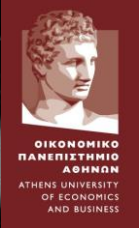


Cybersecurity self-assessment tools: A review



Georgia Lykou

**Air Traffic Safety Electronics Engineer, HCAA
February 2022**



This presentation was partially supported by a Research Project funded by the **Ministry of Digital Governance and Athens University of Economics & Business**, 2021.

Cybersecurity self-assessment tools: A review

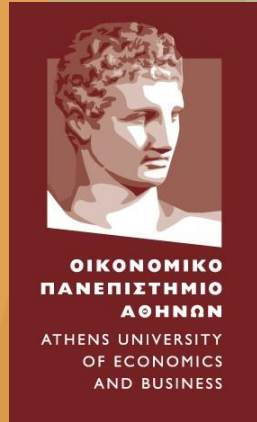


9th
Information Security
Conference

Georgia Lykou, B.Sc., M.Sc., MBA, Ph.D.
Air Traffic Safety Electronics Engineer, HCAA
&
Athens University of Economics & Business, Greece

Why self-assessment tools?

- ❖ Self-assessment tools can support organizations to:
 - ▶ build up on knowledge and security awareness,
 - ▶ check implemented cybersecurity practices and responsibilities,
 - ▶ identify security weaknesses,
 - ▶ evaluate the status of security for a system,
 - ▶ establish cybersecurity targets,
 - ▶ improve resilience,
 - ▶ manage organizational risk.



Information and Decision Flows

Risk Management



Implementation



ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

Overview of Self-Assessment Tools

1) CS²SAT

2) CSET

3) SSAT

4) CRR



ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

CS2SAT - CS2SAT

File Diagram Edit Help

Assessment Info SAL Questions Admin Questions Component Diagram Component Questions Assessment Report Document Library

Admin Questions

- Administrative
 - Applied Standards
 - 1. Standards Selection
- NERC
 - Critical Cyber Assets
 - Security Management
 - Personnel and Training
 - Electronic Security Perimeter
 - Physical Security
 - Systems Security Management
 - Incident Reporting & Response
 - Recovery Plans
- NIST SP800-53 Rev.0
 - Access Control
 - Awareness and Training
 - Audit and Accountability
 - Certification-Accreditation
 - Configuration Management
 - Contingency Planning
 - Identification-Authentication
 - Incident Response
 - Maintenance
 - Media Protection
 - Physical & Environ. Protection
 - Planning
 - Personnel Security
 - Risk Assessment

Administrative Applied Standards

Applied Standards

1. Branching Question - Select the Standards to be included in this assessment.

- NERC CIP-002 through CIP-009
- NIST SP800-53 Rev.0
- ISO/IEC 15408 (Common Criteria) v3.1
- DoDI 8500.2

CSET

CYBER SECURITY EVALUATION TOOL

CISA
CYBER-INFRASTRUCTURE

CS2SAT - CS2SAT

File Diagram Edit Help

Assessment Info SAL Questions Admin Questions Component Diagram Component Questions Assessment Report Document Library

Component Questions

- Control Net
 - Web Server
 - Default
 - Audit
 - 1. Does the Web Server alert security personnel to potential security violations? Check all that apply.

Control Net Web Server Default Audit

Audit

1. Does the Web Server alert security personnel to potential security violations? Check all that apply.

- Security personnel are alerted via priority messaging such as email and/or paging.
- In addition, the alerts are part of an integrated event monitoring system.
- No alarms/alerts are incorporated into system.
- Not Applicable.

2. Which of the following events are recorded in the web

- Web server startup and shutdown.
- Fault conditions.
- Login activities.
- Connection information including web sites accessed and user identities.
- Unsuccessful use of authentication mechanisms.

U.S. DEPARTMENT OF
HOMELAND SECURITY

CYBER SECURITY EVALUATION TOOL

CSET

VERSION 4.0

What would you like to do?

- Create a new assessment
- Open the last assessment:
- Open an existing assessment
- Open a recovery file
- View the user guide
- View the tutorials
- Exit the CSET application

Component question.

SCADA SAT (SSAT) - UK

Sandra C Security Advisor Energy
Dan B Security Advisor Water



Overview of Self-Assessment Tools

Tool description	CS ² SAT	CSET	SSAT	CRR
Type	Desktop software application tool	Desktop software application tool	Questionnaire XLS assisted Tool	Questionnaire PDF assisted Tool
Developer	Department of Energy National Laboratories	ICS-CERT / DHS	CPNI	US-CERT / DHS Carnegie Mellon University
Origin	USA	USA	UK	USA
Description	Self-contained tool step-by-step process	Self-contained tool step-by-step process	SSAT Questionnaire which links directly to the CPNI SCADA security good practice.	Self-contained tool
Step Process	6	5	1	1
Survey Method	Structured Questionnaire	Structured Questionnaire	Structured Questionnaire	Structured Questionnaire
Security Expertise Needed	YES	NO	YES	NO
Standards Compliance	NERC CIP, NIST SSP-CIPCS, NIST SSP-ICS, NIST SP 800-53, DoD 8500.2 ISO/IEC 15408	DHS Cat. of CS NERC CIP 002-009 NIST SP 800-82 NIST SP 800-53 NRC Reg. Guide 5.7 CNSSI 1253 INGAA Control Security Guidelines NISTIR 7628 Guide	CPNI Good Practices NIST SPP-CIPCS NIST SPP-ICS ISO/IEC 15408 NERC CIP 002-009 NIST SP 800-53 DoD IA	NIST SP 800-18 NIST SP 800-30 NERC CIP FISCAM Clinger-Cohen law GISRA law FIPS 102 OMB Circul. A-130
Checks ICS Compliance with Security Standard	YES	YES	NO	NO
Database of industry available cyber-security practices	YES	YES	NO	NO
Sector average score	NO	YES	YES	NO
Recommendation List	YES	YES	YES	YES
Type of Result	Full Performance Evaluation	Full Performance Evaluation & Compliance of Selected Std	Scoring Result	Full Performance Evaluation

NIST Cyber-Security Framework

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

4 RESPOND

Develop a plan for disasters and information security incidents

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity



3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees



ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

Questionnaire Content Analysis

NIST Security Self-Assessment Questionnaire

- ▶ Assesses the status of security controls in IT systems.
- ▶ Questions are separated into three major control areas.

Topic Areas of Questions

Management Controls

Policies & Plans
Organizational Risk
Management and
Assessment
Information and
Document Management
Business Continuity
Plan



Operational Controls

Physical Security
Environmental Security
System Protection
Procedures
Maintenance
Account Management
System and Services
Acquisition
Personnel Training
Incident Response



Technical Controls

Audit & Accountability
Access Control
Firewall & IDS
Monitoring & Malware
Configuration
Management
Information Protection
Communication Protection
System Integrity

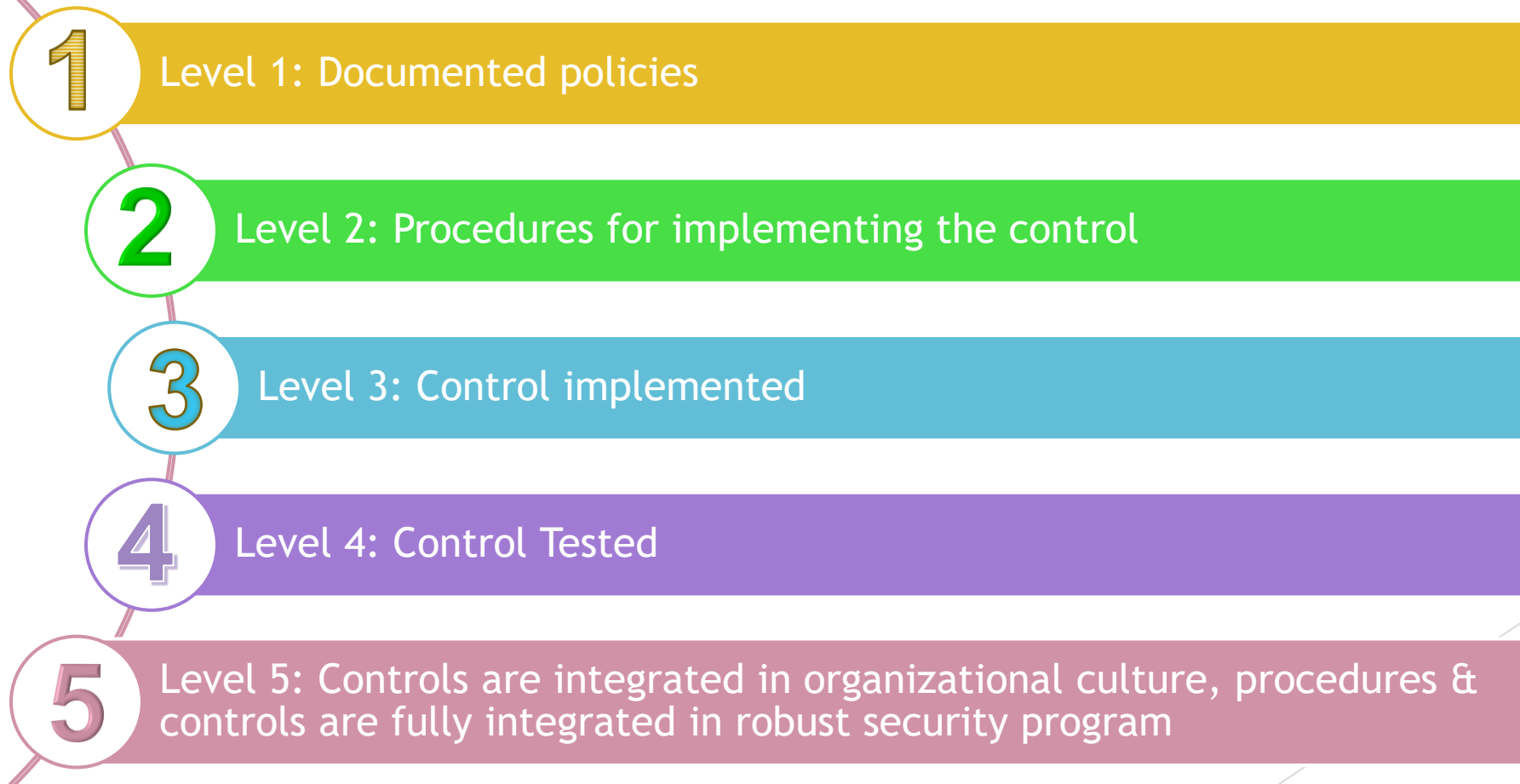


ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

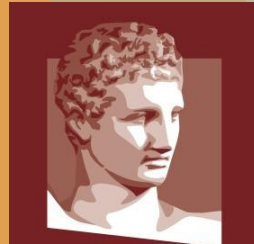
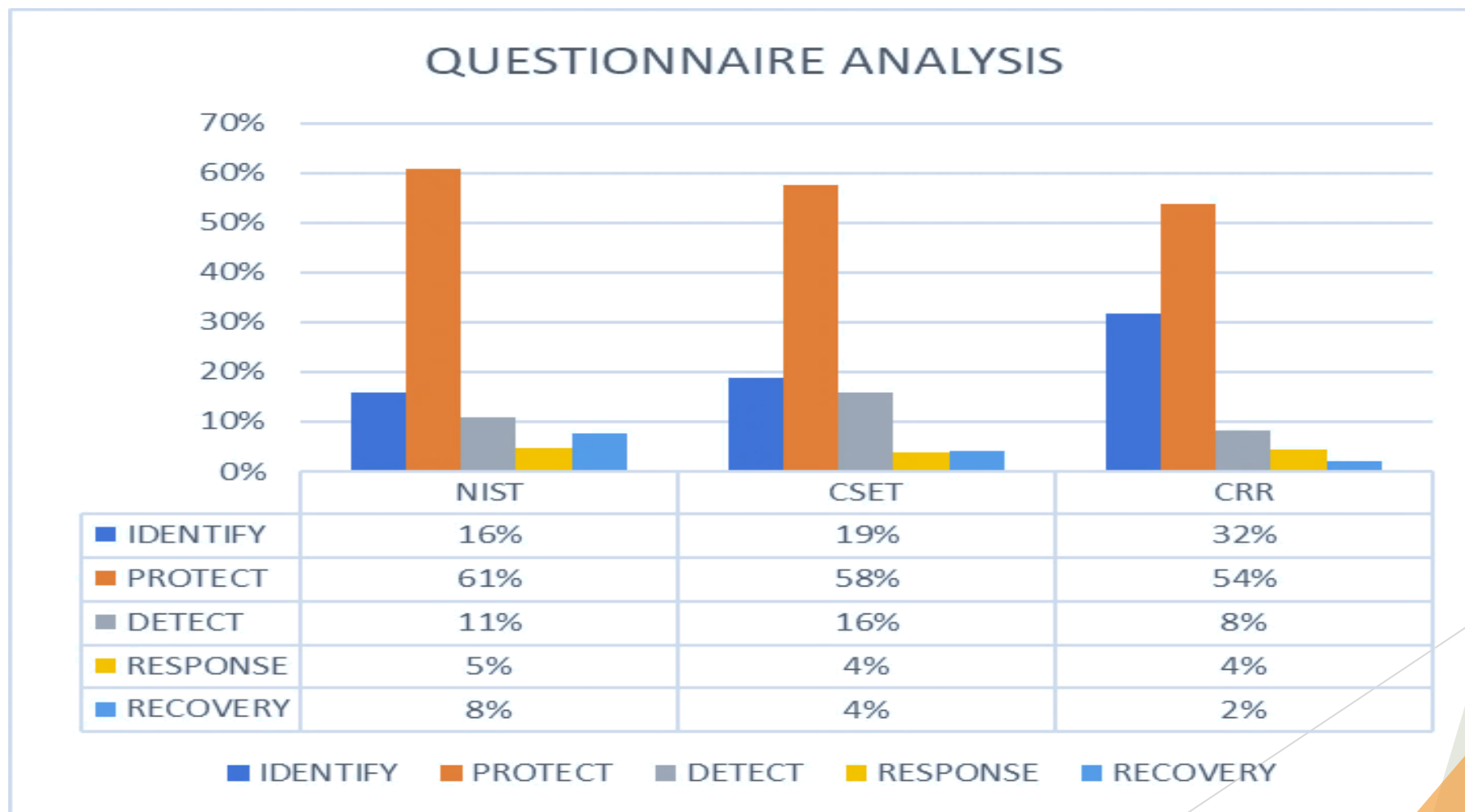
Questionnaire Content Analysis

- ▶ Progressive scale of effective implementation has been developed to measure and evaluate five 5 compliance levels.



Questionnaire Content Analysis

- ▶ All questionnaires are analyzed and classified according to their content, by using the 5 Core Functions of NIST Cybersecurity Framework.

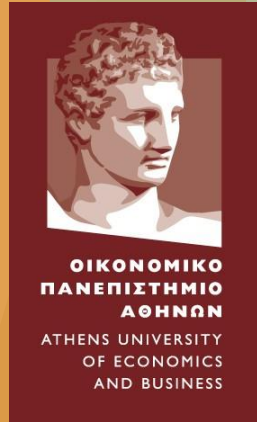


ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

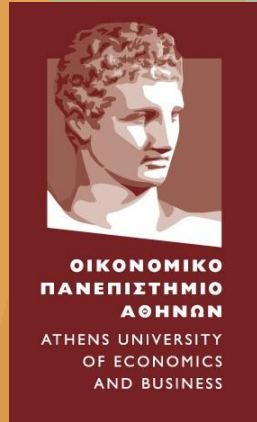
Conclusions

- ▶ Self-assessment tools provide a tailored assessments for cyber vulnerabilities.
- ▶ These tools:
 - ❑ provide structured questionnaires to build organizational knowledge
 - ❑ create a cybersecurity compliance report with compiled statistics and security recommendations.
- ▶ They are not intended to provide an all-inclusive list of control objectives and related techniques.
- ▶ Self-assessment questionnaires are only one component of the overall cyber security assessment
- ▶ A self-assessment cannot reveal all types of security weaknesses.



Conclusions

- ▶ While comparing Cybersecurity self - assessment questionnaires:
 - the majority of the questions focuses on protection measures and technical safeguards to ensure cybersecurity performance.
 - Response and recovery investigation is less examined.
- ▶ From Self - Assessment Tools Comparison, the CSET
 - is the most technical complete tool,
 - covers all particular issues of CIP and ICS and adjusts to users' needs for every standard compliance,
 - can be characterized as the most user-friendly,
 - sometimes, its detailed analysis can be time consuming for users.



References

1. Gritzalis D., Iseppi G., Mylonas A., Stavrou V., "Exiting the risk assessment maze: A meta-survey", *ACM Computing Surveys*, Vol. 51, No. 1, pp. 1-30, January 2018.
2. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in *Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection*, pp. 171-182, Springer (AICT 417), USA, 2013.
3. Lee K., *CS2SAT: The Control Systems Cyber Security Self-Assessment Tool*, No. INL/CON-07-12810, Idaho National Laboratory, USA 2008.
4. Lykou G., Moustakas D., Gritzalis D., "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensors technologies", *Sensors*, Vol. 20, June 2020.
5. Lykou G., Anagnostopoulou A., Gritzalis D., "Smart Airports Cybersecurity: Threat Mitigation and Cyber Resilience", *Sensors*, Vol. 19, January 2019.
6. Lykou G., Anagnostopoulou A., Stergiopoulos G., Gritzalis D., "Cybersecurity self-assessment tools: Evaluating the importance of securing industrial control systems in Critical Infrastructures", in *Proc. of the 13th International Conference on Critical Information Infrastructures Security*, pp. 129-142, Springer, 2018.
7. Lykou G., Mentzelioti D., Gritzalis D., "A methodology for effectively assessing Data Center sustainability", *Computers & Security*, Vol. 76, pp. 327-340, 2018.
8. Stergiopoulos G., Vasilellis E., Lykou G., Kotzanikolaou P., Gritzalis D., "Critical Infrastructure Protection tools: Classification and comparison", in *Proc. of the International Conference on Critical Infrastructure Protection*, USA, March 2016.
9. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 46-60, 2016.
10. US-CERT (2016) *Cyber Resilience Review (CRR)*. Available at: <https://www.us-cert.gov/ccubedvp/assessments>

