Cybersecurity Metrics

CC-01 [Essential] Outline via appropriate methods, and using industry-standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

CC-02 [Essential] Assess and respond appropriately to various risks which can affect the expected operation of information systems. [Evaluating]

Emerging Standard
Developed Standard
Highly Developed Standard

CC-03 [Essential] Investigate current and emerging cyberthreats and incorporate best practices to mitigate them. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

CC-04 [Essential] Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

CC-05 [Essential] Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem. [Understanding]
DAT-E01 [Essential] Implement data security by selecting appropriate cryptographic procedures, algorithms, and tools based on security policy and level of risk in an organization. [Applying]

DAT-E02 [Essential] Discuss forensically sound collection and acquisition of digital evidence. [Understanding]

DAT-E03 [Essential] Apply principles, processes, tools and techniques used in mitigating security threats and responding to security incidents. [Applying]

DAT-E04 [Essential] Use appropriate levels of authentication, authorization, and access control to ensure data integrity and security for information systems and networks. [Applying]

DAT-E05 [Essential] Infer gaps in data security considering current and emerging technologies and the current state and prevailing trends in cybercrime. [Understanding]

DAT-S01 [Supplemental] Perform a forensic analysis on a local network, on stored data within a system as well as mobile devices for an enterprise environment. [Applying]
DAT-S02 [Supplemental] Outline complex technical concepts to technical and non-technical audiences as they relate to data security. [Analyzing]

SOF-E01 [Essential] Write secure code with appropriate documentation for a software system and its related data. [Applying]

SOF-E02 [Essential] Analyze security and ethical considerations at each phase of the software development lifecycle. [Analyzing]

SOF-E03 [Essential] Use documentation, such as third-party library documentation, in a given secure computing scenario. [Applying]

SOF-S01 [Supplemental] Implement isolation to secure a process or application. [Applying]

SOF-S02 [Supplemental] Discuss the relationship between an organization’s mission and secure software design. [Understanding]
SOF-S03 [Supplemental] Write software specifications, including security specifications, for a given process or application. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

SOF-S04 [Supplemental] Assess a given test plan, from a security perspective. Evaluating [Evaluating]

Emerging Standard
Developed Standard
Highly Developed Standard

SOF-S05 [Supplemental] Examine social and legal aspects of software development from a security perspective. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

SOF-S06 [Supplemental] Develop user documentation for software installation with security appropriately included. [Creating]

Emerging Standard
Developed Standard
Highly Developed Standard

COM-E01 [Essential] Discuss vulnerabilities and mitigations of system components throughout their lifecycle. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

COM-E02 [Essential] Perform security testing for given components within a system. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard
COM-S01 [Supplemental] Analyze how component security features impact systems, such as software and firmware updates. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

CON-E01 [Essential] Illustrate the construction and proper configuration of computer networks which adhere to current industry standards and organizational guidelines. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

CON-E02 [Essential] Investigate the impact of various connection and transmission attacks on network hardware and software. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

CON-S01 [Supplemental] Examine characteristics of commonly used physical networking media and interfaces. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

CON-S02 [Supplemental] Distinguish vulnerabilities and example exploits as they apply to network services, architectures, and protocols. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

CON-S03 [Supplemental] Implement appropriate defenses throughout an enterprise to harden the network against attackers. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard
### CON-S04 [Supplemental] Construct and properly configure computer networks which adhere to current industry standards and organizational guidelines. [Creating]

Emerging Standard  
Developed Standard  
Highly Developed Standard

### SYS-E01 [Essential] Discuss security aspects of system management in common system architectures. [Understanding]

Emerging Standard  
Developed Standard  
Highly Developed Standard

### SYS-E02 [Essential] Contrast various methods for authentication and access control in an enterprise, and why one might choose one over another. [Analyzing]

Emerging Standard  
Developed Standard  
Highly Developed Standard

### SYS-E03 [Essential] Perform system security testing with an understanding of normal, secure operation, and document results. [Applying]

Emerging Standard  
Developed Standard  
Highly Developed Standard

### SYS-S01 [Supplemental] Critique security throughout the system lifecycle, including security requirements, system management, system testing, and system disposal. Evaluating [Evaluating]

Emerging Standard  
Developed Standard  
Highly Developed Standard

### SYS-S02 [Supplemental] Outline a security threat model and how system monitoring tools and mechanisms can be used. [Analyzing]

Emerging Standard  
Developed Standard  
Highly Developed Standard
SYS-S03 [Supplemental] Examine appropriate models for managing authentication, access control and authorization across systems in an organization. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

SYS-S04 [Supplemental] Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

SYS-S05 [Supplemental] Discuss legal aspects of system and network requirements, such as support for litigation holds and forensic analysis. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

SYS-S06 [Supplemental] Construct virtual environments including disk and memory structures to meet organization needs. [Creating]

Emerging Standard
Developed Standard
Highly Developed Standard

HUM-E01 [Essential] Discuss identity management in the context of attacks and mitigations. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

HUM-E02 [Essential] Analyze the security of an individual’s data and privacy in the context of an organization and in their personal lives. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard
HUM-E03 [Essential] Describe trends in human behavior which pose risks to individual and organizational privacy and security. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

HUM-S01 [Supplemental] Analyze a variety of physical access controls. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

HUM-S02 [Supplemental] Use a variety of tools and techniques to detect and mitigate social engineering threats. [Applying]

Emerging Standard
Developed Standard
Highly Developed Standard

HUM-S03 [Supplemental] Examine techniques to encourage personal compliance with cybersecurity rules, policies, and ethical norms. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

ORG-E01 [Essential] Describe policies, procedures, and ethical considerations to protect information security. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

ORG-E02 [Essential] Describe security features in operating system and database administration in a local or cloud environment. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard
ORG-E03 [Essential] Summarize the components of a business continuity plan that ensures minimal downtime and quick recovery in the face of cybersecurity incidents or natural disasters. [Understanding]
Emerging Standard
Developed Standard
Highly Developed Standard

ORG-E04 [Essential] Describe physical security features to protect an organization’s computing and information resources. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

ORG-S01 [Supplemental] Analyze risks to information assets in an organization and communicate them to stakeholders. [Analyzing]
Emerging Standard
Developed Standard
Highly Developed Standard

ORG-S02 [Supplemental] Assess administrative procedures for protecting systems from attack and ensuring the availability of system access and functions in an organization. Evaluating [Evaluating]
Emerging Standard
Developed Standard
Highly Developed Standard

ORG-S03 [Supplemental] Analyze the meaning and use of various security metrics and data with the aid of tools, to ensure quality control and security of data. [Analyzing]
Emerging Standard
Developed Standard
Highly Developed Standard

ORG-S04 [Supplemental] Discuss issues related to personnel security in an organization, including the protection of personally identifiable information, and proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool. [Understanding]
Emerging Standard
Developed Standard
Highly Developed Standard
SOC-E01 [Essential] Interpret applicable cyber policies and ethics for a given scenario. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

SOC-E02 [Essential] Summarize applicable national, international, and global security policies and legislation. [Understanding]

Emerging Standard
Developed Standard
Highly Developed Standard

SOC-E03 [Essential] Distinguish social dynamics of computer attackers in a global context. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

SOC-S01 [Supplemental] Attribute specific cyber laws and potential economic impact for a given cybercrime scenario. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

SOC-S02 [Supplemental] Compare different cyber ethics theories that impact on individuals and society. [Analyzing]

Emerging Standard
Developed Standard
Highly Developed Standard

Association for Computing Machinery

- Login
- Acceptable Use
- Privacy Policy

Copyright © 2020 ACM CCECC