Automation Improvement in Cyber Risk Management

Kire Jakimoski
Faculty of Informatics
AUE-FON
Skopje, Republic of N. Macedonia
kire.jakimoski@fon.edu.mk

***Abstract*—Consolidated risk posture of organizations is more than needed nowadays in extended detection and response cybersecurity environments. Integration and automation of the modern risk management includes using controls from platforms and standards like ISO 27001, CIS v8 that should be synchronized and well mapped. Integrated and converged security approach for obtaining integrated and automated risk management is used in this paper. Main goal in this research is to propose a framework for efficient cyber risk management applicable for every type of organization. Proposed framework for automation improvement in cyber risk management includes four main entities and workflow process that describes the relation between the entities. To show the possible practical implementation of this framework, it is tested on a real risk auditing tool [11]. Another benefit of this paper is the mapping of the generated risks in the framework with CIS v8 controls and ISO 27001 controls for compliance purposes, as well as with the configuration settings of the XDR appliance explained in [11]. Mapping with the configuration settings of the selected XDR appliance makes risk mitigation process more successful. Outcome of the proposed framework is to enable simplified, automated, and efficient cyber risk management. Presented solution for automated and integrated risk management is more than needed for the organizations that want to secure their working environment from cyber attacks.**

Keywords—CIS Controls, CSR (Cybersecurity Review), eCISO (electronic Chief Information Security Officer), GRC (Governance, Risk and Compliance), ISO 27001, Risk Management, vCISO (virtual Chief Information Security Officer).

I. INTRODUCTION

Nowadays cybersecurity is complex issue like never and requires everyone's attention and contribution. Cyber threats, vulnerabilities and risks are key issues that must be assessed and considered very seriously from organizations. Compliance also plays big role in decreasing the risks in the cyber space including IoT devices. Research in [1] shows that compliance increases the probability of successful cleanup of the infected IoT devices by 32%, while the presence of competing malware reduces it by 54%. This is just one example that shows the importance of compliance in cyber risk management. Cyber Risk Management is also crucial and more than needed in 5G mobile networks. Authors in [2] present a high-level categorization of cyber attacks in 5G environment. So, integrated cyber risk management is also crucial for mitigating these types of cyber attacks in the 5G mobile networks.

Authors in [3] propose cyber and privacy risk management tool for assessing cyber and privacy risks in automated manner with decision-supportive capabilities. Although this tool gives advice about the potential security and privacy risks that are affecting target infrastructures, it doesn't offer mitigation actions.

Authors in [4] analyze the formulation of state perceptions of risk and uncertainty. Artificial Intelligence is also playing big role in automating risk management in cybersecurity space. In [5] benefits of using Artificial Intelligence in cybersecurity to protect businesses are presented with cases of risk management. Integrated cybersecurity risk management is presented in [6] including prediction of risk types through machine learning techniques and systematic identification of critical assets. Cyber risk management is more than needed in every aspect of our lives. Per example, cyber risk management is needed for automated smart ships [7]. Authors in [7] discuss attack scenarios that can be used for cybersecurity risk management and propose a secure ship network topology. Cybersecurity risk management of smart cities is discussed in [8], where authors assess smart cities and their cybersecurity measures, with a specific focus on the regulatory framework and technical standards. So, above papers [4-8] just show how cyber risk management is very important in different types of organizations and fields.

Automated risk management on IoT devices is presented in [9]. Authors in [9] propose solution called STewARD that allows users to create isolated software-defined network slices, to which they assign a required trust level using very simple risk assessment. Limitation of this tool is that it can be used just for devices in a home network.

Cybersecurity risk management necessity in the smart power grid is detailed in [10]. Authors in this paper state that specifics of how information security services are used for the power grid depend upon appropriate risk assessment and risk control. Anyway, proposed solutions in the field of security risk management are just in the context of the smart power grid.

Taking into account the limitations of the risk management tools mentioned in other papers the research in this paper proposes a framework for cybersecurity risk management that is applicable for every type of organization from small to large. Proposed framework simplifies the complex cybersecurity risk management process.

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:08:08 UTC from IEEE Xplore. Restrictions apply.

Improvements in the proposed framework are designed to be used in a real environment. In this context, proposed framework could be used to upgrade the already existing Risk Audit Tool in [11]. This Risk Audit Tool is part of the Compliance Controls Section in the manual of the XDR appliance presented in [11]. Previous contributions of this concept are already published in [12].

The remainder of this paper is organized as follows. Section 2 presents general information about cybersecurity risk management including risk assessment and risk treatment processes. In section 3 proposal for integrated and automated cyber risk management is presented. Integrated risk management framework is presented with a workflow process between four main entities in this framework that are integrated together to give complete risk management solution. Mapping of the generated risks from the platform and configuration settings of the XDR appliance that help to mitigate these risks is presented in details. Mapping of the generated risks is also done with ISO 27001 Annex A Controls and CIS Controls Version 8. Section 4 concludes this paper.

II. Cybersecurity Risk Management

A crucial part of an ISMS (Information Security Management System) is the risk management. Risk is the happening of an unwanted event or the non-happening of a wanted event which adversely affects business [13]. Realization of risk occurs when:

- the objectives of the business are unachieved,
- a failure of safeguarding business assets from loss occurs,
- there is non-compliance with organization policies and procedures or external legislation and regulation,
- the utilization of business resources is not efficient or effective,
- the confidentiality, integrity and availability of information is not reliable.

Cybersecurity Risk Management is an ongoing process for identification, analysis, and description of potential events and circumstances that can produce impacts to Information Security objectives. According to this information, management can take decisions about what risks are at acceptable level, and which risks require treatment to ensure potential impacts do not materialize.

A. Risk Assessment and Risk Treatment

Risk assessment and **treatment** processes are key areas for implementation and maintenance of a successful ISMS and they are crucial part of the ISO/IEC 27001 and ISO/IEC 27005 standards. Protection against information security threats is on appropriate level only when risks are completely understandable that ensures implementation of appropriate security controls. It is essential that organizations have an adequate risk assessment and treatment process in place to ensure that potential impacts do not become real, or if they do, contingencies are in place to deal with them. Processes should be sufficiently clear so that subsequent assessments could produce consistent, valid, and comparable results, even when carried out by different people.

Risk Treatment Plan is the outcome of the evaluation of the treatment options. This document should include the following:

- Risks requiring treatment,
- Risk Owner,
- Recommended treatment option,
- Controls to be implemented,
- Responsibility for the identified actions,
- Timescales for actions,
- Residual risk levels post controls implementation.

Implementation of security controls is very important for the risk treatment process, so Annex A of the ISO/IEC 27001 standard is very important document for identification of the appropriate controls. In this context Statement of Applicability (SoA) document is crucial for the selection of the Annex A controls from ISO/IEC 27001 standard.

Regular reviews are very important for successful management of the cybersecurity risks. Besides full annual review, the relevant risk assessments should be reviewed also upon significant changes to the business, i.e., introduction of new or changed IT services, office moves, and at least quarterly.

III. Proposal for Integrated Cyber Risk Management

Automation and integration of the cybersecurity risk management is very important in the new XDR (Extended Detection and Response) cybersecurity technologies that monitor and mitigate cybersecurity threats [14, 15]. Per example, Risk Auditing application of the Crystal Eye (CE) Platform [11] implements quick security controls assessment which assists in detection of 20 general risks that have a negative outcome on each organization or business. This application includes risk management quick questionnaire and supports risk auditing and assessment of multiple assets owned by a specific organization. After answering the questions with short “Yes” or “No” answers, preliminary risk posture of the company or business is automatically generated.

GRC (Governance, Risk and Compliance) platform is also very important part in getting automated cybersecurity risk management process done. It relates risk management process with the organization’s business units, assets, security controls, and compliance management.

Risk management process is also related with the compliance management in the GRC concept. When managing risks in the GRC platform, Treatment of the risks is crucial part with its appropriate Treatment Documents. Per example, “Key Management Lifecycle” policy is related with the specific risk(s) associated with this specific policy document. Security operations in the GRC concept include also Security Incidents and Project Management.

All aspects mentioned above are considered in the design of the proposed framework for efficient cybersecurity risk management in this research. Cybersecurity risk management using the GRC methodology is taken into account in this research as a basis that is integrated with an already implemented practical Risk Audit tool [11] that generates 20 general cybersecurity risks. Other two entities that are also incorporated in the proposed framework are Risk Server, and

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:08:08 UTC from IEEE Xplore. Restrictions apply.

CSR (Cybersecurity Review) process. More details how they are related together are graphically explained in Fig. 1.

Hence, the proposed cybersecurity risk management framework in this research is using four entities in the whole concept: Risk Audit tool (example in [11], Risk Server, GRC platform and CSR process. Fig. 1 presents the workflow process using the four entities: CSR, CE Risk Audit application, Risk Server and GRC platform.

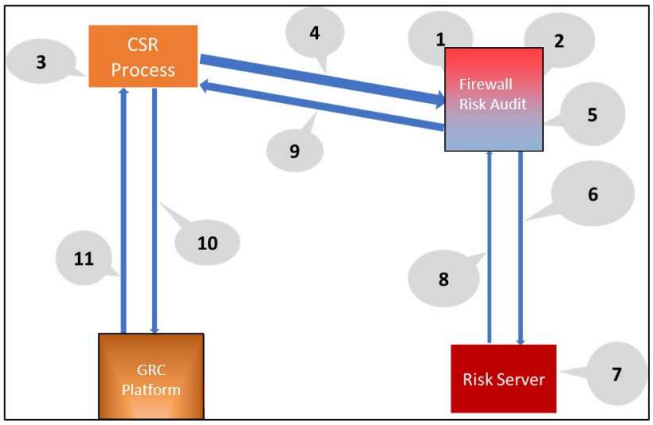

Fig. 1. Workflow Process using CSR, Risk Audit, Risk Server and GRC Platform.

Numbers from 1 to 11 in Fig. 1 are implementation steps of the proposed integrated solution for cyber risk management. Details of these implementation steps are presented here:

1. Client answers 20 short preliminary questions with Yes or No.
2. Risk audit application automatically evaluates and generates 20 pending risks without details about the level of the risk.
3. Client answers CSR detailed questions from the 20 categories.
4. Compliance team maps the answers from CSR questions with the pending risks generated in step 2.
5. Compliance team reviews and evaluates the level of each risk according to the analysis of the answers in step 3.
6. Risks with defined levels are then sent to the Risk Server.
7. Compliance team performs the following tasks to manage the risks:
   - Close Risk,
   - Edit Risk,
   - Plan a Mitigation,
   - Perform a Review,
   - Assign a Status to the Risk,
   - Plan a Mitigation,
   - Perform a Review,
   - Change a Status,
   - Add a Comment.
8. The Risk Report gets automatically updated based on the tasks/actions performed by the compliance team in the risk server.
9. Results from the risk reports are used as input for the CSR Report.
10. Findings from the CSR report can be used as input for managing the assets, risks, controls, policies in the GRC platform.
11. Calendar could be used in the GRC platform to initiate alarms for reviews of the CRS process.

Cybersecurity risks have strong connection with cybersecurity controls and that's why it is very important to map them correctly to mitigate the risks. Practical integration of the cybersecurity risks and controls is presented in the following Tables 1 and 2. This second phase of mapping actually completes the proposed solution for automated and integrated cyber risk management.

Table 1 gives mapping of the generated risks in the implementation step 2 above, with the configuration options of the XDR appliance [11]. Possessing information which configuration option of the XDR appliance mitigates which cybersecurity risk is very important part for the whole process of cybersecurity risk management. So, Table 1 is practical example of how cybersecurity risks could be efficiently mapped with the configuration options in the XDR appliance that could treat these risks.

TABLE I. EXAMPLE OF MAPPING THE RISKS WITH THE CONFIGURATION SETTINGS OF A MODERN XDR APPLIANCE [11]

Pending Risk	GUI of XDR Appliance
1. Attackers can use unauthorized and unmanaged devices to gain access to network.	Left-hand Navigation Panel > Network Control > Device Management > Network Map
2. Attackers can use unauthorized and unmanaged software to collect sensitive information from compromised systems and other systems connected to them.	Left-hand Navigation Panel > Security Configuration > Application Whitelisting; Left-hand Navigation Panel > Security Configuration > Protocol Filtering > Application Filter
3. Attackers can exploit vulnerable services and settings to compromise operating systems and applications.	Left-hand Navigation Panel > Security Configuration > Advanced Firewall; Left-hand Navigation Panel > Network Control > Infrastructure > DNS Server
4. Attackers can take advantage of gaps between the appearance of new knowledge and remediation to compromise computer systems.	Left-hand Navigation Panel > Compliance Controls > Vulnerability Scanning
5. Attackers can misuse administrative privileges to spread inside the enterprise.	Left-hand Navigation Panel > System Configuration > Accounts Manager > Accounts; Left-hand Navigation Panel > System Configuration > Accounts Manager > Active Directory Authentication
6. Attackers can hide their location, malicious software, and activities on victim machines due to deficiencies in security logging and analysis.	Left-hand Navigation Panel > Security Configuration > Log Processing and Reporting; Left-hand Navigation Panel > Compliance Controls > Network Backup > Forensic Logging; Left-hand Navigation Panel > Reports > Log Viewer
7. Attackers can craft content to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks.	Left-hand Navigation Panel > Network Control > Email Scanning Gateway; Left-hand Navigation Panel > Security Configuration > Content Filter

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:08:08 UTC from IEEE Xplore. Restrictions apply.

8. Attackers can use malicious software to attack our systems, devices, and data.	Left-hand Navigation Panel > Security Configuration > Gateway Security > Anti-Malware File Scanner; Left-hand Navigation Panel > Security Configuration > Gateway Security > Anti-phishing; Left-hand Navigation Panel > Security Configuration > Gateway Security > Antivirus
9. Attackers can scan for remotely accessible network services that are vulnerable to exploitation.	Left-hand Navigation Panel > Security Configuration > Protocol Filtering; Left-hand Navigation Panel > Network Control > Infrastructure > Network Settings; Left-hand Navigation Panel > Security Configuration> Advanced Firewall Application
10. Attackers can make significant changes to configurations and software on compromised machines, and it may be extremely difficult to remove all aspects of their presence.	Left-hand Navigation Panel > System Configuration > Backup > Baremetal Backup and Restore; Left-hand Navigation Panel > System Configuration > Backup > Configuration Backup and Restore; Left-hand Navigation Panel > System Configuration > Backup > Storage Manager
11. Attackers can gain access to sensitive data, alter important information, or use compromised machines to pose as trusted systems on our network by exploiting vulnerable services and settings	Left-hand Navigation Panel > Network Control > Infrastructure > DHCP Server; Left-hand Navigation Panel > Network Control > Infrastructure > DNS Server; Left-hand Navigation Panel > Network Control > Infrastructure > Network Settings; Left-hand Navigation Panel > Network Control > Infrastructure > SSH Server
12. Attackers can exploit vulnerable systems on extranet perimeters to gain access inside our network.	Left-hand Navigation Panel > Security Configuration > Intrusion Protection & Detection
13. Attackers can exfiltrate data from our networks compromising the privacy and integrity of sensitive information.	Left-hand Navigation Panel > Compliance Controls > Data Loss Protection; Left-hand Navigation Panel > Compliance Controls > Network Backup > Network File Share; Left-hand Navigation Panel > Security Configuration > Log Processing and Reporting
14. Attackers can find and exfiltrate important information, cause physical damage, or disrupt operations due to improper separation of sensitive and critical assets from less sensitive information.	Left-hand Navigation Panel > Compliance Controls > Data Loss Protection; Left-hand Navigation Panel > Security Configuration > Advanced Firewall Application; Left-hand Navigation Panel > Network Control > Infrastructure > Network Settings; Left-hand Navigation Panel > System Configuration > Accounts Manager > Active Directory Authentication; Left-hand Navigation Panel > Compliance Controls > Network File Share
15. Attackers can gain wireless access and bypass our security perimeters in order to steal data.	Left-hand Navigation Panel > Network Control > Device Management > Network Map; Left-hand Navigation Panel > Network Control > Wireless Access Point
16. Attackers can impersonate legitimate users by exploiting legitimate but inactive user accounts.	Left-hand Navigation Panel > System Configuration > Account Manager > Accounts; Left-hand Navigation Panel > System Configuration > Account Manager > Active Directory Authentication; Left-hand Navigation Panel > System Configuration > Account Roles > Groups; Left-hand Navigation Panel > System Configuration > Account Roles > Users
17. Attackers can exploit employee knowledge gaps to compromise systems and networks.	Security Awareness Training as part of the eCISO and vCISO services
18. Attackers can take advantage of vulnerabilities in software to gain control over vulnerable machines.	Left-hand Navigation Panel > Security Configuration > Application Whitelistening; Left-hand Navigation Panel > Security Configuration > Protocol Filtering > Application Filter
19. An attacker may have a greater impact, cause more damage, infect more systems, and exfiltrate more sensitive data due to a poor incident response plan	Left-hand Navigation Panel > Compliance Controls > Incident Response Services; Left-hand Navigation Panel > Compliance Controls > Incident and Event Services SIEM
20. Attackers can take advantage of unknown vulnerabilities due to a lack of testing of organization defences.	Left-hand Navigation Panel > Compliance Controls > Vulnerability Scanning

It is very important to relate the cybersecurity risks with world standards for cybersecurity controls like ISO 27001 [16] or CIS v8 [17] for compliance purposes. This is done in Table 2, which presents the relation of each of the 20 general cybersecurity risks used in the proposed framework with the ISO 27001 Annex A Controls and CIS v8. This information is very important to relate the specific controls with the specific risks that could be generated by the Risk Auditing tool.

TABLE II. MAPPING OF THE PENDING RISKS WITH CIS V.8 CONTROLS AND ISO 27001 ANNEX A CONTROLS

General Risks	Related Controls in CIS Controls Version 8	Related ISO 27001 Annex A Controls
1. Attackers can use unauthorized and unmanaged devices to gain access to network.	1. Inventory and Control of Enterprise Assets	A.8.1.1; A.11.2.5; A.13.1.1; A.9.1.2
2. Attackers can use unauthorized and unmanaged software to collect sensitive information from compromised systems and other systems connected to them.	2. Inventory and Control of Software Assets	A.8.1.1; A.12.5.1; A.12.6.2
3. Attackers can exploit vulnerable services and settings to compromise operating systems and applications.	4. Secure Configuration of Enterprise Assets and Software	A.8.1.3; A.14.2.5; A.14.2.2; A.12.1.2
4. Attackers can take advantage of gaps between the appearance of new knowledge and remediation to compromise computer systems.	7. Continuous Vulnerability Management	A.9.2.3; A.12.6.1
5. Attackers can misuse administrative privileges to spread inside the enterprise.	6. Access Control Management	A.9.2.3; A.9.4.2; A.9.4.3; A.9.4.4; A.12.4.3
6. Attackers can hide their location, malicious software, and activities on victim machines due to deficiencies in security logging and analysis.	8. Audit Log Management	A.12.4.1; A.12.4.3: A.12.4.4

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:08:08 UTC from IEEE Xplore. Restrictions apply.

7. Attackers can craft content to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks.	9. Email and Web Browser Protections	A.8.1.3; A.12.2.1: A.12.6.2; A.13.1.1; A.13.2.3
8. Attackers can use malicious software to attack our systems, devices, and data.	10. Malware Defences	A.12.2.1: A.12.4.1
9. Attackers can scan for remotely accessible network services that are vulnerable to exploitation.	4. Secure Configuration of Enterprise Assets and Software 13. Network Monitoring and Defence	A.13.1.1; A.13.1.2; A.13.1.3
10. Attackers can make significant changes to configurations and software on compromised machines, and it may be extremely difficult to remove all aspects of their presence.	11. Data Recovery	A.12.3.1
11. Attackers can gain access to sensitive data, alter important information, or use compromised machines to pose as trusted systems on our network by exploiting vulnerable services and settings	12. Network Infrastructure Management 4. Secure Configuration of Enterprise Assets and Software	A.12.1.2; A.13.1.1; A.13.1.3
12. Attackers can exploit vulnerable systems on extranet perimeters to gain access inside our network.	13. Network Monitoring and Defence 15. Service Provider Management	A.9.4.2; A.13.1.1
13. Attackers can exfiltrate data from our networks compromising the privacy and integrity of sensitive information.	3. Data Protection	A.8.2.1; A.13.2.3; A.6.2.1; A.8.3.1
14. Attackers can find and exfiltrate important information, cause physical damage, or disrupt operations due to improper separation of sensitive and critical assets from less sensitive information.	6. Access Control Management	A.8.1.1; A.9.1.1; A.10.1.1; A.12.4.3; A.13.1.1; A.13.1.3
15. Attackers can gain wireless access and bypass our security perimeters in order to steal data.	4. Secure Configuration of Enterprise Assets and Software 6. Access Control Management	A.8.1.1; A.8.1.3; A.10.1.1; A.13.1.1; A.13.1.3
16. Attackers can impersonate legitimate users by exploiting legitimate but inactive user accounts.	5. Account Management	A.8.1.1; A.8.1.3; A.9.2.1; A.9.2.6; A.10.1.1; A.12.4.1; A.13.1.1
17. Attackers can exploit employee knowledge gaps to compromise systems and networks.	14. Security Awareness and Skills Training	A.7.2.2
18. Attackers can take advantage of vulnerabilities in software to gain control over vulnerable machines.	16. Application Software Security	A.10.1.1; A.12.1.4; A.12.6.1; A.14.2.1; A.14.2.5
19. An attacker may have a greater impact, cause more damage, infect more systems, and exfiltrate more sensitive data due to a poor incident response plan	17. Incident Response Management	A.16.1.1; A.16.1.3
20. Attackers can take advantage of unknown vulnerabilities due to a lack of testing of organization defences.	18. Penetration Testing	A.12.6.1: A.16.1

IV. Conclusion

Smart and automated management of the cybersecurity risks nowadays is more than needed for any type of organization from small to large involved in any type of business. This research paper proposes automated and integrated solution for cybersecurity risk management that is tested in a real environment. Proposed platform includes ISO 27001 standard, CIS Controls version 8, Risk Auditing Tool, Risk Server, GRC platform, and CSR process with vCISO and eCISO services. Mapping of the configuration settings of the selected XDR appliance with the ISO 27001 standard and CIS Controls version 8 is also done to include the well-known standards in the automation of the cybersecurity risk management process. Coordination and relation between the four entities in the proposed platform together with the help of the ISO 27001 standard and CIS Controls version 8 improves, simplifies, and automates the complex process of cybersecurity risk management.

Benefits of this paper in the field of automation and integration of the cybersecurity risk management will help cybersecurity experts in improving the risk management which is one of the most important and complex issues in cybersecurity.

First benefit is the proposal explained in Fig. 1 that includes four main entities that enable fast and efficient cyber risk management.

Second benefit is in the mappings of the twenty risks included in the proposal in Fig. 1 with well-known ISO 27001 and CIS v8 controls (Table 2) as well as in the mappings of the same risks with the configuration settings of a real XDR appliance (Table 1). These mappings will help in the mitigation process of the evaluated risks. Relation of each risk with the appropriate settings of the XDR appliance (Table 1) will help to reduce the risks that are previously evaluated with the proposed framework in Fig. 1. Relation of each risk with ISO 27001 and CIS v8 standards will also help to fulfill the compliance requirements in cybersecurity.

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:08:08 UTC from IEEE Xplore. Restrictions apply.

REFERENCES

[1] Elsa Rodríguez, Susanne Verstegen, Arman Noroozian, Daisuke Inoue, Takahiro Kasama, Michel van Eeten, Carlos H Gañán, User compliance and remediation success after IoT malware notifications, Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab015, https://doi.org/10.1093/cybsec/tyab015

[2] Mohan, Jaya Preethi, Niroop Sugunaraj, and Prakash Ranganathan. "Cybersecurity threats for 5G networks." *2022 IEEE international conference on electro information technology (eIT)*. IEEE, 2022.

[3] Gonzalez-Granadillo, G.; Menesidou, S.A.; Papamartzivanos, D.; Romeu, R.; Navarro-Llobet, D.; Okoh, C.; Nifakos, S.; Xenakis, C.; Panaousis, E. Automated Cyber and Privacy Risk Management Toolkit. Sensors 2021, 21, 5493. https://doi.org/10.3390/s21165493.

[4] Aaron F Brantly, Risk and uncertainty can be analyzed in cyberspace, Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab001, https://doi.org/10.1093/cybsec/tyab001

[5] Mosteanu NR. Artificial intelligence and cybersecurity–face to face with cyber attack–a maltese case of risk management approach. Ecoforum Journal. 2020 May 9;9(2).

[6] Kure HI, Islam S, Mouratidis H. An integrated cybersecurity risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications. 2022 Feb 2:1-31.

[7] Furumoto K, Kolehmainen A, Silverajan B, Takahashi T, Inoue D, Nakao K. Toward automated smart ships: Designing effective cyber risk management. In2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics) 2020 Nov 2 (pp. 100-105). IEEE.

[8] Vitunskaite M, He Y, Brandstetter T, Janicke H. Smart cities and cybersecurity: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Computers & Security. 2019 Jun 1;83:313-31.

[9] Boussard M, Papillon S, Peloso P, Signorini M, Waisbard E. STewARD: SDN and blockchain-based Trust evaluation for Automated Risk management on IoT Devices. InIEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) 2019 Apr 29 (pp. 841-846). IEEE.

[10] Ray PD, Harnoor R, Hentea M. Smart power grid security: A unified risk management approach. In44th Annual 2010 IEEE international Carnahan conference on security technology 2010 Oct 5 (pp. 276-285). IEEE.

[11] Piranha, R., Controls, C. and Auditing, R., 2022. *Risk Auditing | Crystal Eye Manual*. [online] Manual.redpiranha.net. Available at: <https://manual.redpiranha.net/40/compliance-controls/risk-auditing> [Accessed 25 February 2022].

[12] Jakimoski, Kire, Adam Bennett, and Adam Holliday. "Positioning Cybersecurity Risk Management Within a Consolidated Security Platform." Building Cyber Resilience against Hybrid Threats. IOS Press, 2022. 134-144.

[13] ISO 9001 Toolkit: Version 3. Risk and Opportunity Assessment Process. CertiKit. Avalialbe at: https://issuu.com/public-it/docs/qms-doc-06-2_risk_and_opportunity_assessment_proce [Accessed 04 March 2022].

[14] Gartner Top 9 Security and Risk Trends for 2020. *www.gartner.com*. Available at: < https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020> [Accessed 15 February 2022].

[15] Understanding XDR Security: Complete Guide". *Cynet.* Available at: <https://www.cynet.com/xdr-security/understanding-xdr-security-concepts-features-and-use-cases/> [Accessed 15 February 2022]

[16] ISO 27001 Annex A Controls. International Organization for Standardization. Available at: < https://www.iso.org/standard/54534.html> [Accessed 28 April 2022].

[17] CIS Critical Security Controls Version 8. Center for Internet Security. Available at: < https://www.cisecurity.org/controls/v8> [Accessed 28 April 2023.

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:08:08 UTC from IEEE Xplore. Restrictions apply.