exam Outline in the following languages:

[CC - English](https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/exam-outlines/Certified-in-Cybersecurity-Exam-Outline-August-2022-English.pdf)  |  [CC - Chinese](https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/exam-outlines/Certified-in-Cybersecurity-Exam-Outline-August-2022-Chinese.pdf)  |  [CC - Japanese](https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/exam-outlines/Certified-in-Cybersecurity-Exam-Outline-August-2022-Japanese.pdf)  |  [CC - German](https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/exam-outlines/Certified-in-Cybersecurity-Exam-Outline-August-2022-German.pdf)  |  [CC - Spanish](https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/exam-outlines/Certified-in-Cybersecurity-Exam-Outline-August-2022-Spanish.pdf)

## About Certified in Cybersecurity

ISC2 developed the Certified in Cybersecurity (CC) credential for newcomers to the field, to recognize the growing trend of people entering the cybersecurity workforce without direct IT experience. Getting Certified in Cybersecurity provides employers with the confidence that you have a solid grasp of the right technical concepts, and a demonstrated aptitude to learn on the job. As an ISC2 certification, those who hold the CC are backed by the world’s largest network of certified cybersecurity professionals helping them continue their professional development and earn new achievements and qualifications throughout their career.

The topics on the CC exam include:

* Security Principles
* Incident Response, Business Continuity (BC) and Disaster Recovery (DR) Concepts
* Access Controls Concepts
* Network Security
* Security Operations

### Certified in Cybersecurity Examination Information

|  |  |
| --- | --- |
| **Length of exam** | 2 hours |
| **Number of items** | 100 |
| **Item format** | Multiple choice |
| **Passing grade** | 700 out of 1000 points |
| **Exam language availability** | English, Chinese, Japanese, German, Spanish |
| **Testing center** | Pearson VUE Testing Center |

## Certified in Cybersecurity Examination Weights

| **Domains** | **Average Weight** |
| --- | --- |
| 1. Security Principles | 26% |
| 2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts | 10% |
| 3. Access Controls Concepts | 22% |
| 4. Network Security | 24% |
| 5. Security Operations | 18% |
| **Total** | **100%** |

###### [Boost your chances of passing the exam with the CC eTextbook](https://enroll.isc2.org/product?catalog=CC-EPUB-DESC&utm_source=isc2&utm_medium=button&utm_campaign=GBL-CCetextbook&utm_term=cc-exam-outline&utm_content=training&_gl=1*1q8i4eg*_gcl_au*MTM5MDA3MTI1OS4xNzQxMDcyMzU2*_ga*MTYxNDY3OTAwLjE3MTQxMTcwODg.*_ga_7V1PGHSZT0*MTc0MTA3MjM1NS4zLjEuMTc0MTA3MjkyMC41MC4wLjExMzg5NDczNjc." \t "_blank)

[Build your fundamental cybersecurity knowledge and prepare for the exam.](https://enroll.isc2.org/product?catalog=CC-EPUB-DESC&utm_source=isc2&utm_medium=button&utm_campaign=GBL-CCetextbook&utm_term=cc-exam-outline&utm_content=training&_gl=1*1q8i4eg*_gcl_au*MTM5MDA3MTI1OS4xNzQxMDcyMzU2*_ga*MTYxNDY3OTAwLjE3MTQxMTcwODg.*_ga_7V1PGHSZT0*MTc0MTA3MjM1NS4zLjEuMTc0MTA3MjkyMC41MC4wLjExMzg5NDczNjc." \t "_blank)

[Get eTextbook](https://enroll.isc2.org/product?catalog=CC-EPUB-DESC&utm_source=isc2&utm_medium=button&utm_campaign=GBL-CCetextbook&utm_term=cc-exam-outline&utm_content=training&_gl=1*1q8i4eg*_gcl_au*MTM5MDA3MTI1OS4xNzQxMDcyMzU2*_ga*MTYxNDY3OTAwLjE3MTQxMTcwODg.*_ga_7V1PGHSZT0*MTc0MTA3MjM1NS4zLjEuMTc0MTA3MjkyMC41MC4wLjExMzg5NDczNjc." \t "_blank)

## Domains

## 1.1 - Understand the security concepts of information assurance

* Confidentiality
* Integrity
* Availability
* Authentication (e.g., methods of authentication, multi-factor authentication (MFA))
* Non-repudiation
* Privacy

## 1.2 - Understand the risk management process

* Risk management (e.g., risk priorities, risk tolerance)
* Risk identification, assessment and treatment

## 1.3 - Understand security controls

* Technical controls
* Administrative controls
* Physical controls

## 1.4 - Understand ISC2 Code of Ethics

* Professional code of conduct

## 1.5 - Understand governance processes

* Policies
* Procedures
* Standards
* Regulations and laws

## 2.1 - Understand business continuity (BC)

* Purpose
* Importance
* Components

## 2.2 - Understand disaster recovery (DR)

* Purpose
* Importance
* Components

## 2.3 - Understand incident response

* Purpose
* Importance
* Components

## 3.1 - Understand physical access controls

* Physical security controls (e.g., badge systems, gate entry, environmental design)
* Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)
* Authorized versus unauthorized personnel

## 3.2 - Understand logical access controls

* Principle of least privilege
* Segregation of duties
* Discretionary access control (DAC)
* Mandatory access control (MAC)
* Role-based access control (RBAC)

## 4.1 - Understand computer networking

* Networks (e.g., Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), WiFi)
* Ports
* Applications

## 4.2 - Understand network threats and attacks

* Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-channel)
* Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))
* Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))

## 4.3 - Understand network security infrastructure

* On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreement (MOA))
* Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, Network Access Control (NAC) (segmentation for embedded systems, Internet of Things (IoT))
* Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid)

## 5.1 - Understand data security

* Encryption (e.g., symmetric, asymmetric, hashing)
* Data handling (e.g., destruction, retention, classification, labeling)
* Logging and monitoring security events

## 5.2 - Understand system hardening

* Configuration management (e.g., baselines, updates, patches)

## 5.3 - Understand best practice security policies

* Data handling policy
* Password policy
* Acceptable Use Policy (AUP)
* Bring your own device (BYOD) policy
* Change management policy (e.g., documentation, approval, rollback)
* Privacy policy

## 5.4 - Understand security awareness training

* Purpose/concepts (e.g., social engineering, password protection)
* Importance

A safe and secure cyber world

The Center for Cyber Safety & EducationISC2 CareersCommunityBlog

Frequently Asked QuestionsContact UsPolicies and Procedures

ISC2 Authorized China AgencyISC2 Japan

© Copyright 1996-2025. ISC2, Inc. All Rights Reserved.

All contents of this site constitute the property of ISC2, Inc. and may not be copied, reproduced or distributed without prior written permission. ISC2, CISSP, SSCP, CCSP, CGRC, CSSLP, HCISPP, ISSAP, ISSEP, ISSMP, CC, and CBK are registered marks of ISC2, Inc.

[Sitemap](https://www.isc2.org/sitemap.html)

[](https://community.isc2.org/)[](https://www.facebook.com/isc2fb)[](https://www.linkedin.com/company/isc2)[](https://twitter.com/ISC2)[](https://www.youtube.com/user/ISC2TV)

Certified in Cybersecurity Exam Outline

**Access Period:**

365 days from inital access

**This eTextbook covers the following:**

**Chapter 1: Security Principles**

* • 1: Understand the Security Concepts of Information Assurance
* • 2: Understand the Risk Management Process
* • 3: Understand Security Controls
* • 4: Understand Governance Elements and Processes
* • 5: Understand ISC2 Code of Ethics

**Chapter 2: Incident Response, Business Continuity and Disaster Recovery Concepts**

* • 1: Understand Incident Response
* • 2: Understand Business Continuity
* • 3: Understand Disaster Recovery

**Chapter 3: Access Controls Concepts**

* • 1: Understand Access Control Concepts
* • 2: Understand Physical Access Controls
* • 3: Understand Logical Access Controls

**Chapter 4: Network Security**

* • 1: Understand Computer Networking
* • 2: Understand Network (Cyber) Threats and Attacks
* • 3: Understand Network Security Infrastructure

**Chapter 5: Security Operations**

* • 1: Understand Data Security
* • 2: Understand System Hardening
* • 3: Understand Best Practice Security Policies
* • 4: Understand Security Awareness Training

**Technology Requirements:**

The CC eTextbook uses VitalSource eReader, which will allow you to view materials on multiple devices and platforms, online and offline.

The following may be among system requirements to access your eTextbook.

* A stable and continuous internet connection.

**Hardware Specifications**

* • Processor 2 GHz +
* • RAM 4 GB +
* • Monitor minimum resolution (1024 x 768)
* • Video Card
* • Keyboard and Mouse or other assistive technology

**Supported Operating Systems**

* • Macintosh OS X 10.10 to present
* • Windows 10 to present

**Supported Browsers**

* • Google Chrome
* • Microsoft Edge
* • Mozilla Firefox

**Application Software**

* VitalSource eReader

## Online Training

# Continuing education

Stay relevant and on top of the latest trends. Leverage our online courses to gain interactive, engaging and timely learning experiences throughout your career. Each course is designed with input from leading industry experts and based on proven learning techniques to maximize your time and content retention.

The self-paced learning format delivers modular content combined with interactive activities involving videos, labs, case studies, quizzes, etc. Learn at your own pace on your own time and earn valuable Continuing Professionals Education (CPE) credits towards your ISC2; certifications. (Note: Credits may be eligible for continuing education credits for non-ISC2 certifications. Please review the requirements established by the credentialing organization for eligibility.)

**ISC2; Members and Associates have free unlimited access to courses** that are denoted as ‘Free for Members’ by logging in above and clicking the ‘My Courses’ menu item.

**For individual course purchases learners will have access to the course content for 180 days from the time of purchase.** Please note, we do not offer time extensions for you to complete this training course.

**For All Access and Express Learning Bundle purchases learners will have access to the course content for 365 day from the time of purchase.** Please see course description for pricing and CPEs.

**1** [2](https://enroll.isc2.org/?page=2&pagename=Continuing-education) [3](https://enroll.isc2.org/?page=3&pagename=Continuing-education) [>](https://enroll.isc2.org/?page=2&pagename=Continuing-education) [>|](https://enroll.isc2.org/?page=3&pagename=Continuing-education)

|  |  |  |
| --- | --- | --- |
|  | Certification |  |
|  | [Defining the Boundaries of Zero Trust](https://enroll.isc2.org/product?catalog=ISC2-CPD-DEFBOUNZEROTRUST-PUB)  This learning experience invites you to review the set of guiding principles for workflow, system design, and operations that create a zero trust architecture. (2.0 CPE) | Top of Form  Bottom of Form |
| Top of Form  Bottom of Form |
|  | [Software Inventory and SBOM](https://enroll.isc2.org/product?catalog=ISC2-CPD-SoftwareInventorySBOM-PUB)  This course invites you to expand your knowledge of how Software Bill of Materials (SBOM) can help cybersecurity professionals effectively mitigate vulnerabilities and ensure compliance. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Software Inventory and SBOM](https://enroll.isc2.org/product?catalog=ISC2-CPD-SoftwareInventorySBOM-MBR)  This course invites you to expand your knowledge of how Software Bill of Materials (SBOM) can help cybersecurity professionals effectively mitigate vulnerabilities and ensure compliance. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Working in the Cloud](https://enroll.isc2.org/product?catalog=ISC2-CPD-WorkingCloudV2-PUB)  This course invites you to learn about the range of challenges security professionals face as they work to utilize, optimize and secure critical assets in the cloud. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Working in the Cloud](https://enroll.isc2.org/product?catalog=ISC2-CPD-WorkingCloudV2-MBR)  This course invites you to learn about the range of challenges security professionals face as they work to utilize, optimize and secure critical assets in the cloud. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Moving to the Cloud](https://enroll.isc2.org/product?catalog=ISC2-CPD-MovingCloudV2-PUB)  This course invites you to learn about the strategic and security considerations necessary to transition an organization to cloud computing in alignment with business needs. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Moving to the Cloud](https://enroll.isc2.org/product?catalog=ISC2-CPD-MovingCloudV2-MBR)  This course invites you to learn about the strategic and security considerations necessary to transition an organization to cloud computing in alignment with business needs. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Cloud Basics](https://enroll.isc2.org/product?catalog=ISC2-CPD-CloudBasicsV2-PUB)  This course invites you to learn about essential cloud concepts and principles, including key drivers for use, essential characteristics, and service and deployment models within cloud architectures. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Cloud Basics](https://enroll.isc2.org/product?catalog=ISC2-CPD-CloudBasicsV2-MBR)  This course invites you to learn about essential cloud concepts and principles, including key drivers for use, essential characteristics, and service and deployment models within cloud architectures. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Building Your Personal Brand and Digital Presence](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-BUILDPERBRAND-MBR)  This course invites you to review the essentials of building a personal brand and digital presence that reflects your core values, unique strengths and professional aspirations. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Resume/CV/Portfolio Building and Management](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-RESUMECVPORT-MBR)  This course invites you to review the critical components of documents such as resumes, CVs and portfolios that showcase your unique strengths and value to potential employers. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Identifying and Building Your Network](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-IDENTBUILDNETWRK-MBR)  This course invites you to review the critical role networking plays in professional development by unlocking new opportunities, facilitating knowledge sharing and supporting long-term career success. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Identifying Your Cyber Path and Industry](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-IDENTCYBERPATHSINDUSTRY-MBR)  This course invites you to explore a wide range of opportunities in cybersecurity and plan a skill development path toward a successful career. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Nailing the Interview Process](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-NAILINGTHEINTERVIEWPROCESS-MBR)  This course invites you to review actionable strategies and skills to excel in any interview scenario and stand out from the competition. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Managing the Offer and Negotiation Process](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-MANAGINGOFFERNEGOTIATIONPROCESS-MBR)  This course invites you to review the essential knowledge and skills to navigate job offers, negotiate confidently and transition smoothly into new roles. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Managing the Offer and Negotiation Process](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-MANAGINGOFFERNEGOTIATIONPROCESS-PUB)  This course invites you to review the essential knowledge and skills to navigate job offers, negotiate confidently and transition smoothly into new roles. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Nailing the Interview Process](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-NAILINGTHEINTERVIEWPROCESS-PUB)  This course invites you to review actionable strategies and skills to excel in any interview scenario and stand out from the competition. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Identifying Your Cyber Path and Industry](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-IDENTCYBERPATHSINDUSTRY-PUB)  This course invites you to explore a wide range of opportunities in cybersecurity and plan a skill development path toward a successful career. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Identifying and Building Your Network](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-IDENTBUILDNETWRK-PUB)  This course invites you to review the critical role networking plays in professional development by unlocking new opportunities, facilitating knowledge sharing and supporting long-term career success. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |
|  | [Resume/CV/Portfolio Building and Management](https://enroll.isc2.org/product?catalog=ISC2-PDI-SEC-RESUMECVPORT-PUB)  This course invites you to review the critical components of documents such as resumes, CVs and portfolios that showcase your unique strengths and value to potential employers. | Top of Form  Bottom of Form |

|  |
| --- |
| Top of Form  Bottom of Form |

**1** [2](https://enroll.isc2.org/?page=2&pagename=Continuing-education) [3](https://enroll.isc2.org/?page=3&pagename=Continuing-education) [>](https://enroll.isc2.org/?page=2&pagename=Continuing-education) [>|](https://enroll.isc2.org/?page=3&pagename=Continuing-education)

Top of Form

Bottom of Form

[Go to the main content](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517#skipToMainContent)

**Privacy and Cookies** This website stores cookies on your computer which help us make the website work better for you.

ISC2 logo

[Collapsed, toggle side navigation to expand](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517)

Edit my profile  Tshingombe Tshingombe Tshitadi    
ISC2 ID: 1907033

* [Dashboard](https://wsr.pearsonvue.com/testtaker/registration/Dashboard/ISC2)

* [My Profile](https://wsr.pearsonvue.com/testtaker/common/MastHeadExternalReturnUrlRedirect/ISC2)

* [Sign out](https://wsr.pearsonvue.com/testtaker/common/SessionExpired.htm?signOut)

Top of Form

Bottom of Form

**Find an exam**

Top of Form

Find an Exam: 

Bottom of Form

Top of Form

Bottom of Form

Top of Form

|  |
| --- |

Bottom of Form

Top of Form

|  |
| --- |
| CC | [Certified in Cybersecurity (CC)](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Certified in Cybersecurity (CC)) |
| CCSP | [Certified Cloud Security Professional (CCSP)](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Certified Cloud Security Professional (CCSP)) |
| CGRC | [Certified in Governance Risk and Compliance](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Certified in Governance Risk and Compliance) |
| CISSP | [Certified Information Systems Security Professional](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Certified Information Systems Security Professional) |
| CSSLP | [Certified Secure Software Lifecycle Professional](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Certified Secure Software Lifecycle Professional) |
| ISSAP | [Information Systems Security Architecture Professional](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Information Systems Security Architecture Professional) |
| ISSEP | [Information Systems Security Engineering Professional](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Information Systems Security Engineering Professional) |
| ISSMP | [Information Systems Security Management Professional](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Information Systems Security Management Professional) |
| SSCP | [Systems Security Certified Practitioner](https://wsr.pearsonvue.com/testtaker/registration/SelectExamPage/ISC2?conversationId=1682517" \o "Systems Security Certified Practitioner) |

Bottom of Form

* [Terms](https://wsr.pearsonvue.com/legal/appterms/)
* [Privacy](https://wsr.pearsonvue.com/legal/appprivacy/)
* [Contact](https://wsr.pearsonvue.com/contact/)

Copyright 1996-2025 Pearson Education Inc. or its affiliate(s). All rights reserved.

https://vtswebresources.pearsonvue.com/webresources/testtaker/images/ajax-loader.gif

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | | **Certification is Just the Beginning**  Achieving your certification isn’t the end of your journey. ISC2 members and associates are part of a global community of cybersecurity professionals with access to a long list of benefits that include continuing professional education, peer-to-peer networking and exclusive discounts.    Stay focused on your goal and make the most of what’s ahead. |  |  |  |  | | --- | --- | --- | | |  |  | | --- | --- | | |  | | --- | | [Preview Your Benefits](https://cl.s12.exct.net/?qs=141fdf9b710e6444d89fd17bd0cf187a854ed00c4473ccf0b18b088185164756ef7b5c16c9cef7a0b7e831aac3da3ecd866b01ce947282799983786b9beba9dc) | | |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  |  |  |  | | --- | --- | | |  | | --- | |  | | | | | |  |  |  | | --- | --- | --- | | |  |  | | --- | --- | | |  | | --- | |  | | | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | |  | | ISC2 625 N Washington Street, Suite 400, Alexandria, VA 22314, United States • [www.isc2.org](https://cl.s12.exct.net/?qs=141fdf9b710e64448965569cd7dc7f5c32e8e2507c489168a6f39379ef562a5990aab37fea58ddc024bb9c3e9e9fb810d20e93b83a773dce6dce0e68e7b9f9ec)  © 1996–2024. ISC2, Inc. All rights reserved. | |  |  |  | | --- | --- | | |  | | --- | | You're receiving this email because you've expressed interest in Certifications, Education Resources and Offers. Click to [unsubscribe](https://cl.S12.exct.net/unsub_center.aspx?qs=bd1419acc75bfc7408a74d111787099437caaea4bb40d3b246c1b2229d43c952fa7e4d35b94f8df3870959e9fc69587d4326380aa8dea61ef3f1ad857e64118bb94ec02128a2f950), or update your [subscription preferences](https://cl.s12.exct.net/?qs=141fdf9b710e644474aad03487a00371b862ce461264e262da2bc3dd556b5fd9a7b28185ae0cb4fa91a2977413cf8326fb557d55f9765cd08eb9c91325253336) on the Member Website. | | | | | | | | | | |
| https://lh3.googleusercontent.com/a/ACg8ocKXAkWuMsvk1UB4tteph7ml8jYF0m9hC26Hrh4GoZCA5eWrXg=s80-p-mo |  |

[Register for exam](https://www.isc2.org/register-for-exam)

Effective Date: September 2024

**SSCP Certification Exam Outline**

View and download the latest PDF version of the SSCP Certification Exam Outline in the following languages:

[SSCP - English](https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/certifications/Certs/SSCP/EXAMS-SSCP-Exam_Outline-English.pdf)  |  [SSCP - Japanese](https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/certifications/Certs/SSCP/EXAMS-SSCP-Exam_Outline-Japanese.pdf)  |  [SSCP - Spanish](https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/certifications/Certs/SSCP/EXAMS-SSCP-Exam_Outline-Spanish.pdf)

**About SSCP**

The Systems Security Certified Practitioner (SSCP) is the ideal certification for those with proven technical skills and practical, hands-on security knowledge in operational IT roles. It provides confirmation of a practitioner’s ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

The broad spectrum of topics included in the SSCP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following domains:

* Security Concepts and Practices
* Access Controls
* Risk Identification, Monitoring, and Analysis
* Incident Response and Recovery
* Cryptography
* Network and Communications Security
* Systems and Application Security

**Experience Requirements**

Candidates must have a minimum of one year cumulative work experience in one or more of the domains of the SSCP CBK. A one year prerequisite pathway will be granted for candidates who received a degree (bachelors or masters) in a cybersecurity program.

A candidate that doesn’t have the required experience to become an SSCP may become an Associate of ISC2 by successfully passing the SSCP examination. The Associate of ISC2 will then have two years to earn the one year required experience. You can learn more about SSCP experience requirements and how to account for part-time work and internships at [www.isc2.org/Certifications/SSCP/SSCP-Experience-Requirements](https://www.isc2.org/certifications/sscp/sscp-experience-requirements).

**Accreditation**

SSCP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

**Job Task Analysis (JTA)**

ISC2 has an obligation to its membership to maintain the relevancy of the SSCP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the SSCP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today’s practicing information security professionals.

**SSCP Examination Information**

|  |  |
| --- | --- |
| **Length of exam** | 3 hours |
| **Number of items** | 125 |
| **Item format** | Multiple choice |
| **Passing grade** | 700 out of 1000 points |
| **Language availability** | English, Japanese and Spanish |
| **Testing center** | Pearson VUE Testing Center |

**SSCP Examination Weights**

| **Domains** | **Average Weight** |
| --- | --- |
| 1. Security Concepts and Practices | 16% |
| 2. Access Controls | 15% |
| 3. Risk Identification, Monitoring and Analysis | 15% |
| 4. Incident Response and Recovery | 14% |
| 5. Cryptography | 9% |
| 6. Network and Communications Security | 16% |
| 7. Systems and Application Security | 15% |
| **Total** | **100%** |

**Domains**

**1.1 - Comply with codes of ethics**

* ISC2 Code of Ethics
* Organizational code of ethics

**1.2 - Understand security concepts**

* Confidentiality
* Integrity
* Availability
* Accountability
* Non-repudiation
* Least privilege
* Segregation of duties (SoD)

**1.3 - Identify and implement security controls**

* Technical controls (e.g., firewalls, intrusion detection systems (IDS), access control list (ACL)
* Physical controls (e.g., mantraps, cameras, locks)
* Administrative controls (e.g., security policies, standards, procedures, baselines)
* Assessing compliance requirements
* Periodic audit and review

**1.4 - Document and maintain functional security controls**

* Deterrent controls
* Preventative controls
* Detective controls
* Corrective controls
* Compensating controls

**1.5 - Support and implement asset management lifecycle (i.e., hardware, software, and data)**

* Process, planning, design and initiation
* Development /Acquisition (e.g., DevSecOps, testing)
* Inventory and licensing (e.g., open source, closed-source)
* Implementation/Assessment
* Operation/Maintenance/End of Life (EOL)
* Archival and retention requirements
* Disposal and destruction

**1.6 - Support and/or implement change management lifecycle**

* Change management (e.g., roles, responsibilities, processes, communications, audit)
* Security impact analysis
* Configuration management (CM)

**1.7 - Support and/or implement security awareness and training (e.g., social engineering/phishing/tabletop exercises/awareness communications)**

**1.8 - Collaborate with physical security operations (e.g., data center/facility assessment, badging and visitor management, personal device restrictions)**

**2.1 - Implement and maintain authentication methods**

* Single/Multi-factor authentication (MFA)
* Single sign-on (SSO) (e.g., Active Directory Federation Services (ADFS), OpenID Connect)
* Device authentication (e.g., certificate, Media Access Control (MAC) address, Trusted Platform Module (TPM))
* Federated access (e.g., Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))

**2.2 - Understand and support internetwork trust architectures**

* Trust relationships (e.g., 1-way, 2-way, transitive, zero)
* Internet, intranet, extranet, and demilitarized zone (DMZ)
* Third-party connections (e.g., application programming interface (API), app extensions, middleware)

**2.3 - Support and/or implement the identity management lifecycle**

* Authorization
* Proofing
* Provisioning/De-provisioning
* Monitoring, Reporting, and Maintenance (e.g., role changes, new security standards)
* Entitlement (e.g., inherited rights, resources)
* Identity and access management (IAM) systems

**2.4 - Understand and administer access controls**

* Mandatory
* Discretionary
* Role-based (e.g., subject-based, object-based, Privileged Access Management (PAM))
* Rule-based
* Attribute-based

**3.1 - Understand risk management**

* Risk visibility and reporting (e.g., risk register, sharing threat intelligence, indicators of Compromise (IOC), Common Vulnerability Scoring System (CVSS), socialization, MITRE/ATT&CK model)
* Risk management concepts (e.g., impact assessments, threat modeling, scope)
* Risk management frameworks
* Risk tolerance (e.g., appetite, risk quantification)
* Risk treatment (e.g., accept, transfer, mitigate, avoid)

**3.2 - Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)**

**3.3 - Perform security assessments and vulnerability management activities**

* Risk management frameworks implementation
* Security testing
* Risk review (e.g., internal, supplier, architecture)
* Vulnerability management lifecycle (e.g., scanning, reporting, analysis, remediation)

**3.4 - Operate and monitor security platforms (e.g., continuous monitoring)**

* Source systems (e.g., applications, security appliances, network devices, hosts)
* Events of interest (e.g., errors, omissions, anomalies, unauthorized changes, compliance violations, policy failures)
* Log management (e.g., policy, integrity, preservation, architectures, configuration, aggregation, tuning)
* Security information and event management (SIEM) (e.g., real-time monitoring, analysis, tracking, audit)

**3.5 - Analyze monitoring results**

* Security baselines and anomalies (e.g., correlation, noise reduction)
* Visualizations, metrics, and trends (e.g., notifications, dashboards, timelines)
* Event data analysis
* Document and communicate findings (e.g., escalation)

**4.1 - Understand and support incident response lifecycle (e.g., National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO))**

* Preparation (e.g., defining roles, training programs)
* Detection, analysis, and escalation (e.g., incident communication, public relations)
* Containment
* Eradication
* Recovery (e.g., incident documentation)
* Post incident activities (e.g., lessons learned, new countermeasures, continuous improvement)

**4.2 - Understand and support forensic investigations**

* Legal (e.g., civil, criminal, administrative) and ethical principles
* Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)
* Reporting of analysis
* Organization Security Policy Compliance

**4.3 - Understand and support business continuity plan (BCP) and disaster recovery plan (DRP)**

* Emergency response plans and procedures (e.g., information system contingency, pandemic, natural disaster, crisis management)
* Interim or alternate processing strategies
* Restoration planning (e.g., Restore Time Objective (RTO), Restore Point Objectives (RPO), Maximum Tolerable Downtime (MTD))
* Backup and redundancy implementation
* Testing and drills (e.g., playbook, tabletop, disaster recovery exercises, scheduling)

**5.1 - Understand reasons and requirements for cryptography**

* Confidentiality
* Integrity and authenticity
* Data sensitivity (e.g., personally identifiable information (PII), intellectual property (IP), protected health information (PHI))
* Regulatory and industry best practice (e.g., Payment Card Industry Data Security Standards (PCI-DSS), International Organization for Standardization (ISO))
* Cryptography entropy (e.g., quantum cryptography, quantum key distribution)

**5.2 - Apply cryptography concepts**

* Hashing
* Salting
* Symmetric/Asymmetric encryption/Elliptic curve cryptography (ECC)
* Non-repudiation (e.g., digital signatures/certificates, Hash-based Message Authentication Code (HMAC), audit trails)
* Strength of encryption algorithms and keys (e.g., Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (RSA)
* Cryptographic attacks and cryptanalysis

**5.3 - Understand and implement secure protocols**

* Services and protocols
* Common use cases (e.g., credit card processing, file transfer, web client, virtual private network (VPN), transmission of PII data)
* Limitations and vulnerabilities

**5.4 - Understand public key infrastructure (PKI)**

* Fundamental key management concepts (e.g., storage, rotation, composition, generation, destruction, exchange, revocation, escrow)
* Web of Trust (WOT) (e.g., Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), blockchain)

**6.1 - Understand and apply fundamental concepts of networking**

* Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
* Network topologies
* Network relationships (e.g., peer-to-peer (P2P), client server)
* Transmission media types (e.g., wired, wireless)
* Software-defined networking (SDN) (e.g., Software-Defined Wide Area Network (SD-WAN), network virtualization, automation)
* Commonly used ports and protocols

**6.2 - Understand network attacks (e.g., distributed denial of service (DDoS), man-in-the-middle (MITM), Domain Name System (DNS) cache poisoning)**

* Countermeasures (e.g., content delivery networks (CDN), firewalls, network access controls, intrusion detection and prevention systems (IDPS))

**6.3 - Manage network access controls**

* Network access controls, standards and protocols (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1X, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+))
* Remote access operation and configuration (e.g., thin client, virtual private network (VPN), virtual desktop infrastructure)

**6.4 - Manage network security**

* Logical and physical placement of network devices (e.g., inline, passive, virtual)
* Segmentation (e.g., physical/logical, data/control plane, virtual local area network (VLAN), access control list (ACL), firewall zones, micro-segmentation)
* Secure device management

**6.5 - Operate and configure network-based security appliances and services**

* Firewalls and proxies (e.g., filtering methods, web application firewall (WAF), cloud access security broker (CASB))
* Network intrusion detection/prevention systems
* Routers and switches
* Traffic-shaping devices (e.g., wide area network (WAN) optimization, load balancing)
* Network Access Control (NAC)
* Data Loss Prevention (DLP)
* Unified Threat Management (UTM)

**6.6 - Secure wireless communications**

* Technologies (e.g., cellular network, Wi-Fi, Bluetooth, Near-Field Communication (NFC))
* Authentication and encryption protocols (e.g., Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP), Wi-Fi Protected Access 2 (WPA2), Wi-Fi Protected Access 3 (WPA3))

**6.7 Secure and monitor Internet of Things (IoT) (e.g., configuration, network isolation, firmware updates, End of Life (EOL) management)**

**7.1 - Identify and analyze malicious code and activity**

* Malware (e.g., rootkits, spyware, scareware, ransomware, trojans, virus, worms, trapdoors, backdoors, fileless, app/code/operatin3 system (OS)/mobile code vulnerabilities)
* Malware countermeasures (e.g., scanners, anti-malware, containment and remediation, software security)
* Types of malicious activity (e.g., insider threat, data theft, distributed denial of service (DDoS), botnet, zero-day exploits, web-based attacks, advanced persistent threat (APT))
* Malicious activity countermeasures (e.g., user awareness/training, system hardening, patching, isolation, data loss prevention (DLP))
* Social engineering methods (e.g., SPAM email, phishing/smishing/vishing, impersonation, scarcity, whaling)
* Behavior analytics (e.g., machine learning, Artificial Intelligence (AI), data analytics)

**7.2 - Implement and operate endpoint device security**

* Host-based intrusion prevention system (HIPS)
* Host-based intrusion detection system (HIDS)
* Host-based firewalls
* Application white listing
* Endpoint encryption (e.g., full disk encryption)
* Trusted Platform Module (TPM) (e.g., hardware security module management)
* Secure browsing (e.g., digital certificates)
* Endpoint detection and response (EDR)

**7.3 - Administer and manage mobile devices**

* Provisioning techniques (e.g., corporate owned, personally enabled (COPE), Bring Your Own Device (BYOD), Mobile Device Management (MDM))
* Containerization
* Encryption
* Mobile application management

**7.4 - Understand and configure cloud security**

* Deployment models (e.g., public, private, hybrid, community)
* Service models (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS))
* Virtualization (e.g., hypervisor, Virtual Private Cloud (VPC))
* Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery, shadow information technology (IT))
* Data storage, processing, and transmission (e.g., archiving, backup, recovery, resilience)
* Third-party/Outsourcing requirements (e.g., service-level agreement (SLA), data portability/ privacy/destruction/auditing)
* Shared responsibility model

**7.5 - Operate and maintain secure virtual environments**

* Hypervisor (i.e., Type 1 (e.g., bare metal), Type 2 (e.g., software))
* Virtual appliances
* Containers
* Continuity and resilience
* Storage management (e.g., data domain)
* Threats, attacks, and countermeasures (e.g., brute-force attack, virtual machine escape, threat hunting)

**Additional Examination Information**

**Supplementary References**

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at [www.isc2.org/certifications/References](https://www.isc2.org/certifications/references).

**Examination Policies and Procedures**

ISC2 recommends that SSCP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at [www.isc2.org/Register-for-Exam](https://www.isc2.org/register-for-exam).

A safe and secure cyber world

The Center for Cyber Safety & EducationISC2 CareersCommunityBlog

Frequently Asked QuestionsContact UsPolicies and Procedures

ISC2 Authorized China AgencyISC2 Japan

© Copyright 1996-2025. ISC2, Inc. All Rights Reserved.

All contents of this site constitute the property of ISC2, Inc. and may not be copied, reproduced or distributed without prior written permission. ISC2, CISSP, SSCP, CCSP, CGRC, CSSLP, HCISPP, ISSAP, ISSEP, ISSMP, CC, and CBK are registered marks of ISC2, Inc.

[Sitemap](https://www.isc2.org/sitemap.html)

[](https://community.isc2.org/)[](https://www.facebook.com/isc2fb)[](https://www.linkedin.com/company/isc2)[](https://twitter.com/ISC2)[](https://www.youtube.com/user/ISC2TV)

SSCP Exam Outline

**Agree to ISC2 policies**

Top of Form

[back to previous step](https://wsr.pearsonvue.com/testtaker/registration/PolicyAcceptancePage/ISC2?conversationId=1682517)

Bottom of Form

Top of Form

[CC: Certified in Cybersecurity (CC)](javascript:void(0);)

Bottom of Form

Top of Form

**ISC2 policies**

**Admission Policy**

Plan to arrive at your test center at least **30 minutes** before your exam start time. To check in for your appointment the following is **required**:

* Show **two (2)** valid, unexpired forms of personal ID (examples include: government issued ids, passports, etc.). Both must have your name (exactly as it appears in your exam registration) and signature, and one of the two must have your photo. For more information about acceptable IDs please visit: <https://www.isc2.org/Exams/Exam-Day> and look under What You Need to Bring to the Test Center tab for more information.
  + **Unacceptable form of ID:** **Digital IDs** (A digital ID is an electronic representation of personally identifying information that may be used to verify the identity of a person)

For additional information regarding the Aadhaar ID, please visit [Aadhaar ID Policy for Pearson VUE](https://www.pearsonvue.com/content/dam/VUE/vue/global/documents/global-id-policy/Pearson-VUE-Aadhaar-ID-Policy-English.pdf).

* Minors under 18 – Minor must be accompanied by a parent or guardian on the day of exam.
  + Please refer for ID requirements for minors, <https://www.isc2.org/exams/exam-day>
* Provide your signature.
* Submit to a [palm vein scan](https://www.isc2.org/-/media/ISC2/Documents/palm-vein_candidate-isc2.ashx?la=en&hash=A575A664E77B78B6BB2708413EFB6C7913645C08)(unless expressly prohibited by law).
* Have your photo taken. Hats, scarves, and coats may not be worn for your photo. Additionally, you may not wear these items in the test room.
* Leave your personal belongings outside the testing room. You will have access to secure storage. As storage space is limited, please plan appropriately. Pearson VUE test centers do not assume responsibility for your personal belongings.
* Receive a short orientation from the Test Administrator (TA). After the orientation, the TA will escort you to a testing station.
* Sign and agree to the [Non-Disclosure Agreement](https://www.isc2.org/Exams/Non-Disclosure-Agreement) that will be presented at the beginning of your exam. Please take a moment to review the agreement now so that you are familiar with it when you sit for your exam.

Where selected by your Test Sponsor, you agree that Pearson VUE will collect your palm vein pattern at the test center on the day of your exam and retain that information, to the extent permitted by law. Your palm vein scan will be used for the purposes of identification verification on the day of your test and on your future test days, detecting and preventing any fraud, and maintaining the security and integrity of the testing program. For more information on Pearson VUE‘s policy for use and retention of personal data including biometric data like palm vein scans, please see our [Privacy and Cookies Policy](https://wsr.pearsonvue.com/privacy). Your agreement to these Testing policies includes agreement to the Privacy and Cookies Policy.

**Reschedule Policy**

* **If you wish to reschedule** your exam appointment, you must contact [Pearson VUE](https://home.pearsonvue.com/contact).
* There is no fee for rescheduling the Certified in Cybersecurity (CC) exam. For all other certifications, there is a US$50 fee for exam appointment rescheduled.
* If you choose to **go online to reschedule** your appointment, you must do so **at least 48 hours prior to your appointment**.
* If you choose to **call the Pearson customer support team to reschedule**, you must do so **at least 24 hours prior to your appointment**.
* If you do not reschedule your exam appointment without proper advanced notice, as outlined above, it will result in a no-show, and you will **forfeit your exam fee**. If you used the ISC2 Candidate promo code, as part of the One Million Certified in Cybersecurity initiative, you will **not be able to register again with that code**.
* Once scheduled you have up to 365 days to sit for your exam. Failure to sit for your examination within 365 days will result in a no-show and forfeiture of all exam and rescheduling fees.

**Cancellation Policy**

* If you wish to cancel your exam appointment, you must contact [Pearson VUE](https://home.pearsonvue.com/contact).
* There is no fee for canceling the Certified in Cybersecurity (CC) exam. For all other certifications, there is a US$100 fee for exam appointment cancelations.
* If you choose to **go online to cancel** your appointment, you must do so **at least 48 hours prior to your appointment**.
* If you choose to **call the** [Pearson customer support team](https://home.pearsonvue.com/contact) to **cancel**, you must do so **at least 24 hours prior to your appointment**.
* If you do not cancel your exam appointment without proper advanced notice, as outlined above, it will result in a no-show, and will **forfeit your exam fee**. If you used the ISC2 Candidate promo code, as part of the One Million Certified in Cybersecurity initiative, you will **not be able to register again with that code.**

**Additional Information**

**ISC2 Terms and Conditions**

* ISC2 requires that all candidates for certification read and accept the terms and conditions set forth here: [https://www.isc2.org/uploadedFiles/Certification\_Programs/CBT-Examination-Agreement.pdf.](https://www.isc2.org/uploadedFiles/Certification_Programs/CBT-Examination-Agreement.pdf) Candidates that do not agree to the terms and conditions will not be permitted to sit for any ISC2 examination.

**Non-Disclosure Agreement (NDA)**

* Failure to read or accept the ISC2 NDA agreement within the allotted five minutes will result in exam termination and forfeiture of exam appointment. Forfeiture of exam appointment also includes forfeiture of all exam fees. To take the examination at a later date you will be required to re-register for the exam and pay all applicable registration fees.

**Important Information on ISC2 Exams**

* One of the benefits to candidates taking an examination via Computer-Based Testing is that most candidates receive their scores immediately upon completing their examination. In some cases, ISC2 must conduct periodic psychometric analyses prior to releasing exam results. For the small number of candidates affected by this process, it is expected that candidates will receive their results within 6 -8 weeks following the exam.
* ISC2 offers two types of computer-based exams – linear and adaptive – however neither exam type allows for candidates to skip an item, nor can items be returned to later during administration. Once an answer is confirmed it cannot be changed, reviewed, or revisited.
* Frequently asked questions (FAQs) and answers for common inquiries that can be found here: <https://www.isc2.org/Frequently-Asked-Questions>.

**Accommodations Policy**

ISC2 provides reasonable and appropriate accommodations for people who have a documented need for exam accommodations. Accommodations must be requested and approved by ISC2 prior to scheduling your examination. If you wish to request an accommodation, please visit <https://www.isc2.org/Register-for-Exam> and look under the Requesting Special Accommodations tab for information and instructions on how to request an accommodation. Test accommodations are individualized and considered on a case-by-case basis. Once an accommodation is approved, ISC2 will inform the Pearson VUE Accommodations team. Please allow up to three business days for Pearson VUE to receive this information. Then, contact

Top of Form

[Cart](https://wsr.pearsonvue.com/testtaker/checkout/ExternalOrderConfirmPage/ISC2?conversationId=1682707)

Bottom of Form

[Collapsed, toggle side navigation to expand](https://wsr.pearsonvue.com/testtaker/checkout/ExternalOrderConfirmPage/ISC2?conversationId=1682707)

Edit my profile  Tshingombe Tshingombe Tshitadi    
ISC2 ID: 1907033

* [Dashboard](https://wsr.pearsonvue.com/testtaker/registration/Dashboard/ISC2)
* [My Profile](https://wsr.pearsonvue.com/testtaker/common/MastHeadExternalReturnUrlRedirect/ISC2)
* [Sign out](https://wsr.pearsonvue.com/testtaker/common/SessionExpired.htm?signOut)

Top of Form

Bottom of Form

**Almost there...**

Top of Form

[back to previous step](https://wsr.pearsonvue.com/testtaker/checkout/ExternalOrderConfirmPage/ISC2?conversationId=1682707)

Bottom of Form

Top of Form

**Confirm Order Details**

| **Description** | **Details** | **Price** |
| --- | --- | --- |
| Exam  CC: Certified in Cybersecurity (CC)  Language: English  Length: 120 minutes | Appointment  Friday, March 14, 2025  Start time: 8:00 AM Africa/Johannesburg - SAST  Location  Pearson Professional Centers-Johannesburg  Pearson VUE 6th Floor Sandton City Office Tower Sandton City Shopping Centre 158 5th Street, SANDTON Johannesburg 2146 South Africa | 199.00 |

**Payment Details**

**Exams for**

Name:

Tshingombe Tshingombe Tshitadi

ISC2 ID:

1907033

**Order Total**

|  |  |
| --- | --- |
| Subtotal: | 199.00 |
| Tax: | 0.00 |
| TOTAL DUE: | USD 199.00 |
|  | USD 199.00 |

Bottom of Form

Pearson VUE, so you can schedule your exam, contact information can be found at [www.pearsonvue.com/isc2/contact](http://www.pearsonvue.com/isc2/contact).

Accommodations are not a guarantee of improved performance or exam completion. Once an initial exam appointment is scheduled, there may be a US$50 fee to reschedule an exam with an approved accommodation.

Bottom of Form

# Agree to ISC2 policies

Top of Form

[back to previous step](https://wsr.pearsonvue.com/testtaker/registration/PolicyAcceptancePage/ISC2?conversationId=1682707)

Bottom of Form

Top of Form

[CCSP: Certified Cloud Security Professional (CCSP)](javascript:void(0);)

[CGRC: Certified in Governance Risk and Compliance](javascript:void(0);)

[CISSP: Certified Information Systems Security Professional](javascript:void(0);)

[CSSLP: Certified Secure Software Lifecycle Professional](javascript:void(0);)

[ISSAP: Information Systems Security Architecture Professional](javascript:void(0);)

[ISSMP: Information Systems Security Management Professional](javascript:void(0);)

[SSCP: Systems Security Certified Practitioner](javascript:void(0);)

Certification **Exam Outline**

Effective Date: November 15, 20222

ISSMP Certification Exam Outline

**About CISSP-ISSMP**

The Information Systems Security Management Professional (ISSMP) is a CISSP who specializes in establishing,

presenting and governing information security programs and demonstrates management and leadership

skills. CISSP-ISSMPs direct the alignment of security programs with the organization’s mission, goals and

strategies in order to meet enterprise financial and operational requirements in support of its desired risk

position.

The broad spectrum of topics included in the CISSP-ISSMP Common Body of Knowledge (CBK®) ensure its

relevancy across all disciplines in the field of information security management. Successful candidates are

competent in the following six domains:

• Leadership and Business Management

• Systems Lifecycle Management

• Risk Management

• Threat Intelligence and Incident Management

• Contingency Management

• Law, Ethics and Security Compliance Management

**Experience Requirements**

Candidates must be a CISSP in good standing and have two years cumulative paid work experience

in one or more of the six domains of the CISSP-ISSMP CBK. You can learn more about CISSP-ISSMP

experience requirements and how to account for part-time work and internships at

www.isc2.org/Certifications/CISSP-Concentrations#steps-to-certification.

Accreditation

CISSP-ISSMP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the CISSP-ISSMP. Conducted at

regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that

are performed by security professionals who are engaged in the profession defined by the CISSP-ISSMP. The

results of the JTA are used to update the examination. This process ensures that candidates are tested on the

topic areas relevant to the roles and responsibilities of today’s practicing information security professionals.3

ISSMP Certification Exam Outline

**CISSP-ISSMP Examination Information**

**CISSP-ISSMP Examination Weights**

**Length of exam**

**Number of items**

**Item format**

**Passing grade**

**Exam availability**

**Testing center**

3 hours

125

Multiple choice

700 out of 1000 points

English

Pearson VUE Testing Center

**Domains**

**Weight**

1. Leadership and Business Management

20%

2. Systems Lifecycle Management

18%

3. Risk Management

19%

4. Threat Intelligence and Incident Management

17%

5. Contingency Management

15%

6. Law, Ethics and Security Compliance Management

11%

**Total: 100%**4

ISSMP Certification Exam Outline

**Domain 1:**

**Leadership and Business Management**

1.1 Establish security’s role in organizational culture, vision and mission

» Define information security program vision and mission

» Align security with organizational goals, objectives and values

» Define security’s relationship to the overall business processes

» Define the relationship between organizational culture and security

1.2 Align security program with organizational governance

» Identify and navigate organizational governance structure

» Validate roles of key stakeholders

» Validate sources and boundaries of authorization

» Advocate and obtain organizational support for security initiatives

1.3 Define and implement information security strategies

» Identify security requirements from business initiatives

» Evaluate capacity and capability to implement security strategies

» Manage implementation of security strategies

» Review and maintain security strategies

» Prescribe security architecture and engineering theories, concepts and methods

1.4 Define and maintain security policy framework Determine applicable external standards

» Determine applicable external standards

» Determine data classification and protection requirements

» Establish internal policies

» Advocate and obtain organizational support for policies

» Develop procedures, standards, guidelines and baselines

» Ensure periodic review of security policy framework5

ISSMP Certification Exam Outline

» Define roles and responsibilities

» Determine and manage team accountability

» Build cross-functional relationships

» Resolve conflicts between security and

other stakeholders

» Identify communication bottlenecks

and barriers

» Integrate security controls into human

resources processes

» Evaluate service management agreements

(e.g., risk, financial)

» Govern managed services

(e.g., infrastructure, cloud services)

» Manage impact of organizational change (e.g.,

mergers and acquisitions, outsourcing)

» Ensure that appropriate regulatory compliance

statements and requirements are included in

contractual agreements

» Monitor and enforce compliance with

contractual agreements

1.5 Manage security requirements in contracts and agreements

1.6 Manage security awareness and training programs

» Promote security programs to key stakeholders

» Identify needs and implement training programs by target segment

» Monitor and report on effectiveness of security awareness and training programs

1.7 Define, measure and report security metrics

» Identify Key Performance Indicators (KPI)

» Associate Key Performance Indicators (KPI) to the risk posture of the organization

» Use metrics to drive security program development and operations

1.8 Prepare, obtain and administer security budget

» Prepare and secure annual budget

» Adjust budget based on evolving risks and threat landscape

» Manage and report financial responsibilities

1.9 Manage security programs

1.10 Apply product development and project management principles

» Incorporate security into project lifecycle

» Identify and apply appropriate project management methodology

» Analyze project time, scope and cost relationship6

ISSMP Certification Exam Outline

2.1 Manage integration of security into Systems Development Life Cycle (SDLC)

» Integrate information security gates (decision points) and requirements into lifecycle

» Implement security controls into system lifecycle

» Oversee security configuration management (CM) processes

2.2 Integrate new business initiatives and emerging technologies into the

security architecture

» Integrate security into new business initiatives and emerging technologies

» Address impact of new business initiatives on security posture

2.3 Define and oversee comprehensive vulnerability management programs

(e.g., vulnerability scanning, penetration testing, threat analysis)

» Identify, classify and prioritize assets, systems and services based on criticality to business

» Prioritize threats and vulnerabilities

» Manage security testing

» Manage mitigation and/or remediation of vulnerabilities based on risk

2.4 Manage security aspects of change control

» Integrate security requirements with change control process

» Identify and coordinate with the stakeholders

» Manage documentation and tracking

» Ensure policy compliance (e.g., continuous monitoring)

**Domain 2:**

**Systems Lifecycle Management** 7

ISSMP Certification Exam Outline

**Domain 3:**

**Risk Management**

3.1 Develop and manage a risk management program

» Identify risk management program objectives

» Communicate and agree on risk management objectives with risk owners and other stakeholders

» Determine scope of organizational risk program

» Identify organizational security risk tolerance/appetite

» Obtain and verify organizational asset inventory

» Analyze organizational risks

» Determine countermeasures, compensating and mitigating controls

» Perform cost-benefit analysis (CBA) of risk treatment options

3.2 Conduct risk assessments

» Identify risk factors

3.3 Manage security risks within the supply chain (e.g., supplier, vendor, third-party risk)

» Identify supply chain security risk requirements

» Integrate supply chain security risks into organizational risk management

» Validate security risk control within the supply chain

» Monitor and review the supply chain security risks8

ISSMP Certification Exam Outline

4.1 Establish and maintain threat intelligence program

» Aggregate threat data from multiple threat intelligence sources

» Conduct baseline analysis of network traffic, data and user behavior

» Detect and analyze anomalous behavior patterns for potential concerns

» Conduct threat modeling

» Identify and categorize an attack

» Correlate related security event and threat data

» Create actionable alerting to appropriate resources

4.2 Establish and maintain incident handling and investigation program

» Develop program documentation

» Establish incident response case management process

» Establish incident response team

» Apply incident management methodologies

» Establish and maintain incident handling process

» Establish and maintain investigation process

» Quantify and report financial and operational impact of incidents and investigations to stakeholders

» Conduct root cause analysis (RCA)

**Domain 4:**

**Threat Intelligence and Incident**

**Management** 9

ISSMP Certification Exam Outline

5.1 Facilitate development of contingency plans

» Identify and analyze factors related to the Continuity of Operations Plan (COOP)

» Identify and analyze factors related to the business continuity plan (BCP) (e.g., time, resources, verification)

» Identify and analyze factors related to the disaster recovery plan (DRP) (e.g., time, resources, verification)

» Coordinate contingency management plans with key stakeholders

» Define internal and external crisis communications plans

» Define and communicate contingency roles and responsibilities

» Identify and analyze contingency impact on business processes and priorities

» Manage third-party contingency dependencies

» Prepare security management succession plan

5.2 Develop recovery strategies

» Identify and analyze alternatives

» Recommend and coordinate recovery strategies

» Assign recovery roles and responsibilities

5.3 Maintain contingency plan, Continuity of Operations Plan (COOP), business continuity

plan (BCP) and disaster recovery plan (DRP)

» Plan testing, evaluation and modification

» Determine survivability and resiliency capabilities

» Manage plan update process

5.4 Manage disaster response and recovery process

» Declare disaster

» Implement plan

» Restore normal operations

» Gather lessons learned

» Update plan based on lessons learned

**Domain 5:**

**Contingency Management** 10

ISSMP Certification Exam Outline

10

6.1 Identify the impact of laws and regulations that relate to information security

6.2 Adhere to the (ISC)

2

Code of Ethics as related to management issues

6.3 Validate compliance in accordance with applicable laws, regulations and industry

best practices

6.4 Coordinate with auditors and regulators in support of the internal and external

audit processes

6.5 Document and manage compliance exceptions

» Identify and document compensating controls and workarounds

» Report and obtain authorized approval of risk waiver

**Domain 6:**

**Law, Ethics and Security Compliance**

**Management**

» Identify applicable privacy laws

» Identify legal jurisdictions the organization and

users operate within (e.g., trans-border data flow)

» Identify export laws

» Identify intellectual property (IP) laws

» Identify applicable industry regulations

» Identify and advise on non-compliance risks

» Inform and advise senior management

» Evaluate and select compliance framework(s)

» Implement the compliance framework(s)

» Define and monitor compliance metrics

» Plan

» Schedule

» Coordinate audit activities

» Evaluate and validate findings

» Formulate response

» Validate implemented mitigation and

remediation actions11

ISSMP Certification Exam Outline

**Additional Examination Information**

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing

relevant resources that pertain to the CBK and identifying areas of study that may need

additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)2 recommends that CISSP-ISSMP candidates review exam policies and procedures

prior to registering for the examination. Read the comprehensive breakdown of this

important information at www.isc2.org/Exams/Before-Your-Exam.

Legal Info

For any questions related to (ISC)

2

’s legal policies, please contact the (ISC)2 Legal

Department at legal@isc2.org.

Any Questions?

(ISC)2 Americas

Tel: +1.866.331.ISC2 (4722)

Email: info@isc2.org

(ISC)2 Asia-Pacific

Tel: +(852) 28506951

Email: isc2asia@isc2.org

(ISC)2 EMEA

Tel: +44 (0)203 300 1625

Email: info-emea@isc2.org

11

v222Certification **Exam Outline**

Effective Date: November 13, 20202

ISSEP Certification Exam Outline

**About CISSP-ISSEP**

The Information Systems Security Engineering Professional (ISSEP) is a CISSP who specializes in the practical

application of systems engineering principles and processes to develop secure systems. An ISSEP analyzes

organizational needs, defines security requirements, designs security architectures, develops secure designs,

implements system security, and supports system security assessment and authorization for government and

industry.

The broad spectrum of topics included in the ISSEP Common Body of Knowledge (CBK®) ensure its relevancy

across all disciplines in the field of security engineering. Successful candidates are competent in the following

five domains:

• Systems Security Engineering Foundations

• Risk Management

• Security Planning and Design

• Systems Implementation, Verification and Validation

• Secure Operations, Change Management and Disposal

**Experience Requirements**

Candidates must be a CISSP in good standing and have two years cumulative paid work experience

in one or more of the five domains of the CISSP-ISSEP CBK. You can learn more about CISSP-ISSEP

experience requirements and how to account for part-time work and internships at

www.isc2.org/Certifications/CISSP-ISSEP/experience-requirements.

Accreditation

CISSP-ISSEP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the ISSEP. Conducted at regular

intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are

performed by security professionals who are engaged in the profession defined by the ISSEP. The results of

the JTA are used to update the examination. This process ensures that candidates are tested on the topic

areas relevant to the roles and responsibilities of today’s practicing information security professionals.3

ISSEP Certification Exam Outline

**CISSP-ISSEP Examination Information**

**CISSP-ISSEP Examination Weights**

**Length of exam**

**Number of items**

**Item format**

**Passing grade**

**Exam availability**

**Testing center**

3 hours

125

Multiple choice

700 out of 1000 points

English

Pearson VUE Testing Center

**Domains**

**Weight**

1. Systems Security Engineering Foundations

25%

2. Risk Management

14%

3. Security Planning and Design

30%

4. Systems Implementation, Verification and Validation

14%

5. Secure Operations, Change Management

and Disposal

17%

**Total: 100%**4

ISSEP Certification Exam Outline

**Domain 1:**

**Systems Security Engineering Foundations**

1.1 Apply systems security engineering fundamentals

1.2 Execute systems security engineering processes

1.3 Integrate with applicable system development methodology

1.4 Perform technical management

1.5 Participate in the acquisition process

1.6 Design Trusted Systems and Networks (TSN)

» Understand systems security engineering trust

concepts and hierarchies

» Identify the relationships between systems and

security engineering processes

» Apply structural security design principles

» Integrate security tasks and activities

» Verify security requirements throughout

the process

» Integrate software assurance methods

» Perform project planning processes

» Perform project assessment and control

processes

» Perform decision management processes

» Perform risk management processes

» Perform configuration management processes

» Perform information management processes

» Perform measurement processes

» Perform Quality Assurance (QA) processes

» Identify opportunities for security process

automation

» Identify organizational security authority

» Identify system security policy elements

» Integrate design concepts

(e.g., open, proprietary, modular)

» Prepare security requirements for acquisitions

» Participate in selection process

» Participate in Supply Chain Risk Management

(SCRM)

» Participate in the development and review of

contractual documentation5

ISSEP Certification Exam Outline

**Domain 2:**

**Risk Management**

2.1 Apply security risk management principles

2.2 Address risk to system

2.3 Manage risk to operations

» Establish risk context

» Identify system security risks

» Perform risk analysis

» Perform risk evaluation

» Recommend risk treatment options

» Document risk findings and decisions

» Determine stakeholder risk tolerance

» Identify remediation needs and other system changes

» Determine risk treatment options

» Assess proposed risk treatment options

» Recommend risk treatment options

» Align security risk management with Enterprise Risk Management (ERM)

» Integrate risk management throughout the lifecycle6

ISSEP Certification Exam Outline

3.1 Analyze organizational and operational environment

3.2 Apply system security principles

3.3 Develop system requirements

3.4 Create system security architecture and design

**Domain 3:**

**Security Planning and Design**

» Capture stakeholder requirements

» Identify relevant constraints and assumptions

» Assess and document threats

» Determine system protection needs

» Develop Security Test Plans (STP)

» Incorporate resiliency methods to address threats

» Apply defense-in-depth concepts

» Identify fail-safe defaults

» Reduce Single Points of Failure (SPOF)

» Incorporate least privilege concept

» Understand economy of mechanism

» Understand Separation of Duties (SoD) concept

» Develop system security context

» Identify functions within the system and security

Concept of Operations (CONOPS)

» Document system security requirements baseline

» Analyze system security requirements

» Develop functional analysis and allocation

» Maintain traceability between specified design

and system requirements

» Develop system security design components

» Perform trade-off studies

» Assess protection effectiveness7

ISSEP Certification Exam Outline

**Domain 4:**

**Systems Implementation, Verification**

**and Validation**

4.1 Implement, integrate and deploy security solutions

4.2 Verify and validate security solutions

» Perform system security implementation and integration

» Perform system security deployment activities

» Perform system security verification

» Perform security validation to demonstrate security controls meet stakeholder security requirements8

ISSEP Certification Exam Outline

**Domain 5:**

**Secure Operations, Change Management**

**and Disposal**

5.1 Develop secure operations strategy

5.2 Participate in secure operations

5.3 Participate in change management

5.4 Participate in the disposal process

» Specify requirements for personnel conducting operations

» Contribute to the continuous communication with stakeholders for security relevant aspects of the system

» Develop continuous monitoring solutions and processes

» Support the Incident Response (IR) process

» Develop secure maintenance strategy

» Participate in change reviews

» Determine change impact

» Perform verification and validation of changes

» Update risk assessment documentation

» Identify disposal security requirements

» Develop secure disposal strategy

» Develop decommissioning and disposal procedures

» Audit results of the decommissioning and disposal process9

ISSEP Certification Exam Outline

**Additional Examination Information**

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing

relevant resources that pertain to the CBK and identifying areas of study that may need

additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)² recommends that ISSEP candidates review exam policies and procedures prior to

registering for the examination. Read the comprehensive breakdown of this important

information at www.isc2.org/Register-for-Exam.

Legal Info

For any questions related to (ISC)²’s legal policies, please contact the (ISC)2 Legal

Department at legal@isc2.org.

Any Questions?

(ISC)² Americas

Tel: +1-866-331-ISC2(4722)

Email: membersupport@isc2.org

(ISC)² Asia Pacific

Tel: +852-2850-6951

Email: membersupportapac@isc2.org

(ISC)² EMEA

Tel: +44-203-960-7800

Email: membersupportemea@isc2.org

9

7/2020

Attachments

Rate this

Details

### Lenovo and Intel are Driving AI Innovation at the Edge

Flynn Maloy, Chief Marketing Officer of Lenovo ISG

Jan 23 2025| 0 mins

Lenovo and Intel’s long-standing partnership is transforming industries by bringing cutting-edge AI solutions to the edge and beyond. From PCs to data centers, our collaboration has consistently pushed technological boundaries. The strength of Lenovo’s ThinkEdge portfolio is enabling AI-driven applications in manufacturing sites, retail stores, schools, and more. Join @Flynn Maloy, Chief Marketing Officer of Lenovo ISG, as he details how Lenovo and Intel® are leading the way in AI innovation: - Comprehensive solutions for diverse industries: From computer vision in manufacturing to advanced AI in education and retail, Lenovo and Intel’s joint solutions empower a variety of applications. - Next-gen AI with CPUs: Not every AI workload requires massive GPUs. Intel’s CPUs are driving the next wave of edge AI, particularly in inferencing and delivering efficient and accessible AI solutions. - Scalable and powerful edge portfolio: Lenovo’s edge clients and servers, powered by Intel, are designed to meet the demands of modern businesses, offering flexibility and performance across workloads. - A partnership that drives innovation: With a shared vision for the future of AI, Lenovo and Intel continue to push the boundaries of what’s possible for our customers. Together, Lenovo and Intel are leading the charge in making AI more accessible, scalable, and impactful for businesses worldwide.

### State of Cloud 2025: Navigating EMEA’s Cloud Revolution

John Bradshaw, Director of Cloud Computing Technology and Strategy, EMEA, Akamai & Bryan Glick, Editor in Chief, Computer Weekly

Feb 27 2025| 18 mins

Boris Cipot, Senior Security Engineer

Sep 05 2024| 30 mins

### Python is a fast, platform-agnostic, and easy-to-learn programming language that is suited for beginners and experienced developers alike. Ever since its first release in 1991, Python has had a constant presence in the computer world and has become a go-to language thanks to its easy-to-understand code and versatility. Today, Python can boast a wide array of libraries and frameworks, and they are the cornerstone of fast and easy Python programming—the so-called Pythonic way of development. But like all programming languages, Python is not immune to security threats. Secure coding best practices must be adopted to avoid risks from attackers. In this webinar, we’ll explore Python security best practices that should employed when building secure application. One-Stop DevOps: Simplifying Toolchains with GitLab and Google Cloud

Nate Avery, Outbound Product Manager - Google | Jackie Porter, Director of Product - Gitlab | Torsten Volk, Principal Analyst - ESG

Dec 04 2024| 28 mins

Enterprise Strategy Group (ESG) data shows that 65% of developers’ time is consumed by overhead tasks related to context switching, pipeline integration, compliance, monitoring and logging, managing secrets, and so on. This avalanche of tasks—not to mention the dozen or more tools involved to execute them—slows down productivity, increases the risk of security vulnerabilities, and complicates automated deployment in the DevSecOps pipeline. In this webinar, ESG Principal Analyst Torsten Volk joins Nate Avery, Google’s Outbound Product Manager, and Jackie Porter, GitLab’s Product Marketing Director, to explain how to deliver code faster, enhance developer productivity, and improve security across the DevOps tool chain and into the cloud. Save your seat to discover how to resolve pressing DevSecOps pain points like tool sprawl, and how GitLab and Google’s integration greatly assists with this process, reducing manual developer tasks and unifying security automation.Watch our on-demand panel discussion with Bryan Glick, Editor in Chief at Computer Weekly, as we explore the key trends shaping cloud innovation in 2025. Discover how AI integration, edge-native applications, and distributed cloud are transforming strategies across EMEA. Gain actionable insights on application modernisation, cost optimisation, and real-world success stories to help your organisation thrive. Key Takeaways: - How regional challenges are driving cloud adoption - Distributed cloud’s role in AI and performance optimisation - Strategies for modernising applications and cutting costs Watch now on-demand! Bottom of Form