TIA QuEST Forum

SECURITY RESOURCES GUIDE

Release Version 2.0

Contents

Purpose:

This document is intended to identify resources which may be useful to an organization in its pursuit of Product and/or organizational security. This list is informational only, is not definitive, and is not a recommendation or endorsement of any kind. TIA QuEST Forum disclaims any warranties, implied or expressed, relating to the nature of the products and services provided by these resources, including, but not limited to, their quality, appropriateness, adequacy, usefulness, merchantability, fitness for use, legal sufficiency, or otherwise. Use of the resources provided is at your own risk. You should investigate the resource to determine its adequacy and applicability, and compare it with others which may be available to you. TIA QuEST Forum disclaims all liability for damages or costs of any kind which may arise from contacting the resources, or using any of the products or services of the resources listed. Inclusion in the Resource Guide is open to both member and non-member organizations. If you would like to have your organization or product included, please email a request to: information@questforum.org

Acknowledgements:

Executive Board

Chief Executive Officer	Fraser Pajak ,	QuEST Forum

IGQ Work Group

Co-Chair	Sheronda Jeffries	Cisco Systems
Co-Chair	William (Bill) Jibby	ARRIS Group, Inc.
Co-Secretary	Nancy Patterson	Alcatel-Lucent
Co-Secretary	Jason Becker	Verizon Communications Inc.

Contributing Author

Co-Chair	Sheronda Jeffries	Cisco Systems
IGQ-Member	Charanjot Singh Gill	DeMog Technologies LLC

1. Standards and Codes of Practice

a) ISO/IEC 27000 family - Information Security Management Systems

The ISO/IEC 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. Information Security Management Systems is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process.

ISO/IEC 27000 Information Security Management System (ISMS) family of standards from ISO

b) National Institute of Standards and Technology

National Institute of Standards and Technology (NIST) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues.

National Institute of Standards and Technology (NIST)
National Cybersecurity Center of Excellence (NCCOE)

c) Control Objectives for Information and Related Technologies (COBIT)

COBIT framework defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model. COBIT also provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business. It is the product of a global task force and development team from ISACA, a nonprofit, independent association of more than 140,000 governance, security, risk and assurance professionals in 187 countries.

COBIT 5

d) Common Criteria

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. The CC is the driving force for the widest available mutual recognition of secure IT products.

Common Criteria

2. Industry Bodies

a) TIA Cybersecurity Working Group

The TIA Cybersecurity Working Group advocates public policy positions related to the security of ICT equipment and services from a vendor perspective as it relates to critical infrastructure, supply chain and information sharing. The mission of the Cybersecurity Working Group is to promote consensus-based positions to the Congress, the Administration, Federal Agencies, and any other relevant governmental bodies.

TIA Cybersecurity Working Group

b) 3rd Generation Partnership Project (3GPP) – SA WG3

The 3rd Generation Partnership Project (3GPP) unites telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) & provides their members with a stable environment to produce Reports & Specifications that define 3GPP technologies.

Services & Systems Aspects Work Group 3 (SA WG3) has the overall responsibility for security and privacy in 3GPP systems. The WG performs analysis of potential threats to these systems. Based on the threat analysis, the WG determines the security and privacy requirements for 3GPP systems, and specifies the security architectures and protocols.

3GPP (TSG SA WG3 Security)

c) American National Standards Institute's Homeland Defense and Security Standardization Collaborative

The American National Standards Institute's Homeland Defense and Security Standardization Collaborative (HDSSC) has as its mission to identify existing consensus standards, or, if none exist, assist government agencies and those sectors requesting assistance to accelerate development and adoption of consensus standards critical to homeland security and homeland defense.

ANSI Homeland Defense and Security Standardization Collaborative (HDSSC)

d) ETIS - Information Security Working Group

ETIS is a membership based organization bringing together the major telecommunications providers in Europe to share knowledge in a trusted environment. The Information Security Working Group serves as a platform for sharing experiences on the development of Information Security touching on strategies, governance and cyber threats in Telecommunications.

ETIS Information Security Working Group

e) Cloud Security Alliance

Cloud Security Alliance (CSA) is dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA's comprehensive research program works in collaboration with industry, higher education and government on a global basis. CSA offers cloud security-specific research, education, certification, events and products. CSA also operates cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, 3rd party audit and continuous monitoring.

Cloud Security Alliance

3. Government Agencies and Resources

a) Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from various government agencies and private industry.

The Federal Risk and Authorization Management Program (FedRAMP)

b) United States Computer Emergency Readiness Team (US-CERT)

US-CERT strives for a providing safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world. It provides cybersecurity protection to Federal civilian executive branch agencies. It develops timely and actionable information for distribution to various federal, state and local government agencies. US-CERT also responds to incidents and analyzing data about emerging cyber threats.

United States Computer Emergency Readiness Team (US-CERT)

c) United States Department of Homeland Security (US-DHS)

Department of Homeland Security's mission is to ensure US homeland is safe, secure, and resilient against terrorism and other hazards. The Department is the lead for the federal government for securing civilian government computer systems, and works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems.

Department of Homeland Security (DHS)
National Infrastructure Protection Plan (NIPP)

4. Professional and Other Organizations

a) CERT

Division of the Software Engineering Institute (SEI) that is involved in studying and solving problems with widespread cybersecurity implications, research security vulnerabilities in software products. They contribute to long-term changes in networked systems and develop cutting-edge information and training to help improve cybersecurity. CERT develops tools, products, and methods to help organizations conduct forensic examinations, analyze vulnerabilities, and monitor large-scale networks. They also help organizations determine how effective their security-related practices are. CERT collaborates with high-level government organizations, such as the U.S. Department of Defense and the Department of Homeland Security (DHS); law enforcement, including the FBI; the intelligence community; and many industry organizations.

CERT – Software Engineering Institute, Carnegie Mellon

b) ASIS International

ASIS International is an organization for security professionals worldwide. ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the Global Security Exchange, as well as specific security topics. ASIS international provides its members and the security community with access to a full range of programs and services. It also publishes magazine 'Security Management'.

ASIS International

c) ISACA

ISACA is an independent, nonprofit, global association that engages in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit, and assurance professionals worldwide. ISACA also provides training and certification program for IT professionals (details in section 5 below).

ISACA

d) International Information System Security Certification Consortium

$(ISC)^2$ is world's Leading Cybersecurity and IT Security Professional organization. $(ISC)^2$ is a nonprofit membership association for information security leaders. It is committed to helping

its members learn, grow and thrive. Consortium is more than 125,000 certified members strong. Organization also specializes in training and certifications for cybersecurity professionals (details in section 5 below)

(ISC)²

e) SANS Institute

SANS is a trusted source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system. SANS also provides training designed to help IT Security professionals master the practical steps necessary for defending systems and networks against the most dangerous threats.

The SANS Institute

f) Center for Internet Security (CIS)

Center for Internet Security is a non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals.

Center for Internet Security

g) Common Vulnerabilities and Exposures (CVE®)

Common Vulnerabilities and Exposures (CVE®) maintains a list of common identifiers for publicly known cybersecurity vulnerabilities. CVE is now the industry standard for vulnerability and exposure identifiers. CVE Entries are used to discuss or share information about unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

Common Vulnerabilities and Exposures

5. Individual Certifications

a) Global Information Assurance Certifications (GAIC)

GIAC is an information security certification entity that specializes in technical and practical certification of IT professionals. GIAC mission is to provide assurance that a certified individual has the knowledge and skills necessary for a practitioner in key areas of computer, information and software security. GIAC certifications are trusted by thousands of companies and government agencies, including the United States National Security Agency (NSA).

GIAC provides over 30 different certifications in various domains like Cyber-Defense, Penetration Testing, Developer, Security Administration, Digital Forensics and Incident Response. Additional information can be found on GIAC website.

GIAC Certifications

b) (ISC)² Certifications

(ISC)² specializes in training and certifications for cybersecurity professionals. Listed below is a high-level overview of some certification offered by the organization. Additional information can be found on (ISC)² website.

- Certified Information Systems Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)
- Certified Cloud Security Professional (CCSP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Lifecycle Professional (CSSLP)

c) ISACA Certifications

ISACA certifications are globally accepted and recognized. They combine the achievement of passing an exam with credit for work and educational experience. Additional information can be found on ISACA website under certification section. ISACA offers the following certifications:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified in Risk and Information Systems Control (CRISC)
- Cybersecurity Nexus – CSX Practitioner Certification (CSX-P)

6. Newsletters, Alerts, Blogs, and Collaboration Sites

a) Industrial Control Systems Cyber Emergency Response Team

An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

ICS-CERT Newsletters and Alerts

b) Carnegie Mellon University Vulnerability Notes Database

The Vulnerability Notes Database provides information about software vulnerabilities. Vulnerability Notes include summaries, technical details, remediation information, and lists of affected vendors.

Carnegie Mellon CERT Knowledgebase

c) SANS Computer Security NewsBites

SANS NewsBites is a semiweekly high-level executive summary of the most important news articles that have been published on computer security during the last week. Each news item is very briefly summarized and includes a reference on the web for detailed information.

SANS Computer Security News/Newsletters

d) Vendor Specific Security Center websites

- Microsoft Security Tech Center
- Oracle Security
- Cisco Security Center