information

MDPI

Article

Exploring Effective Approaches to the Risk Management Framework (RMF) in the Republic of Korea: A Study

Giseok Jeong [1,2], Kookjin Kim [3], Sukjoon Yoon [3], Dongkyoo Shin [2,3,4] and Jiwon Kang [2,3,*]

[1] Maritime Guided Weapon Program Team, Defense Acquisition Program Administration, Gwacheon 13809, Republic of Korea; unicorn65@korea.kr
[2] Department of Computer Engineering, Sejong University, Seoul 05006, Republic of Korea; shindk@sejong.ac.kr
[3] Cyber Warfare Research Institute, Sejong University, Seoul 05006, Republic of Korea; kjkim@sju.ac.kr (K.K.); ysjoony@sejong.ac.kr (S.Y.)
[4] Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, Republic of Korea
* Correspondence: jwkang@sejong.ac.kr

Abstract: As the world undergoes rapid digitalization, individuals and objects are becoming more extensively connected through the advancement of Internet networks. This phenomenon has been observed in governmental and military domains as well, accompanied by a rise in cyber threats consequently. The United States (U.S.), in response to this, has been strongly urging its allies to adhere to the RMF standard to bolster the security of primary defense systems. An agreement has been signed between the Republic of Korea and the U.S. to collaboratively operate major defense systems and cooperate on cyber threats. However, the methodologies and tools required for RMF implementation have not yet been fully provided to several allied countries, including the Republic of Korea, causing difficulties in its implementation. In this study, the U.S. RMF process was applied to a specific system of the Republic of Korea Ministry of National Defense, and the outcomes were analyzed. Emphasis was placed on the initial two stages of the RMF: 'system categorization' and 'security control selection', presenting actual application cases. Additionally, a detailed description of the methodology used by the Republic of Korea Ministry of National Defense for RMF implementation in defense systems is provided, introducing a keyword-based overlay application methodology. An introduction to the K-RMF Baseline, Overlay, and Tailoring Tool is also given. The methodologies and tools presented are expected to serve as valuable references for ally countries, including the U.S., in effectively implementing the RMF. It is anticipated that the results of this research will contribute to enhancing cyber security and threat management among allies.

Keywords: risk management framework (RMF); cyber risk; cyber security; system classification; security control selection; overlay; tailoring; organizations

Citation: Jeong, G.; Kim, K.; Yoon, S.; Shin, D.; Kang, J. Exploring Effective Approaches to the Risk Management Framework (RMF) in the Republic of Korea: A Study. *Information* **2023**, *14*, 561. https://doi.org/10.3390/info14100561

Academic Editor: Leandros Maglaras

Received: 28 August 2023
Revised: 9 October 2023
Accepted: 10 October 2023
Published: 12 October 2023

1. Introduction

The world is being positioned within the swift flow of digitization. This transformation has been driving the development of Internet networks through the connection of humans and objects, consequently converting the entire globe into one vast network. Through this evolution, stronger connections have brought about innovations in all sectors of society, especially in government and military domains. However, along with these positive changes, technological advancements have also escalated threats in cyberspace [1–3].

Cybersecurity is no longer optional. It has become an imperative, and governments and corporations worldwide are relentlessly working to overcome it. In the U.S., the Federal Information Processing Standards (FIPS) and the National Institute of Standards and Technology (NIST) developed the RMF to create a unified information protection framework [4]. In alignment with this trend in information protection, the U.S. Department of Defense (DoD) transitioned from the original DIACAP to the RMF in 2008 and issued the Department of Defense Instruction 8510.01 [5–11]. Furthermore, they strongly urge allied nations sharing key defense systems to reinforce cybersecurity by complying with RMF standards. As part of these efforts, South Korea and the U.S. have signed a cooperative agreement to operate major defense systems jointly and address the ensuing cybersecurity threats.

However, due to insufficient comprehension of the methodologies and tools needed to implement the RMF, several allied countries, including South Korea, are facing challenges. To overcome these obstacles, this paper aims to apply the U.S. RMF process to the Republic of Korea Ministry of National Defense (K-MND)'s OO system and analyze the results. The objective of this study is to present practical application methods and cases for the initial two stages of the RMF, namely 'System Categorization' and 'Security Control Selection.' This will describe the detailed methodology that the K-MND has used to apply the RMF to the defense OO system and introduce a keyword-based overlay application method. Lastly, the K(Korea)-RMF Baseline, Overlay, and Tailoring Tool will be introduced.

This paper aims to provide methodologies and tools that can assist countries like South Korea, an ally of the U.S., in implementing the RMF more effectively. By doing so, it seeks to offer solutions for enhancing cybersecurity and managing associated threats to allied countries. These endeavors are expected to foster a deeper understanding and strategic approach to cybersecurity, ultimately contributing to the effective management and control of threats in cyberspace.

The structure of this paper is as follows: Section 1 discusses the need for RMF application. Section 2 investigates research cases where THE RMF was applied. In Section 3, detailed methodologies on how the K-MND-applied RMF are presented. Section 4 applies the methodology introduced in this paper to the OO system, conducts experiments using the K-RMF Baseline, Overlay, and Tailoring Tool, and derives results. Section 5 reflects on the conclusions of this study.

2. Research on the RMF

In this chapter, a detailed examination of what the RMF is will be conducted. Subsequently, research cases applying the RMF will be thoroughly investigated and analyzed. Through this process, an attempt will be made to understand how the RMF is being used across various industries and sectors. Additionally, details regarding the application projects and methodologies will be provided, and various cases offering insights into the RMF's implementation will be investigated and analyzed.

2.1. Risk Management Framework

The RMF is applied to all IT systems within the NIST, DoD, and National Security Systems (NSS) service components [12]. Moreover, the associated policy is structured as shown in Table 1.

DoDI 8500.01 "Cybersecurity" [13] establishes its policy based on NIST SP 800-39 [14], NIST SP 800-37 [15], and CNSSP 22 [16]. DoDI 8500.01 provides detailed content on the cybersecurity guidelines of the U.S. Department of Defense. This document offers comprehensive guidance on how to establish a cybersecurity program to protect and defend the Department of Defense's information and IT systems. It also explains the application methods within various departments and offices in the Department of Defense and outlines the roles and responsibilities of the primary authorization officials and senior information security officers of the Department of Defense. DoDI 8510.01 "Risk Management Framework for DoD IT" [5] sets its policy based on NIST SP 800-30 [17], NIST SP 800-53 [18], NIST SP 800-53A [19], NIST SP 800-137 [20], NIST SP 800-60 [21], NIST 800-160(DRAFT) [22], CNSSI 1253 [23], DRAFT CNSSI 1253A [23], and CNSS 4009 [24]. DoDI 8510.01 introduces the Risk Management Framework (RMF) for the U.S. Department of Defense's IT systems. This document is designed to protect the Department of Defense's IT resources and information assets, offering a continuous and integrated approach to cyber threats. Central to DoDI 8510.01 is the emphasis on the certification and authorization process of the Department of Defense IT's systems through the application of the RMF. This includes evaluating the effectiveness of security measures, identifying the risk level of systems, and implementing and validating required security controls. Such an approach is crucial for the Department of Defense to manage risks to information and information systems effectively, support the Department's mission, and ensure the confidentiality, integrity, and availability of information and information systems. In conclusion, DoDI 8510.01 serves as a key guideline to protect the Department of Defense's IT systems, manage risks, and offer an integrated approach to cybersecurity. It plays a central role in promoting the protection and effective use of the Department of Defense's IT resources and information assets.

Table 1. RMF Policies of NIST, DoD, and NSS.

NIST	DoD	NSS
NIST SP 800-39 [14] Managing Information Security Risk	DoDI 8500.01 "Cybersecurity" [13] IT Definitions Security Controls Guidance Enterprise Governance	CNSSP 22 [16] IA Risk Management Policy for NSS
NIST SP 800-37 [15] Risk Management Framework		
NIST SP 800-30 [17] Risk Assessment	DoDI 8510.01 "Risk Management Framework for DoD IT" [5]	CNSSI 1253 [23] Categorization Baselines NSS Assignment Values
NIST SP 800-53 [18] Cybersecurity Controls and Enhancements		
NIST SP 800-53A [19] Cybersecurity Control Assessment Procedures		DRAFT CNSSI 1253A [23] Implementation and Assessment Procedures
NIST SP 800-137 [20] Continuous Monitoring		
NIST SP 800-60 [21] Mapping Types of Information to Security Categories		CNSS 4009 [24] Information Assurance/Cybersecurity Definitions
NIST 800-160(DRAFT) [22] Security Engineering Guideline		

The processes of the RMF are as follows:

1. Categorize: The information of the system and the system itself are classified according to the standards of FIPS 199 and the associated NIST SP 800-60. At this stage, the type of system information is identified, and the risk level is determined based on confidentiality, integrity, and availability.
2. Select: Security controls proposed in standards like NIST SP 800-53 are selected. This stage involves determining appropriate security controls based on the system's security requirements and associated risk levels.
3. Implement: The selected security controls are applied and implemented in the system. The implementation stage encompasses the design, development, configuration, and installation of the controls.
4. Assess: The effectiveness of the implemented security controls is evaluated. This assessment is conducted using security testing and evaluation techniques to accurately understand the system's security status.
5. Authorize: Decisions on system risk acceptance and operation are made. System owners or senior officials can authorize or deny the operation of the system based on the evaluation results and the system's overall security status.
6. Monitor: The security status of the system is continuously monitored, risks are tracked, and security controls are modified or updated as necessary. This stage emphasizes

ensuring continuous improvement in security status and the ability to respond to new threats or changes.

2.2. RMF Research by Industry

The RMF is an integrated framework that provides methods to identify, assess, and manage risks that may arise in a company or organization's information system. Initially developed for the security of governmental agencies' information systems, it is now utilized across various industries and sectors. Several cases related to this have been researched and analyzed.

2.2.1. The Aviation and Defense Industries

Robertson, J. et al. [25] proposed a cloud-based computing framework for artificial intelligence (AI) innovation to support operations across various domains. The cloud was explained based on Amazon Web Services (AWS), and the RMF was employed to meet information protection requirements [26]. They defined system boundaries, compiled system inventories, and categorized the types of information processed by the system. They suggested that upon completing the RMF process, an authority to operate (ATO) can be granted for a specific system or set of systems.

Kim, I. et al. [27] proposed a mission-based cybersecurity testing and assessment model for RMF-related weapon systems. The testing and assessment were conducted through simulations, with the first stage of simulation detailing the process of specifying threat scenarios in connection with the RMF.

Pearson, J. et al. [28] applied the RMF to address process discontinuity issues in the U.S. Army's aviation safety and cybersecurity group. They explored ways to enhance resilience against cyber-attacks and reduce risks related to flight safety and mission readiness. This study identified the causes of discontinuity using organizational discontinuity theory and sought methods for improvement. Expert interviews and document analysis for data triangulation were utilized.

2.2.2. The Automotive and Manufacturing Industries

Haitao, Z. et al. [29] proposed a systematic and structured threat model for intelligent vehicles based on some research on threat analysis and risk assessment techniques used in existing information systems and real-life experiences in the automotive sector. This threat model enhanced the existing Threat Assessment and Remediation Analysis (TARA) [30] model by incorporating the RMF's cybersecurity requirements. An experimental application of the improved TARA model based on the RMF for over-the-air programming (OTA) [31] business concluded that 46 man-days were consumed to complete threat analysis, indicating enhanced efficiency and accuracy.

Chhawri, S. et al. [32] discussed applying advanced automotive cybersecurity technologies to smart vehicle projects, software safety, and software architecture. They also covered the advantages of employing such technologies in the DoD and how they can help implement infrastructure methodologies at reduced cost. They applied the NIST RMF for automotive use cases based on threat modeling and risk assessment processes. As a result, they developed security test cases and presented a comprehensive test process for automotive security.

Thangavelu, S. et al. [33] emphasized the defects at the design stage in the manufacturing process where caution is required. They proposed a conceptual process model that enables manufacturers to minimize threats and integrate robustness into the drone ecosystem. This conceptual model was enhanced by referencing the conventional system threat approach and the RMF provided by NIST. The proposed model aims to improve system security and minimize risks resulting from human errors or design failures.

2.2.3. The Environmental and Energy Industries

Jiang, L. et al. [34] proposed a risk management model targeting the power industry, evaluated security controls, and made enhancements for infrastructure strengthening. To apply the RMF for risk management in power systems, they underwent five stages: threat modeling, impact analysis, risk assessment, cost analysis, and a security control proposal. As a result, they presented that security loss rates can be measured using benefit matrices, dependency matrices, and vector matrices.

Miranda, A. W. Et al. [35] introduced a risk assessment method to evaluate grid-connected commercial solar power plants. To utilize this methodology, they presented an initial risk management framework based on the RMF to address cybersecurity outcomes and best practices. The results showed substantial losses when the metering system is compromised, calculated according to the RMF's security control items.

De Peralta, F. et al. [36] proposed a framework for the U.S. Department of Energy to identify cybersecurity vulnerabilities in marine renewable energy systems and determine risks. They recommended using the NIST RMF, suggesting that it assists marine renewable energy (MRE) system owners and operators in prioritizing cybersecurity risk management activities. Utilizing this framework allows MRE system owners and operators to minimize cybersecurity risks and maintain system safety and reliability.

The ELECTRON architecture was proposed by Radoglou-Grammatikis, P. et al. [37]. It was designed to address the cyber-physical risks of the smart electric grid and includes key frameworks such as BORDER, CYPER, BRIDGE, and PRINCE.

Emphasis is placed on the dynamic evaluation of device security and dynamic risk assessment in a collaborative manner throughout the entire lifecycle of power grid components by Liatifis, A. et al. [38]. For this purpose, continuous risk re-calculation is combined with persistent device security evaluation based on network topology information. Additionally, the Risk Assessment Module is tasked with the dynamic risk assessment, and the risk value of the related assets is recalculated upon receiving various security alerts.

2.2.4. The Medical and Health Industries

Udroiu, A.M. et al. [39] proposed a method that can be used to assess and improve the security of medical institutions under significant pressure during the pandemic, applying the NIST cybersecurity framework and The Health Information Trust Alliance (HITRUST) model [40]. They noted numerous cyber-attacks targeting patients' personal data and specific treatment and scientific data during the pandemic period, exposing medical systems to extensive risks associated with the theft, exploitation, inaccessibility, or destruction of this sensitive data. They improved this security using both the NIST RMF and the HITRUST [41–43]. All the proposed models aimed to maintain flexibility for expansion and further development. They suggested two approaches: adapting the self-assessment questionnaire and guiding the implementation or enhancement of the cybersecurity program.

Van Devender, M. S. et al. [44] presented a risk assessment framework for threats and vulnerability evaluation in the computing and cybersecurity domains of medical devices. They described how to analyze the security threats and vulnerabilities of a particular medical device by applying the NIST RMF. As a result, they proposed the application of the RMF process to the FDA's Center for Devices and Radiological Health, emphasizing its effectiveness.

Information regarding the security assessment of cloud-based healthcare applications was provided by Miller, J. C. [45]. The importance of adhering to the Health Insurance Portability and Accountability Act (HIPAA) policy was emphasized by him [46], along with a guide to evaluating potential vulnerabilities. Additionally, he elaborated on how to utilize the RMF for the security assessment of cloud-based healthcare applications. A method to identify the security vulnerabilities of the application using the RMF and to plan and implement suitable security control items to address them was presented by him.

2.2.5. The Internet of Things (IoT) Industry

The development of a new model to calculate the economic impact of IoT cyber risks by applying the Cyber Value at Risk and MicroMort models for measuring the economic impact of cyber risks was undertaken by Radanliev, P. [47]. In this study, distinctions were made between IoT risk vectors and vertices, and a model was proposed that uses the IoT MicroMort-based Value at Risk model to measure the maximum possible loss over a given time.

The RMF was applied to the risk assessment of power IoT by Li, K. et al. [48]. By integrating it with the improved AHP (analytic hierarchy process), the risks and threats of power IoT were analyzed. In the experiment, a simple scenario of power IoT was simulated to validate the effectiveness of the proposed risk assessment method. From the simulation results, it was demonstrated that the proposed risk assessment method can be dynamically implemented in power IoT.

Network data in an IoT environment were analyzed by Brandon, A. et al. [49] to support risk management. The exploration of data analysis was presented, showing how organizations can use the RMF to manage the security of IoT networks. The primary objective was to demonstrate the ability to analyze IoT traffic and discern whether an attack has been executed or is in progress. Additionally, once the appearance of an attack is understood, practical applications of toolsets become possible.

From the studies investigated in Sections 2.2.1–2.2.5, a summary is presented in Table 2.

Based on the studies summarized in Table 2, when examining the application areas of the RMF, it can be discerned that the RMF plays a pivotal role in information protection and risk management across various industries:

1. The aviation and defense industries: The RMF has been employed to meet information protection requirements in key areas such as the design of cloud-based computing frameworks, the detailing of threat scenarios in simulations, and resolving process issues within cybersecurity groups. This confirms that, in the aviation and defense sector, the RMF plays a vital role in satisfying information security needs in conjunction with technological advancements.
2. The automotive and manufacturing industries: The RMF has been utilized in major areas like the automation of car security testing, the enhancement of efficiency and accuracy in threat analysis and risk assessment, and the improvement of the conceptual process model related to drone production. This suggests a need for the integrated approach of the RMF in the automotive and manufacturing sectors.
3. The environmental and energy industries: The RMF has been applied to diverse topics such as the risk management of power systems, calculating the loss rates of grid-connected commercial solar power plants, and identifying security vulnerabilities in marine renewable energy systems. This indicates that security concerns and risk management are becoming increasingly significant in the environmental and energy sectors.
4. The medical and health industries: The RMF has been employed for improving the HITRUST, cybersecurity in medical device computing, and the security evaluation of cloud-based healthcare applications. This suggests that cybersecurity issues are emerging as significant concerns in the medical sector, necessitating an approach that incorporates the RMF.
5. The IoT industry: The RMF has been applied to various topics, including the calculation of the economic impact of IoT cyber risks, the analysis of risks and threats in power IoT, and the analysis of network data in an IoT environment. This underscores the significance of the RMF in ensuring robust security measures in the rapidly evolving IoT sector.

From the content, it is evident that the RMF is effectively utilized for risk management and information protection across diverse industrial sectors. A distinctive aspect of this research is its emphasis on the application of the RMF at a national policy level. While many studies have either concentrated on industry-specific applications or have not delineated their policy or geographical context, this gap is addressed by our research, which explores the application of the RMF from a national policy perspective. This unique focus not only enriches the existing body of knowledge but also offers a framework for nations considering the policy-based implementation of the RMF. The flexibility and broad applicability of the RMF are thus highlighted, with an expectation of a continued trend in this direction in the future.

Table 2. Application of the RMF in various industries as identified by research.

Industry	Research (Year)	Methods
Aviation and Defense	Robertson, J. et al. [25] (2021)	The RMF was used to meet information security requirements when designing a cloud-based computing framework.
	Kim, I. et al. [27] (2022)	Threat scenarios were concretized in simulation phase 1 linked with the RMF.
	Pearson, J. et al. [28] (2023)	The RMF was applied to resolve process disconnection issues within the cyber security group.
Automotive and Manufacturing	Haitao, Z. et al. [29] (2022)	TARA was improved based on the RMF to enhance efficiency and accuracy in automotive threat analysis and risk assessment.
	Chhawri, S. et al. [32] (2017)	The NIST RMF was applied to automotive use cases and used to automate automotive security tests.
	Thangavelu, S. et al. [33] (2020)	The conceptual process model needed for drone production was improved by referencing the conventional system threat approach and the RMF.
Environmental and Energy	Jiang, L. et al. [34] (2021)	The RMF was applied to the risk management of power systems, allowing for the measurement of security loss rates across various metrics.
	Miranda, A. W. et al. [35] (2017)	Loss rates for grid-connected commercial solar plants were calculated based on RMF control items.
	de Peralta, F. et al. [36] (2020)	A framework was proposed to identify security vulnerabilities in marine renewable energy systems and determine risks based on the RMF.
	Radoglou-Grammatikis, P. et al. [37] (2023)	The collAborative Risk assessMent sYstem (ARMY) was incorporated as a primary component for collaborative risk assessment, and risk evaluations were conducted using quantification techniques at various levels.
	Liatifis, A. et al. [38] (2023)	The system was modeled using attack–defense trees (ADT), and risk assessment, sensitivity analysis, optimization, and continuous monitoring and adjustment were conducted.
Medical and Health	Udroiu, A.M. et al. [39] (2022)	A methodology was presented that improves HITRUST based on the RMF to evaluate and enhance cyber security.
	Van Devender, M. S. et al. [44] (2023)	An RMF-based framework was introduced for threat and vulnerability assessments in the computing cybersecurity field of medical devices.
	Miller, J. C. [45] (2019)	A methodology was presented that uses the RMF for the security evaluation of cloud-based healthcare applications.
IoT	Radanliev, P. [47] (2018)	A new model for calculating the economic impact of IoT cyber risks was developed by applying established models such as Cyber Value at Risk and MicroMort to predict IoT risks.
	Li, K. et al. [48] (2020)	The RMF was used to collect and input information from each link of the power IoT system, initializing the process and evaluating risks at both organizational and system levels.
	Brandon, A. et al. [49] (2019)	The method of analyzing and managing the security of the IoT network using the RMF is explored, with a particular focus on the 'monitor' aspect.

3. RMF Application Method

In the trend of global digitization, efforts to implement the RMF have been consistently made by the K-MND after the signing of a cybersecurity cooperation agreement with the U.S. The RMF has been regarded as a key element for effectively responding to cyber threats and safely operating the main defense systems. However, the detailed methodology, particularly for the national security system (NSS), has not been disclosed, posing challenges to the detailed application of the RMF in Korea's defense system. To effectively apply the RMF to major defense systems, the K-MND developed a methodology focusing on the initial two stages of the RMF process mentioned in Section 2.1.

3.1. Categorize

In the first step, "Categorize", systems operated by the K-MND were categorized, and the importance and risk level of each system were assessed. Figure 1 depicts the K-MND's Categorize process, which was created based on the U.S. Categorize process.

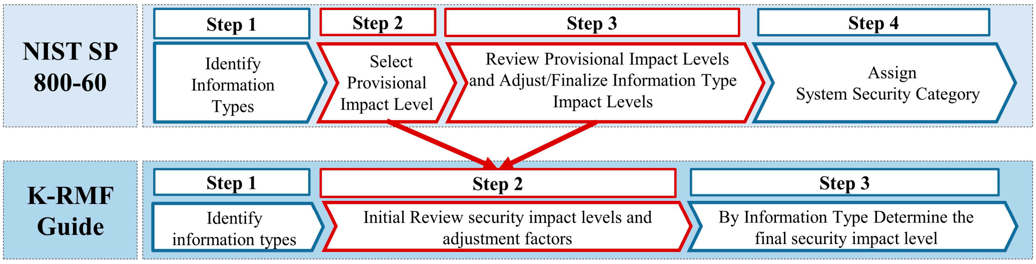

NIST SP 800-60
Step 1
Identify Information Types
Step 2
Select Provisional Impact Level
Step 3
Review Provisional Impact Levels and Adjust/Finalize Information Type Impact Levels
Step 4
Assign System Security Category
K-RMF Guide
Step 1
Identify information types
Step 2
Initial Review security impact levels and adjustment factors
Step 3
By Information Type Determine the final security impact level

Figure 1. The Republic of Korean National Defense Forces Categorize process, based on the U.S. Categorize process.

The U.S. Categorize process comprises four steps, detailed as follows:

1. Step 1. Identify Information Types
   * Identification of mission-based information types and identification of management and support information and legislative and administrative information obligations.
2. Step 2. Select Provisional Impact Level
   * Consideration of security objectives (confidentiality, integrity, and availability) and classification of provisional security impact levels.
3. Step 3. Review Provisional Impact Levels and Adjust/Final Inf. Ty. Imp. Levels
   * Review of the appropriateness of provisional impact levels based on organization, environment, mission, use, and data sharing.
   * Adjustment of target impact levels based on factors determining the security impact for classified information systems.
4. Step 4. Assign System Security Category
   * Review of security category classification for information types, identification, and determination of highest scores for each security objective (confidentiality, integrity, and availability).
   * Highest level adjustment for system security objectives.
   * Determination of the overall information system impact level based on the highest security impact level.

The K-MND simplified the U.S. Categorize process into three steps. Compared to the 4-step process of the U.S., Korea's approach defines the classification and security level of information systems concisely yet effectively as follows:

1. Step 1. Identify Information Types
   * Determination of types of information processed, stored, and transmitted by the system, documented, and reflected in the cybersecurity plan.
   * Classification by referring to the system security classification guide's mission domain (X type), job function (XX items), and information type (XXX items).
   * If information types not included in the system security classification guide are identified, the results are reviewed with the control and personnel departments and then reflected.
2. Step 2. Initial Review Security Impact Levels and Adjustment Factors
   * Comprehensive assessment and adjustment based on the size of the organization/institution, mission characteristics, system operating environment, etc.

* Review and adjustment considering factors such as whether the system processes, stores, or transmits classified or espionage information, whether it can be directly or indirectly accessed by foreigners, and whether it passes through a security domain.

3. Step 3. By Information Type, Determine the Final Security Impact Level
* Creation of a chart of security impact levels by information type, then determination of the final impact level by applying the HWM (High Water Mark) concept.

Several core reasons underlie these changes. The system of the K-MND reflects the specific domestic environment and mission characteristics, making it unsuitable to directly apply the U.S. approach. In Step 1, the focus is on identifying information types, and it comprehensively determines all types of information processed, stored, and transmitted in the system. While this is like the U.S.'s 'Identify Information Types' phase, the K-MND classifies information in more detail through X mission domains, XX job functions, and XXX information types. Table 3 provides an example of this, which is documented in the K-MND's system security classification guide. Within the table, C, I, and A represent confidentiality (C), integrity (I), and availability (A), respectively. Also, H, M, and L stand for high (H), medium (M), and low (L), respectively.

Table 3. Example of the criteria within the Republic of Korea National Defense Forces System security guide.

Behavior	**Duty Function**	**Information Type**	**Initial Security Impact**		
			C	**I**	**A**
Defense policy and planning	Defense policy	National security	H	H	H
		International policy	M	M	M
	...	...	...	...	...
...	...	...	...	...	...

In the U.S. approach, there are two stages: 'Step 2. Select Provisional Impact Level' and 'Step 3. Review Provisional Impact Levels and Adjust/Final Inf. Ty. Imp. Levels'. However, the K-MND has integrated these two processes into one step titled 'Initial Review Security Impact Levels and Adjustment Factors'. This integration helps enhance the efficiency of the procedure and reduces redundancy by addressing the initial assessment and adjustments of security impact in one process.

The 'By Information Type Determine the Final Security Impact Level' step by K-MND is like the U.S.'s 'Assign System Security Category', determining the security impact level for each type of information. Yet, the K-MND integrates the HWM concept, further clarifying the overall impact level of the system.

The modification to the K-MND's Categorize procedure is intended to provide an efficient approach aligned with Korea's defense system and information system environment. Through this, the RMF can be tailored to its specific environment and requirements, enabling more effective evaluation and management of the system's security level. Other countries required to apply the RMF can also adjust it, like the K-MND, reflecting their specific environment and mission characteristics and referring to their system security classification guide.

After altering the Categorize procedure, measures for first class, second class, and three class are selected according to the system where the RMF will be applied. This is Step 1. Identify Information Types. Table 4 sets the criteria for selecting these classes. An example of information types derived from the criteria of Table 4 is seen in Table 5. Information Type in Table 5 lists measures by Class, and Initial Security Impact Level measures the security impact level for each measure based on the C, I, and A rules. Lastly, the Reasons for choosing an information type documents the rationale behind selecting that Information Type.

Table 5 displays the preliminary results of selecting information types for the system where the RMF will be applied. After determining the information types, Step 2. Initial

Review Security Impact Levels and Adjustment Factors designates the security impact levels for each information type and details the reasons for their selection. This table explicitly lists the initial classification and its selection rationale, particularly presenting the security impact levels in the essential C, I, and A domains. This initial categorization will be utilized as a significant reference point in the subsequent process of reviewing and adjusting security impact levels. For instance, in the 'Defensive support' category, subcategories such as 'Command communications' and 'Defense System Integration' are classified as 'H' (High). Such judgments consider that these systems play a crucial role in exchanging information across various platforms and accurately sharing scenarios in the defense domain.

Table 4. Criteria for selecting the first class, second class, and third class tailored to a specific defense system.

Class	Criteria
First Class	- Referenced the system development plan and the system security classification guide of the OO system. - Judgment is based on the "information processed, stored, and transmitted by the system". - From the measures classified into X major mission areas, focusing on matters necessary for defense operations, mission areas related to the OO system were selected.
Second Class	- From the measures classified into XX duty function, emphasizing matters necessary for defense operations, duty functions related to the OO system were chosen. - Select from second class items, which are subcategories of the measures selected in the first class.
Third Class	- From the selected sub-categories, it is necessary to choose the required third class.

Table 5. Example results of the initial information type selection for systems applying the RMF.

Information Type			Initial Security Impact Level			Reasons for Choosing an Information Type
First Class	Second Class	Third Class	C	I	A	
Defensive support	Command communications	Defense networks	H	H	H	An exchange of information with various systems is required.
		...	...	...	...	...
...	...	...	...	...	...	...

Following the designation of initial security impact levels for the selected information types, as shown in Table 5, next is Step 2. Initial Review Security Impact Levels and Adjustment Factors progresses with adjusting the security impact levels. This adjustment considers organizational features, mission characteristics, etc., to modify the security impact level of the system where the RMF will be applied. The adjusted results are presented in Table 6. Information Type is documented up to the third Class, and the Adjusted Security Impact Level notes the revised security impact level. The reason for this adjustment is penned in the Security Impact Level Adjustment Factor. Lastly, supporting documents and page numbers for these reasons are recorded in the references section.

Subsequently, "Step 3. By Information Type Determine the Final Security Impact Level" is executed. Once all of the security impact levels in Table 6 are fixed, the Categorize procedure is deemed complete. Table 6 not only presents an adjusted understanding of security impact levels but also elaborates in detail on various considerations and criteria that influenced such adjustments. This demonstrates that the process of evaluating and re-evaluating the security level of a system where the RMF is applied should be repeatedly and meticulously conducted, ensuring that all possible vulnerabilities and nuances are properly addressed.

Table 6. Example adjustments of security impact levels for systems applying the RMF.

Information Type	Initial Security Impact Level			Security Impact Level Adjustment Factor	References
Third Class	C	I	A		
Defense networks	M	M	H	C: Due to the small operational organizational size of the 00 system and the information being classified as a defense level 2 secret, it is assessed that the impact level of confidentiality breaches is relatively low, and the ripple effect is not deemed fatal; thus, it is adjusted to 'Medium'. I: Unauthorized modifications or destruction of information within the 00 system are not deemed to have a fatal adverse impact on the operational/mission performance of the related organization; therefore, it is adjusted to 'Medium'. A: Due to the time-sensitive nature of interruptions or delays in accessing information within the 00 system, it is maintained at 'High'.	XX guide p. 27
...	...	...	...	...	...

3.2. Select

In the second phase, "Select," keywords are extracted from the system where the RMF will be applied, based on the information types listed in Table 6, which was created during the 'Categorize' phase. On this basis, security control items are overlaid. Subsequently, security control item tailoring is conducted, and a final selection is made.

In the 'Select' phase of the RMF, 'overlay' is used as a tool to choose standard security control items and is used either to strengthen, modify, or replace them. Such overlays contribute to optimizing security controls, reflecting the specific requirements and risk factors of an organization or environment. The following main considerations exist during the overlay application process:

1. Setting security policies, standards, and detailed specifications (parameters) for security control items defined by each military and agency.
2. Clarification of the adjustment process through supplementary explanations.
3. Limiting the use of the respective security control items within given basic assumptions.
4. Recognizing potential conflicts when using various overlays simultaneously and resolving them through consultation with the security authorizing official.

The application of overlays aids in implementing standardized security functions consistently and economically. Justifications and interpretations for any added or removed security control items to supplement the baseline must also be provided. Moreover, the rationale for control item selection, tailoring descriptions, common control items, assumptions, etc., should be explicitly expressed to assist in implementation. When applying an overlay to a system, the specific characteristics of that system must be considered. Procedures must be meticulously defined when distinguishing between main and auxiliary equipment and when integrating with other systems. Also, considerations such as defensive operational levels, the value of information, the mission-critical importance of the system, and the severity of potential system damage must be included.

NIST's SP 800-53 extensively covers such overlays [18]. Customized controls reflect the specific requirements and risk factors of an organization, enhancing the efficiency of security risk management. However, the U.S. does not disclose all overlay items. While CNSSI 1253 Attachments contain overlay templates up to E 1, E 2, F 3, F 4, F 5, and F 6, only

CNSSI 1253 Attachments E 1: Security Overlays Template and CNSSI 1253 Attachments F 5: Classified Information Overlay are publicly available [23]. To overcome this, this paper proposes a keyword-based overlay application method. First, the characteristics of the system are identified, and overlays are applied according to these characteristics, with keywords being researched. When describing relevant information for a specific system where the RMF will be applied and extracting keywords, they can be extracted as in Table 7. The extracted keywords are emphasized in red.

Table 7. Details and keywords of systems applying the RMF.

Item	Detail
General description	A standard data transmission communication system used to share tactical data (defense secret information, Class II) between reconnaissance assets, command and control, and defense systems and to conduct defensive operations.
Interlocking form	Integrates with vehicle defense systems and Vehicle C4I (command, control, communications, computers, and intelligence) platforms.
...	...

Keywords, as extracted in Table 7, can be added depending on the characteristics of the system, and their inclusion can be discussed with the security authorizer. Furthermore, detailed keywords can be extracted from these main keywords as shown in Table 8.

Table 8. Detailed keywords of systems applying the RMF.

Main Keyword	Detailed Keyword
Secret	For security control items required by systems involving password creation and authentication, handling classified information and materials, maintaining and repairing classified systems, and authorization, search the keyword ⇒ Secret.
Interlocking	For security control items required by systems that operate or feature domain interconnection approvals and restrictions, interconnection agreements, and interconnection security control equipment, search the keywords ⇒ Interconnection, Interface, Network, and NAC.
...	...

Detailed keywords are designed to be extracted based on each main keyword, allowing security control items to be more effectively searched for and identified. For instance, the main keyword "Secret" is utilized to locate security control items in systems such as password creation and authentication, the processing of classified information and data, the maintenance and repair of classified systems, and authorization. Similarly, the other main keywords are employed to search for security control items that include detailed keywords depending on each situation and need. The main keywords and their corresponding detailed keywords can be summarized as in Table 8. Every time detailed keywords are extracted, continuous reviews are received from the security authorizer, and the process is repeated. With each repetition, the number of located security control items continuously decreases. This process is repeated either until the security authorizer stops the repetition or until there comes a point where no more keywords are added, and this can be depicted as shown in Figure 2.

The extracted detailed keywords are used as essential parameters for searching security control items for overlay. Using the detailed keywords identified in Table 8, all security control items in the NIST documents where security control items are described were searched. In this process, documents are thoroughly reviewed for each keyword, ensuring that security requirements or regulations related to each keyword are accurately identified. The security control items extracted through the search process are diverse and can be extracted as shown in Table 9. Table 9 displays the security control items searched based on each keyword, reflecting the diversity and importance of security requirements for interoperability.

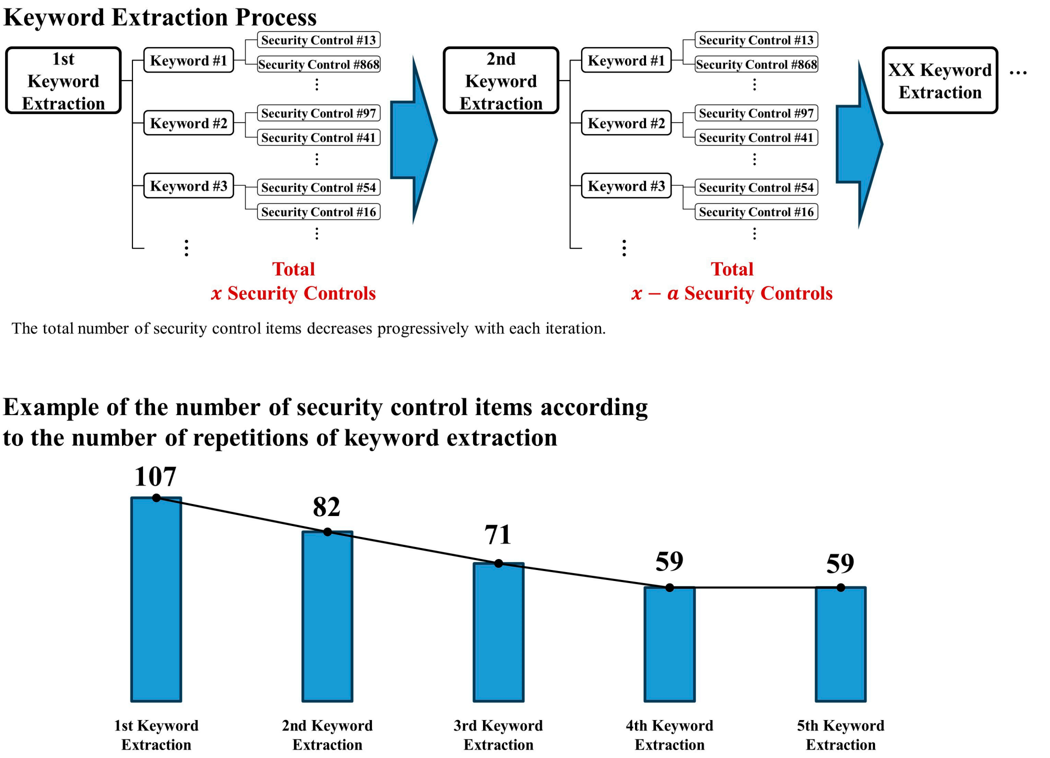


Figure 2. Keyword extraction process and the number of security control items convergence graph.

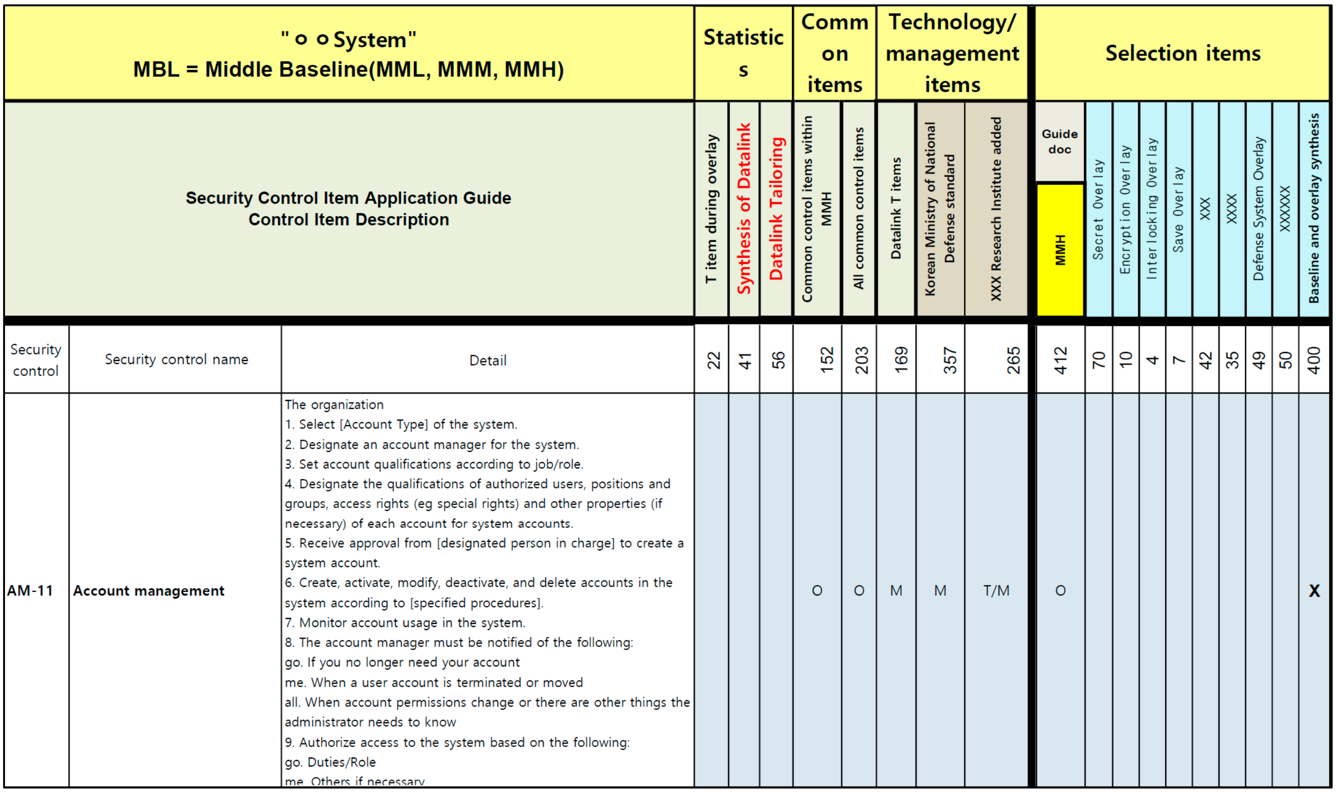
Table 9. Example of security control overlay.

Keyword	Document/ Security Control	Detail	DoD RMF
Secret	Secret Guide/SP-3-35 (continuation of essential functions)	Essential functions must be maintained until the site is fully restored.	CP-2(5)
	...	...	...
...	...	...	...

Table 9 is a table that systematically classifies and summarizes security-related keywords. The 'Keyword' column reflects the detailed keywords previously extracted in Table 8. Subsequently, in the 'Document/Security control' column, the name of the relevant document or guide is initially mentioned, followed by a detailed recording of the reference number of the security control items mentioned within that document or guide. In the 'Detail' column, the core content of the security control items referenced in the document or guide is succinctly yet clearly described. The last 'DoD RMF' column notes the reference number corresponding to the security control item within the DoD's RMF. However, it should be noted that not all items are explicitly listed in the DoD RMF. Some items might not have been publicly disclosed by the DoD or might not have been included in the DoD RMF due to the uniqueness of certain countries or systems. In such cases, it can be interpreted that the item has been written in a more detailed manner than the U.S. security standards, making additional concerns unnecessary.

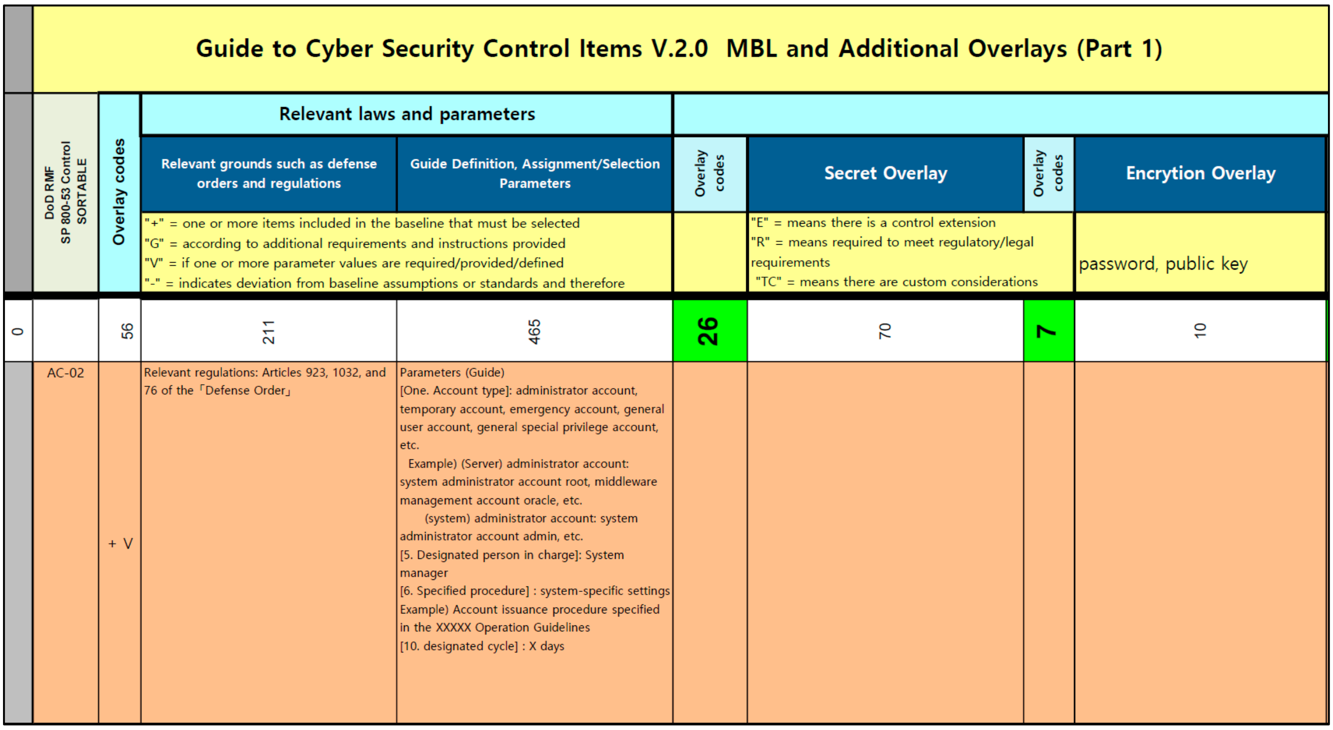
'Tailoring' refers to the process of customizing security control items according to the operational requirements, constraints, or special environmental conditions of a specific system. This process is essential for the effective application of security control items. In actual operational environments, generic security control items may not be suitable for all systems. Therefore, tailoring, adjusting, modifying, or removing those measures to build an optimized security environment tailored to the organization's actual situation is crucial. Once tailoring is complete, a systematic review of the suitability of the selected security control items is needed. Firstly, items that should be commonly applied from the basic security control item baseline are identified and designated. In the next step, if the baseline assumptions set initially change, those items are reviewed again and, if necessary, modified or excluded. Subsequently, items that might cause adverse effects or side effects when applied to the actual system based on technical characteristics and mission requirements are identified, and these are replaced or modified with other security control items. This tailoring strictly follows NIST 800-53.

The U.S. FedRAMP provides a template for overlay and tailoring. This template, used in various pieces of research from 2019 to 2023, is very popular [50–58]. Moreover, the template assists in systematically recording considerations for implementation by specifying the criteria for overlay application, setting goals for additional security control items, explaining related regulations and laws, and detailing tailoring considerations. The K-RMF Baseline, Overlay, and Tailoring Tool was produced based on this FedRAMP template, and this is illustrated in Figures 3–5.



" o o System" MBL = Middle Baseline(MML, MMM, MMH)			Statistics			Common items		Technology/ management items			Selection items									
Security Control Item Application Guide Control Item Description			T item during overlay	Synthesis of Datalink	Datalink Tailoring	Common control items within MMH	All common control items	Datalink T items	Korean Ministry of National Defense standard	XXX Research Institute added	Guide doc MMH	Secret Overlay	Encryption Overlay	Interlocking Overlay	Save Overlay	XXX	XXXX	Defense System Overlay	XXXXXX	Baseline and overlay synthesis
Security control	Security control name	Detail	22	41	56	152	203	169	357	265	412	70	10	4	7	42	35	49	50	400
AM-11	**Account management**	The organization 1. Select [Account Type] of the system. 2. Designate an account manager for the system. 3. Set account qualifications according to job/role. 4. Designate the qualifications of authorized users, positions and groups, access rights (eg special rights) and other properties (if necessary) of each account for system accounts. 5. Receive approval from [designated person in charge] to create a system account. 6. Create, activate, modify, deactivate, and delete accounts in the system according to [specified procedures]. 7. Monitor account usage in the system. 8. The account manager must be notified of the following: go. If you no longer need your account me. When a user account is terminated or moved all. When account permissions change or there are other things the administrator needs to know 9. Authorize access to the system based on the following: go. Duties/Role me. Others if necessary				O	O	M	M	T/M	O									**X**

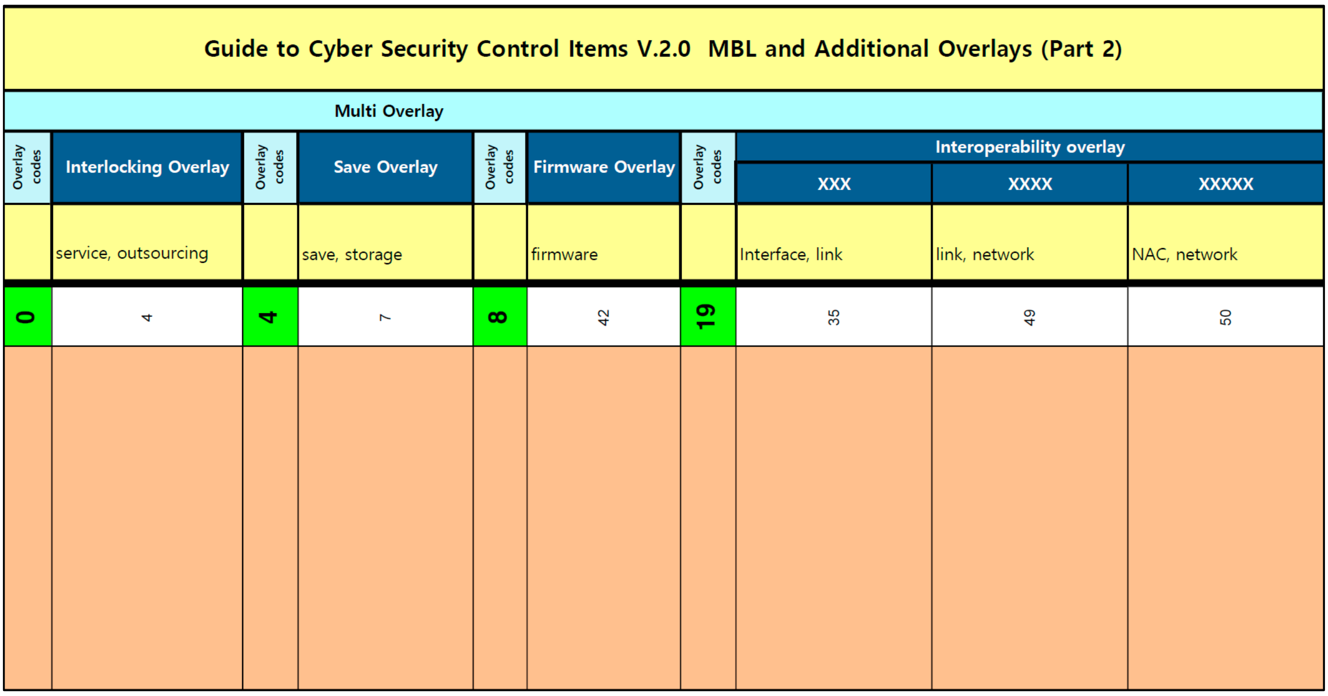
Figure 3. K-RMF Baseline, Overlay, and Tailoring Tool—part 1.



Guide to Cyber Security Control Items V.2.0 MBL and Additional Overlays (Part 1)

			Relevant laws and parameters					
	DoD RMF SP 800-53 Control SORTABLE	Overlay codes	Relevant grounds such as defense orders and regulations	Guide Definition, Assignment/Selection Parameters	Overlay codes	Secret Overlay	Overlay codes	Encrytion Overlay
			"+" = one or more items included in the baseline that must be selected "G" = according to additional requirements and instructions provided "V" = if one or more parameter values are required/provided/defined "-" = indicates deviation from baseline assumptions or standards and therefore			"E" = means there is a control extension "R" = means required to meet regulatory/legal requirements "TC" = means there are custom considerations		password, public key
0		56	211	465	26	70	7	10
	AC-02	+ V	Relevant regulations: Articles 923, 1032, and 76 of the「Defense Order」	Parameters (Guide) [One. Account type]: administrator account, temporary account, emergency account, general user account, general special privilege account, etc. Example) (Server) administrator account: system administrator account root, middleware management account oracle, etc. (system) administrator account: system administrator account admin, etc. [5. Designated person in charge]: System manager [6. Specified procedure] : system-specific settings Example) Account issuance procedure specified in the XXXXX Operation Guidelines [10. designated cycle] : X days				

Figure 4. K-RMF Baseline, Overlay, and Tailoring Tool—part 2.



Guide to Cyber Security Control Items V.2.0 MBL and Additional Overlays (Part 2)

Multi Overlay									
Overlay codes	Interlocking Overlay	Overlay codes	Save Overlay	Overlay codes	Firmware Overlay	Overlay codes	Interoperability overlay		
							XXX	XXXX	XXXXX
	service, outsourcing		save, storage		firmware		Interface, link	link, network	NAC, network
0	4	4	7	8	42	19	35	49	50

Figure 5. K-RMF Baseline, Overlay, and Tailoring Tool—part 3.

Figures 3–5 are represented as a single table, and the main content of this table is designed to visually demonstrate how various security control items are applied to the system. To achieve this, multiple stages and classification methods were utilized to present the importance and application method of each item in detail:

1. MBL (Middle Baseline)
   * The 'Middle Baseline' defines the baseline for the security control items of the system.
   * This baseline is divided into three categories, namely MML, MMM, and MMH, to reflect the various levels and complexities of security requirements.
2. Modification and application process of security control items
   * In the center of the table, the modification process of the security control items is sequentially presented. This process is carried out through overlays, tailoring, and various reviews.
3. Detailed security control items guide
   * The 'AM'11' item, provided as an example, elaborates in detail on account management.
   * Each item includes the purpose and method of a specific security control task, as well as related parameters or examples, offering guidance on how they should be applied in real-world environments.
4. Interpretation of symbols and codes
   * The various symbols and codes included in the table represent the characteristics and requirements of the security control items. These symbols clearly indicate under what conditions each item should be selected or applied.
5. Related legislation and guidelines
   * On the right side of the table, legislation, regulations, and guidelines related to each security control item are provided. This enables users to verify the legal requirements that each item must meet.

Overall, the table visualized in Figures 3–5 offers a comprehensive guideline for systematically managing and applying the security requirements and control items of the system, which can effectively enhance the system's security. Through this research, the following implications were drawn regarding the important points discovered during the adjustment process of security control items:

Firstly, the significant difference between the number of security control items initially set and the number of items finally determined emphasizes the importance of a dynamic approach. This discrepancy highlights not just the need for security controls but also the necessity to reevaluate and adjust according to specific environments and conditions.

Secondly, items added through the overlay process underscore the importance of meticulous consideration for specific environments and conditions. However, the fact that not all added items are included in the final security control items emphasizes the need not just for an increase in items but for the effective optimization of these items.

Thirdly, the importance of a systematic approach, which continually reviews how each item relates to the overall security strategy, rather than just considering security control items in numerical terms, is highlighted.

Lastly, the tailoring process of adjusting standard security control items according to the characteristics of the organization reaffirms the essential role of this process in enhancing the efficiency and effectiveness of security strategies. The insights drawn are expected to assist other organizations in building more fortified security strategies when setting and adjusting security control items.

4. Experiments and Results

In this chapter, the methodology explained in Section 3 was directly applied to the K-MND's OO system from the 'Categorize' to 'Select' phase, and its results were derived. The 'Categorize' phase was initially conducted. Based on the criteria in Table 4, the information type was derived as in Table 10. As a result, when extracting the information type of the K-MND's OO system, a total of 445 information types were identified, and the HWM's Security impact level for C, I, and A was determined to be H, H, and H, respectively.

Table 10. Part of the initial selection result of the OO system information type.

Information Type			Initial Security Impact Level			Reasons for Choosing an Information Type
First Class	**Second Class**	**Third Class**	**C**	**I**	**A**	
Defensive support	Command communications	Defense networks	H	H	H	An exchange of information with various systems is required.
		Defense system integration	H	H	H	Sharing of the situation in the defense area is needed.
	Sharing information	Data exchange	L	L	L	A function to share information about the defense area with defenders is necessary.
. . .	. . .	. . .	. . .	. . .	. . .	. . .
Initial System Security Classification			H	H	H	Apply the HWM

Subsequently, the results of adjusting the security impact level are represented in Table 11. Considering the small operational scale of the system to which the RMF is applied, and the characteristics of the information classified as a level 2 secret, the 'Defense networks' category was adjusted from 'High' to 'Medium' in the C and I sectors. However, considering the time-sensitivity of information access, the A sector remained 'High'. Similarly, the 'Defense System Integration' category was adjusted from 'High' to 'Medium' in the C and I sectors but remained 'High' in the A sector. On the other hand, categories like 'Data Exchange' retained their initial 'Low' classification across all sectors. Consequently, after adjusting the information type of the K-MND's OO system as in Table 11, the items were adjusted from the original 445 to 412, and the HWM's security impact level for C, I, and A was adjusted to M, M, and H, respectively.

Upon completion of Table 11, the 'Categorize' phase is concluded, and the process enters the 'Select' phase. Firstly, the 'Overlay' is carried out. As described in Table 7, the characteristics of the OO system are understood, and based on this, the overlay features are recognized as in Table 12 and relevant keywords are extracted.

After extracting the main keywords, detailed keywords related to them are extracted. Through the process depicted in Figure 2, security control items are searched and then extracted as shown in Table 13. Table 13 displays the number of security control items derived from repeated extractions of the keyword 'encryption'. Similar procedures were conducted for other keywords. The classification code for the security control item is based on NIST 800-53, and one can observe how access control (AC) and system and communication protection (SC) change each time a keyword is repeatedly extracted. Such repetitive extractions continued until no more security control items could be added. This process was conducted under the approval of the security authority. In total, the keyword extraction was repeated five times, resulting in 33 security control items for the 'encryption' keyword. The keyword 'storage' was repeated five times, resulting in 14 security control items, as shown in Figure 6. After extracting security control items for other keywords and removing duplicates, 44 items were identified. Combining these with the items derived from Table 11 resulted in a total of 456 security control items.

Applying the tailoring described in Section 3.2 to the OO system, out of the 456 security control items identified through the overlay, 56 were optimized through tailoring, leaving 400 security control items selected in the end. This showcases how tailoring can optimize security measures in line with an organization's specific characteristics and requirements. The process of modifying the security control items proceeded from the 'Categorize' phase to the 'Select' phase, with the results visually presented in Figure 7. The baseline security control items initially set numbered 445. However, the first review reduced this by 33 based on specific conditions and requirements, bringing the count down to 412. Subsequent overlay processes added 44 more, totaling 456. Finally, considering the actual environment and requirements of the organization, tailoring further optimized 56 items, leaving 400 in the end.

Table 11. Partial results of information type adjustment choices for the OO system.

Information Type	Initial Security Impact Level			Security Impact Level Adjustment Factor	References
Third Class	C	I	A		
Defense networks	M	M	H	C: Due to the small operational organizational size of the 00 system and the information being classified as a level 2 defense secret, it is assessed that the impact level of confidentiality breaches is relatively low, and the ripple effect is not deemed fatal; thus, it is adjusted to 'Medium'. I: Unauthorized modifications or destruction of information within the 00 system are not deemed to have a fatal adverse impact on the operational/mission performance of the related organization; therefore, it is adjusted to 'Medium'. A: Due to the time-sensitive nature of interruptions or delays in accessing information within the 00 system, it is maintained at 'High'.	XX guide p. 27
Defense System Integration	M	M	H	C: The impact level of breaches in confidentiality of the information within the 00 system, based on the organizational size or mission characteristics, is judged to be relatively low and not deemed to have a fatal ripple effect; therefore, it is adjusted to 'Medium'. I: Although unauthorized modifications to the information within the 00 system could significantly affect defensive operations, sharing of defense area information is possible through the defense data communication system, meaning that it is not deemed to have a fatal adverse impact on the operational/mission performance of the related organization; thus, it is adjusted to 'Medium'. A: Information on the defense area within the 00 system is time-sensitive, and the results of access interruptions or delays are time-sensitive; hence, it remains at 'High'.	Defense guide p. 66
Data Exchange	L	L	L	C: No adjustment required. I: No adjustment required. A: No adjustment required.	Exchange guide p. 59
...	...	...	...	...	...
Adjusted System Security Classification	M	M	H	Apply the HWM	Security Guide p. 83

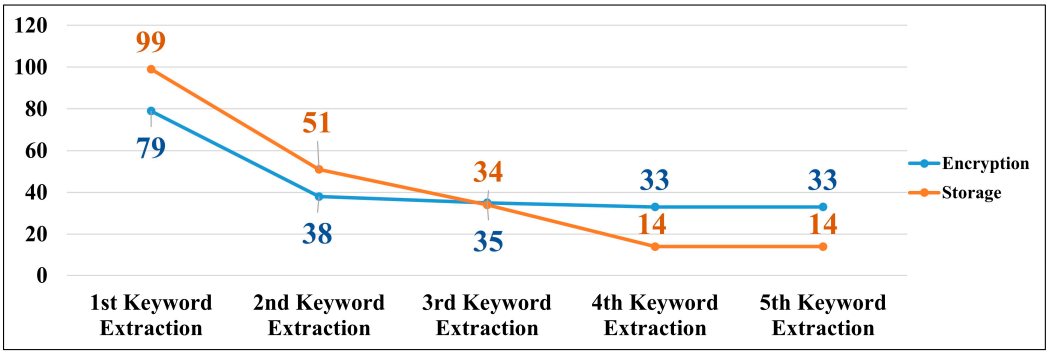


Figure 6. The number of security control items that were repeatedly searched for encryption keywords and storage keywords.

Table 12. Partial Details and Keywords of the OO System.

Item	Detail
General description	A standard data transmission communication system used to share tactical data (defense secret information, Class II) between reconnaissance assets, command and control, and defense systems and to conduct defensive operations. => Security
Transmission method	Time division multiple access (TDMA)
Maximum number of subscribers	Supports simultaneous subscription across X networks and can handle up to XXX subscribers.
Radio distance	20,000 km
Message format	Supports Y and Z message formats.
Interlocking structure	Components include a data link processor, encryption equipment, data link, terminal device, communication gear, storage devices, antennas, and more. => Encryption, Storage
Interlocking form	Integrates with vehicle defense systems and Vehicle C4I (command, control, communications, computers, and intelligence) platforms. => Interlocking
...	...

Table 13. Number of security control items retrieved by repeated searches with the encryption keywords.

Repetition Number	Security Control Code	Number of Security Control Items Retrieved
1	AC	21
	SC	17
	...	...
	Total	79
2	AC	13
	SC	7
	...	...
	Total	38
3	AC	13
	SC	5
	...	...
	Total	35
4	AC	14
	SC	6
	...	...
	Total	33
5	AC	14
	SC	6
	...	...
	Total	33

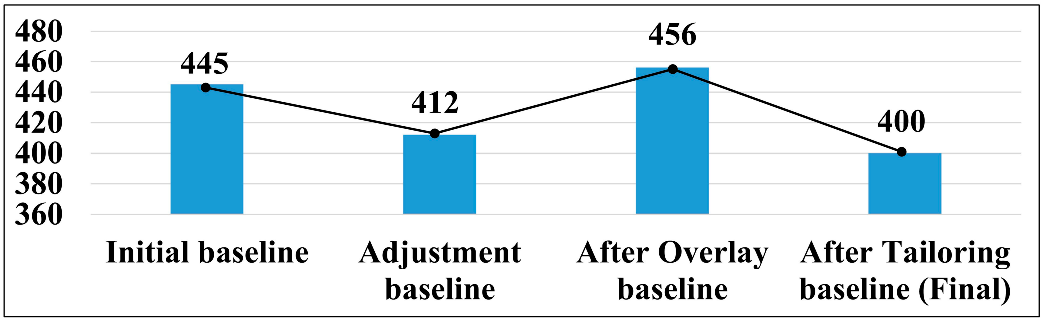


Figure 7. Security control item modification from the 'Categorize' to 'Select' stages.

5. Conclusions

This research conducted an in-depth investigation into how the RMF is utilized across various industries. It confirmed that the RMF can be effectively applied across a broad spectrum of fields, not just confined to specific ones. Section 3 introduced the importance and methodology of systematically adjusting and optimizing security control items. Section 4 applied the methodology from Section 3 using the K-MND OO system as an example. This paper does not provide all keyword items or figures, showcasing only some or providing examples. Detailed information remained confidential, but the methodology was detailed enough for readers to understand and apply the RMF. The difference between the initial setup and final decision for security items emphasized the importance of dynamic approaches and condition-specific adjustments. The research emphasized efficient optimization, not just an increase in security items, by combining overlay and tailoring approaches. For the first time, this research presented a keyword-based overlay application method, which is usable even if the CNSSI 1253 overlay template is not publicly available. This methodology provides opportunities for countries that cannot access CNSSI 1253. Secondly, the K-RMF Baseline, Overlay, and Tailoring Tool served as a convenient tool for systematically managing security requirements and control items. This research's outcomes are expected to aid other organizations or countries in enhancing their security strategies.

Future research aims to analyze the 'Implement' and 'Assess' phases in detail, verifying the effectiveness of the RMF and optimized security items across various systems and environments. In conclusion, using the OO system as an example, the systematic and detailed RMF application method presented in this paper is the path to maximizing security efficiency and effectiveness while also enhancing the ability to respond to real operational environment security threats and vulnerabilities. Furthermore, the RMF can also be utilized in developing next-generation security solutions, educational and training programs, and improving business processes.

Author Contributions: Conceptualization, G.J., K.K., S.Y. and J.K.; funding acquisition, J.K.; methodology, G.J., K.K., S.Y. and D.S.; supervision, J.K.; validation, D.S.; writing—original draft, G.J. and K.K.; writing—review and editing, J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Future Challenge Defense Technology Research and Development Project (9129156) hosted by the Agency for Defense Development Institute in 2020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Manulis, M.; Bridges, C.P.; Harrison, R.; Sekar, V.; Davis, A. Cyber security in new space: Analysis of threats, key enabling technologies and challenges. *Int. J. Inf. Secur.* **2021**, *20*, 287–311.
2. Dunn Cavelty, M.; Wenger, A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemp. Secur. Policy* **2020**, *41*, 5–32.
3. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
4. Force, J.T. Risk management framework for information systems and organizations. *NIST Spec. Publ.* **2018**, *800*, 37.
5. Sherman, J.B. *DoD Instruction 8510.01 Risk Management Framework for DoD Systems*; Department of Defense: Arlington County, VA, USA, 2022.
6. Gorman, C.N. *DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued from August 1, 2015 through July 31, 2016 (REDACTED)*; Department of Defense: Arlington County, VA, USA, 2016.
7. Odell, L.A.; DePuy, C.E.; Fauntleroy, J.C.; Rabren, T.C.; Seitz-McLeese, M.G. *Recommendations for Improving Agility in Risk Management for Urgent and Emerging Capability Acquisit—Ns—Quick Look Report*; JSTOR: Alexandria, VA, USA, 2017.
8. Commanders, C.; Defense, U.; Defense, A. *Subject: DoD Information System Certification and Accreditation Reciprocity*; Department of Defense: Washington, DC, USA, 2003.
9. Landree, E.; Gonzales, D.; Ohlandt, C.; Wong, C. *Implications of Aggregated DoD Information Systems for Information Assurance Certification and Accreditation*; RAND: Santa Monica, CA, USA, 2010.
10. Hutchison, S.J. Cybersecurity: Defending the new battlefield. *Def. AT&L* **2013**, *42*, 34–39.
11. Ross, R. Managing enterprise security risk with NIST standards. *Computer* **2007**, *40*, 88–91. [CrossRef]
12. Combass, T.; Shilling, A. Integrating cybersecurity into NAVAIR OTPS acquisition. In Proceedings of the 2016 IEEE AUTOTEST-CON, Anaheim, CA, USA, 12–15 September 2016; pp. 1–5.
13. Teresa, M.T. *DoDI 8500.01 Cybersecurity*; Department of Defense: Arlington County, VA, USA, 2014.
14. Joint Task Force Transformation Initiative. *SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View*; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2011.
15. Ross, R. NIST SP 800-37, Revision 1. In *Guide for Applying the Risk Management Framework to Federal Information Systems*; NIST: Gaithersburg, MD, USA, 2010.
16. Committee on National Security Systems. *IA Risk Management Policy for NSS*; Committee on National Security Systems: Fort Meade, MD, USA, 2021.
17. Stoneburner, G.; Goguen, A.; Feringa, A. NIST Special Publication 800-30. In *Risk Management Guide for Information Technology Systems*; NIST: Gaithersburg, MD, USA, 2001.
18. NIST. NIST SP 800-53. In *Recommended Security Controls for Federal Information Systems*; NIST: Gaithersburg, MD, USA, 2003; pp. 800–853.
19. Ross, R.; Johnson, A.; Katzke, S.; Toth, P.; Stoneburner, G.; Rogers, G. *Nist Special Publication 800-53a: Guide for Assessing the Security Controls in Federal Information Systems*; Tech. Rep.; NIST: National Institute of Standards and Technology, US Department Commerce: Gaithersburg, MD, USA, 2008.
20. Dempsey, K.; Chawla, N.S.; Johnson, A.; Johnston, R.; Jones, A.C.; Orebaugh, A.; Scholl, M.; Stine, K. *Nist Special Publication 800-137: Information Security Continuous Monitoring (iscm) for Federal Information Systems and Organizations*; Tech. Rep.; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
21. Stine, K.; Rich, K.; Barker, C.; Fahlsing, J.; Gulick, J. NIST SP. 800-60 Rev 1. In *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST: Gaithersburg, MD, USA, 2008.
22. Ross, R.; McEvilley, M.; Winstead, M. *NIST SP 800-160 Volume 1 Revision 1 Engineering Trustworthy Secure Systems Initial Public Draft*; NIST: Gaithersburg, MD, USA, 2022.
23. Committee on National Security Systems. *Categorization Baselines NSS Assignment Values*; Committee on National Security Systems: Fort Meade, MD, USA, 2022.
24. Committee on National Security Systems. *CNSS Instruction 4009*; Committee on National Security Systems: Fort Meade, MD, USA, 2010.
25. Robertson, J.; Fossaceca, J.M.; Bennett, K.W. A cloud-based computing framework for artificial intelligence innovation in support of multidomain operations. *IEEE Trans. Eng. Manag.* **2021**, *69*, 3913–3922. [CrossRef]
26. Explore Our Products. Available online: https://www.aws.com (accessed on 28 August 2023).
27. Kim, I.; Kim, S.; Kim, H.; Shin, D. Mission-Based Cybersecurity Test and Evaluation of Weapon Systems in Association with Risk Management Framework. *Symmetry* **2022**, *14*, 2361. [CrossRef]
28. Pearson, J.; Oni, O. Addressing cybersecurity and safety disconnects in United States army aviation: An exploratory qualitative case study. *Secur. J.* **2023**, 1–17. [CrossRef]
29. Zhang, H.; Luo , L.; Li, R.; Yi, J.; Li, Y.; Chen, L. Research and application of intelligent vehicle cybersecurity threat model. In Proceedings of the 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), Guilin, China, 11–13 July 2022; pp. 102–109. [CrossRef]
30. Wynn, J.; Whitmore, J.; Upton, G.; Spriggs, L.; McKinnon, D.; McInnes, R.; Clausen, L. *Threat Assessment & Remediation Analysis (TARA) (No. MTR110176)*; MITRE: Bedford, MA, USA, 2011.

31. Qi, Y.; Yang, G.; Liu, L.; Fan, J.; Orlandi, A.; Kong, H.; Yu, W.; Yang, Z. 5G over-the-air measurement challenges: Overview. *IEEE Trans. Electromagn. Compat.* **2017**, *59*, 1661–1670. [CrossRef]
32. Chhawri, S.; Tarnutzer, S.; Tasky, T.; Lane, G.R. Smart Vehicles, Automotive Cyber Security & Software Safety Applied to Leader-Follower (LF) and Autonomous Convoy Operations. In Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), Novi, MI, USA, 8–10 August 2017.
33. Thangavelu, S.; Janczewski, L.; Peko, G.; Sundaram, D. A Dynamic Security-dedicated Approach to Commercial Drone Vulnerabilities, Threat Vectors and Their Mitigation. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 1054–1059.
34. Jiang, L.; Shao, L.; Qiu, Y.; Zhou, L. A Risk Management Model for Power Industry based on Impact Analysis. In Proceedings of the 2021 2nd International Conference on Big Data Economy and Information Management (BDEIM), Sanya, China, 3–5 December 2021; pp. 159–163.
35. Miranda, A.W.; Goldsmith, S. Cyber-physical risk management for PV photovoltaic plants. In Proceedings of the 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23–26 October 2017; pp. 1–8.
36. de Peralta, F.; Gorton, A.; Watson, M.; Bays, R.; Boles, J.; Castleberry, J.; Gorton, B.; Powers, F. *Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems*; National Technical Information Service: Alexandria, VA, USA, 2020.
37. Radoglou-Grammatikis, P.; Liatifis, A.; Dalamagkas, C.; Lekidis, A.; Voulgaridis, K.; Lagkas, T.; Fotos, N.; Menesidou, S.-A.; Krousarlis, T.; Alcazar, P.R. ELECTRON: An Architectural Framework for Securing the Smart Electrical Grid with Federated Detection, Dynamic Risk Assessment and Self-Healing. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, 29 August–1 September 2023; pp. 1–8.
38. Liatifis, A.; Alcazar, P.R.; Grammatikis, P.R.; Papamartzivanos, D.; Menesidou, S.; Krousarlis, T.; Alberto, M.M.; Angulo, I.; Sarigiannidis, A.; Lagkas, T.; et al. Dynamic Risk Assessment and Certification in the Power Grid: A Collaborative Approach. In Proceedings of the 2022 IEEE 8th International Conference on Network Softwarization (NetSoft), Milan, Italy, 27 June–1 July 2022; pp. 462–467.
39. Udroiu, A.-M.; Dumitrache, M.; Sandu, I. Improving the cybersecurity of medical systems by applying the NIST framework. In Proceedings of the 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Ploiesti, Romania, 30 June–1 July 2022; pp. 1–7.
40. Alliance, H. *HITRUST CSF*; HITRUST: Frisco, TX, USA, 2019.
41. Reddy, G.N.; Reddy, G. A study of cyber security challenges and its emerging trends on latest technologies. *arXiv* **2014**, arXiv:1402.1842.
42. Ursillo, S.; Arnold, C. *Cybersecurity Is Critical for All Organizations–Large and Small*; International Federation of Accountants: New York, NY, USA, 2019.
43. Ani, U.P.D.; He, H.; Tiwari, A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *J. Cyber Secur. Technol.* **2017**, *1*, 32–74. [CrossRef]
44. Van Devender, M.S. Risk Assessment Framework for Evaluation of Cybersecurity Threats and Vulnerabilities in Medical Devices. Ph.D. Thesis, University of South Alabama, Mobile, AL, USA, 2023.
45. Miller, J.C. Security Assessment of Cloud-Based Healthcare Applications. Master's Thesis, Milligan University, Johnson City, TN, USA, 2019.
46. Bodie, M.T. *HIPPA*; Cardozo L. Rev. De-Novo; Saint Louis University School of Law, Saint Louis University: St. Louis, MO, USA, 2022; p. 118.
47. Radanliev, P. Future developments in cyber risk assessment for the internet of things. *Comput. Ind.* **2018**, *102*, 14–22. [CrossRef]
48. Li, K.; Shi, R.; Yan, J.; Cai, C.; Sun, M.; Li, J. A RMF and AHP-Based Approach to Risk Assessment of Power Internet of Things. In Proceedings of the 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 17–22 August 2020; pp. 684–689.
49. Brandon, A.; Seekins, M.; Joshua, B.V.; Samuel, C.; Haller, J. Network data analysis to support risk management in an IoT environment. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 0063–0068.
50. Warren, K.; Sabetto, R. *FedRAMP: A Practical Approach*; MITRE Corporation: McLean, VA, USA, 2018.
51. McLaughlin, M. *Reforming FedRAMP: A Guide to Improving the Federal Procurement and Risk Management of Cloud Services*; Information Technology and Innovation Foundation: Washington, DC, USA, 2020.
52. McGillivray, K. *Government Cloud Procurement*; Cambridge University Press: Cambridge, UK, 2021.
53. United States Government Accountability Office; Wilshusen, G.C. *Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed: Report to Congressional Requesters*; United States Government Accountability Office: Washington, DC, USA, 2019.
54. Green, S. An Evaluation of Two Host-Based Vulnerability Scanning Tools. Ph.D. Thesis, Utica College, Utica, NY, USA, 2020.
55. Kinsella, D. Building an EERM Toolkit. *Risk Manag.* **2019**, *66*, 20–21.
56. Koo, J.; Kim, Y.-G.; Lee, S.-H. Security requirements for cloud-based C4I security architecture. In Proceedings of the 2019 International Conference on Platform Technology and Service (PlatCon), Jeju, Republic of Korea, 28–30 January 2019; pp. 1–4.

57. Kent, S. *Federal Cloud Computing Strategy*; Executive Office of the President of the United States: Washington, DC, USA, 2019.
58. Mughal, A.A. Cybersecurity Architecture for the Cloud: Protecting Network in a Virtual Environment. *Int. J. Intell. Autom. Comput.* **2021**, *4*, 35–48.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.