American Journal of Innovation in Science and Engineering (AJISE)

ISSN: 2158-7205 (ONLINE)

VOLUME 4 ISSUE 2 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Innovation in Science and Engineering (AJISE)

Volume 4 Issue 2, Year 2025
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v4i2.4289
https://journals.e-palli.com/home/index.php/ajise

Building a Resilient Computer Emergency Response Team (CERT): A Strategic Approach Using SWOT Analysis and the CERT Resilience Maturity Model for Cybersecurity Preparedness in the Bangsamoro Government, Philippines

Mansur L. Panalangin[1*], Ariel Roy L. Reyes[2], Haron A. Mohamad[3], Shahara A. Abo[4], Arnold S. Cararag[5]

Article Information

Received: December 17, 2024

Accepted: January 25, 2025

Published: May 15, 2025

Keywords

Bangsamoro Government, CERT Resilience Management Model (CERT-RMM), Computer Emergency Response Team (CERT), Cyber Threat Mitigation, Cybersecurity Preparedness, Digital Infrastructure Security, Operational Resilience, SWOT Analysis

ABSTRACT

exposed clients to risks during online transactions and service access. These incidents underscore the urgent need to enhance the region's cybersecurity preparedness and establish a resilient Computer Emergency Response Team (CERT). This study evaluates the current state of cybersecurity readiness across selected Bangsamoro Government ministries, offices, and agencies by integrating SWOT analysis with the CERT Resilience Management Model (CERT-RMM). Through this structured approach, the study identifies key strengths, weaknesses, opportunities, and threats while determining the current maturity level of the government's operational resilience. Based on the findings, actionable recommendations are provided to advance maturity levels and build a robust cybersecurity framework. The results aim to support the Bangsamoro Government in strengthening its digital infrastructure, ensuring secure service delivery, and mitigating emerging cyber threats effectively.

INTRODUCTION

Recent cybersecurity incidents affecting Bangsamoro Government websites have highlighted critical vulnerabilities, disrupted operations, and exposed users to potential risks. This study evaluates the cybersecurity preparedness of selected government ministries, offices, and agencies, focusing on the capacity of information officers to manage and secure these platforms. Using an integrated framework of SWOT analysis and the CERT Resilience Management Model (CERT-RMM), the study identifies the region's current maturity level in operational resilience and provides actionable recommendations to strengthen cybersecurity capabilities and ensure robust protection against emerging threats.

The Philippine National Government requires its agencies, offices, and instrumentalities, including local government units, to utilize the Internet to deliver public services and information. The Department of Information and Communications Technology (DICT) was established by virtue of Republic Act 10844, signed into law in 2016. DICT is mandated to strengthen improved public access and provide resource sharing and capacity building at all levels of the government. With this, government agencies established their websites while DICT assists by promulgating policies and issuances. In 2015, EO No. 189 was issued, which mandated all bureaus, offices, agencies, and instrumentalities of the Government to organize their respective Computer Emergency Response Teams (CERTs), subject to the guidelines to be issued by the Cybercrime Investigation and Coordinating Center (CICC). In the Bangsamoro Autonomous Region in Muslim Mindanao (BARMM), the equivalent of DICT is the Bangsamoro Information and Communications Office (BICTO). The Bangsamoro Transition Authority (BTA) passed a resolution in June 2024 urging the BICTO to provide measures to safeguard official websites and pages of the members of the Parliament, ministries, and offices of the Bangsamoro Government from any cyber-attacks. BICTO continuously includes capacity building for the different ministries, offices, and agencies of the BARMM. Currently, it is drafting the Bangsamoro Cybersecurity Plan, which consists of establishing the Bangsamoro CERT under its umbrella.

A Computer Emergency Response Team (CERT) is a group of information security experts responsible for the protection against, detection of, and response to an organization's cybersecurity incidents." Some organizations have developed a CERT Assessment Tool designed to increase a security incident responder's ability to assess risk and identify the incident response plan of critical information systems. The cyber threats that organizations encounter have been evolving. Organizations require new structures and knowledge to approach cyber-attacks and social media threats.

[1] Ministry of Science and Technology, Cotabato City, BARMM, Philippines
[2] University of Southern Philippines, Davao City, Philippines
[3] Talitay National High School, MBHTE, BARMM, DEPEd, Philippines
[4] Ministry of Finance, Treasury Office, BARMM Cotabato City, Philippines
[5] Bangsamoro Information Communication Technology Office, Cotabato City, BARMM, Philippines
[*] Corresponding author's e-mail: mhansur@gmail.com

These requirements can be overwhelming, especially in transitioning organizations. Thus many national and international security communities collaborated for a more secure internet. These collaborations involve a CERT (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team).

DICT has formulated the CERT Manual, which provides the general policies, protocols and classifications, guidelines, and procedures. In the BARMM, the BICTO has started a series of write shops for the crafting of the Bangsamoro Cybersecurity Plan. This paper is intended to provide an overview of the status of these efforts to assess the requirements to establish and operationalize coordinated CERT in the BARMM.

LITERATURE REVIEW

The evolving landscape of cybersecurity poses significant challenges, particularly in safeguarding government systems against exploitation techniques and malicious activities. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. [9] Threats can harm organizational operations, assets, individuals, and other organizations when known and unknown vulnerabilities are exploited, compromising the confidentiality, integrity, or availability of the information being processed, stored, or transmitted. Thus, agency heads at all levels were mandated to detect and report threats at an earlier stage.

Enhancing cybersecurity and protecting critical infrastructures require coordinated national, regional, and international efforts. The US Military wanted to objectively evaluate software/ICT subcontractors' process capability and maturity. The maturity models can be grouped into Progression Maturity Models, Capability Maturity Models (CMMs), and Hybrid Maturity Models. Aside from the maturity levels, organizations also comply with cybersecurity standards. This is generally classified into two main categories: information security and governance standards. Applying one standard may not fulfill all the demands of an organization, and it may be necessary to employ a combination of standards to ensure security against cyber threats and data loss. Each organization needs to understand the vulnerabilities of its system to apply the appropriate standards and structure to ensure cybersecurity.

Forswearing administration assaults, intelligent bombs, misuse apparatuses, busybodies, deceptions, infections, worms, send spam, and botnets are among the most critical cyberattack strategies. To counterattack the threats, network protection is fundamental and critical. This involves forestalling unapproved access and advanced assaults on networks, gadgets, frameworks, projects, and information. The following consists of cybersecurity elements as portrayed in: Infrastructure and network security, Application Security, Cloud Security, Information Security, End user Education, and Disaster Recovery. Moreover, another model for data security is called the CIA Triad. It has three sections, namely, secrecy (Confidentiality), respectability (Integrity), and accessibility (Availability).

The advancement of connectivity has introduced a plethora of security risks and vulnerabilities. The threat landscape constantly evolves, with cybercriminals developing new tactics, techniques, and procedures (TTPs) to evade detection and circumvent security protocols. For improved firewall technology that offers enhanced security features and greater insight into network traffic, Next-Generation Firewalls (NGFWs) are used. It is primarily designed to defend against cyber threats that attack network applications and infrastructure. Cyberattacks on Philippine government websites have been a persistent concern. Between 2020 and 2022, the Department of Information and Communications Technology (DICT) recorded over 3,000 high-level cyberattacks, with nearly half targeting government agencies and emergency response teams. In early 2024, DICT reported thwarting thousands of sophisticated cyberattacks on websites associated with President Ferdinand Marcos, the Philippine Coast Guard, and other government entities. Additionally, a (2022), survey by Kroll indicated that 75% of organizations in the Philippines experienced a cyber incident, significantly higher than the Asia-Pacific average of 59%. These findings highlight the escalating nature of cyber threats against Philippine institutions.

The governance setting in post-conflict afflicted areas highlights the transformative role of Information and Communication Technology (ICT) in governance and development. ICT initiatives such as UNDP's local governance strategies. Information and Communication Technology (ICT) is pivotal in governance and development, particularly in fragile and conflict-affected regions. It enhances transparency, fosters citizen engagement, and streamlines service delivery. It has a critical role, especially in fragile and conflict-affected regions, by improving transparency, fostering citizen engagement, and streamlining service delivery. However, deploying ICT solutions, particularly cybersecurity measures, in resource-limited settings poses significant challenges, including financial constraints, lack of technical expertise, and limited infrastructure. Despite these hurdles, digital transformation has emerged as a vital peacebuilding tool, enabling conflict-affected communities to access essential services, improve communication, and rebuild socio-economic stability. With the complexities of governance, including environmental and political landscapes, ICT supports governance to ensure transparency and fairness in accessing public service. Thus, it will be very challenging without ICT.

The governance and ICT challenges in the Bangsamoro region are deeply rooted in its historical and socio-political context, characterized by decades of armed conflict, political transitions, and attempts to establish autonomous governance. It is necessary to establish early a digital infrastructure as the foundation on which all digital initiatives will be built. The Bangsamoro Organic

Law (BOL) established the Bangsamoro Autonomous Region in Muslim Mindanao (BARMM), introducing governance frameworks that emphasize inclusive development, peacebuilding, and local autonomy . Policies for ICT infrastructure in combination with adequate funds provision, stable government, macro-economic determinants, and innovation environment are crucial for ICT-induced prosperity. However, implementing secure ICT systems within the Bangsamoro government presents several challenges, including inadequate infrastructure, limited technical expertise, and vulnerabilities to cyber threats due to resource constraints and evolving security risks. BICTO has acknowledged these issues, emphasizing the need for strategic planning and robust collaboration between the government and its citizens to address them effectively. Addressing these challenges requires targeted investments in ICT capacity-building, infrastructure, and tailored cybersecurity solutions that align with the region's unique socio-political dynamics. For now, the Bangsamoro Government adopts the National Government policies, such as formulating the Bangsamoro Cyber Security Plan and establishing a Regional CERT.

Establishing Computer Emergency Response Teams (CERTs) in developing regions is essential for addressing the growing challenges of cybersecurity threats. Computer Security Incident Response Teams (CSIRTs) are a key foundation of the cybersecurity ecosystem in developing countries. However, resource-limited settings face persistent challenges, including securing sustainable funding, recruiting skilled professionals, and maintaining operational efficiency. International organizations such as the International Telecommunication Union (ITU) and regional bodies have played a critical role in mitigating these challenges by providing technical assistance, conducting training programs, and offering initial financial support. Community-driven CERT models, which integrate local stakeholders and grassroots organizations, have also emerged as innovative approaches to strengthening cybersecurity resilience in low-resource environments. These efforts underscore the importance of collaborative and multi-stakeholder strategies for ensuring the sustainability and scalability of CERTs in developing regions, emphasizing partnerships among governments, international entities, and local communities as a foundational approach to fostering global cybersecurity resilience.

Policies are already in place to enhance ICT security, including the Data Privacy Act of 2012, which mandates personal data protection, and the E-Commerce Act, which provides a legal basis for online transactions and penalties for cybercrimes. The Cybercrime Prevention Act of 2012 governs government websites and cybersecurity, which outlines different roles in securing public digital assets. International treaties, such as the Budapest Convention on Cybercrime, and regional agreements, like the ASEAN Cybersecurity Cooperation Strategy, influence national cybersecurity policies and guide for adapting to global standards. These frameworks are particularly relevant to the Bangsamoro Autonomous Region, where implementing robust cybersecurity measures is essential for governance and aligning with broader national and international cybersecurity goals.

RESULTS AND DISCUSSION

The Bangsamoro ministries, offices, and agencies (MOAs) were represented by its IT Officers in the workshop for the SWOT Analysis for the establishment of the CERT. The DICT issued the National CERT manual. The NCERT provides services such as incident response, actionable security intelligence, signal intelligence, early warning system, ICT equipment Testing Lab, and web intelligence (WEBINT). In the BARMM, the Bangsamoro Information Communications Technology Office (BICTO), is mandated to ensure the implementation of, review, and periodic updating of the Bangsamoro e-government plans. It shall develop, manage, and maintain the Bangsamoro Government-owned ICT infrastructure, configure centralized information systems, and promote collaborative efforts to ensure ICT capabilities and capacities across levels in the BARMM. The following table summarizes the output of the workshop.

Strengths and Weaknesses

Identifying the Strengths was used to map existing capabilities to the CERT-RMM domains and levels. The Strengths provide evidence of maturity levels (e.g., robust legislative frameworks could indicate a "Defined" level in governance). Further, whether the strengths are isolated (indicative of lower maturity) or integrated across the organization (indicative of higher maturity) was determined.

1.Legislative and Policy Framework. The participants revealed that existing laws, policies, and frameworks provide a solid foundation for implementing IT initiatives and ensuring cybersecurity. This is supported by their responses, such as the existing ability to enact legislative measures, implementation of E.O No. 189, S 2015, Bangsamoro e-Government Master Plan, ongoing formulation of the Bangsamoro Cybersecurity Plan, existing law for CERT, cloud server infra, and implementation of existing IT policies.

2. Institutional Support and Collaboration. This theme encompasses the strengths of partnerships, internal support systems, and stakeholder collaboration. The participants shared that there is a presence of support from the Bangsamoro Gov't, partners, and other stakeholders, institutional support from BICTO, BCERT, and NCERT, and strong connections to highly technical consultants.

3. Organizational Commitment and Autonomy. This reflects the strength in the commitment and autonomy of the BARMM and its leadership to prioritize and advance IT initiatives. The participants said that there is a strong will & determination to establish CERT and the fact that the BARMM is an autonomous region.

4. Resourcefulness and Capacity Building. This part

highlights the availability of personnel and the willingness to learn and align with strategic priorities. The participants also shared that many potential personnel are willing to learn aligned with/ the priority agenda of the Chief Minister.

5. Existing Infrastructure and Rapid Response Capabilities. These items relate to the region's existing IT infrastructure and ability to respond effectively to cyber challenges. Participants said that some MOAs have established Data Center facilities, and there is a presence of quick response to cyber-attacks that provide reliable responses.

6. BICTO's Strategic Initiatives and Services. This focuses on the initiatives and services offered by BICTO, which bolster IT governance and cybersecurity efforts.

These Strengths were organized to identify their relevance to the CERT-RMM domains and level of maturity using the metrics provided above. The identified weaknesses are as follows:

1. Governance Weaknesses. Lack of established ICT policies and governance frameworks, no Parliament Bill or legal mandate for CERT, Absence of leadership appreciation and support for cybersecurity initiatives, and bureaucratic delays impacting decision-making and implementation.

2. Process Maturity Weaknesses. There is no structured CERT framework or dedicated focal person to oversee processes, Limited technical expertise, unstructured roles (e.g., no software developers, database administrators, or network/system administrators), and reactive and uncoordinated processes due to a lack of staff and skills.

3. Infrastructure Readiness Weaknesses. There is poor IT infrastructure quality (e.g., SME-grade equipment), limited or no monitoring capabilities (e.g., SIEM tools, vulnerability assessment tools), Unsecured and unconsolidated IT assets, and lack of resources to upgrade or maintain infrastructure.

4. Response Capability Weaknesses. Unpreparedness for cyber threats due to insufficient training and resources, lack of incident response tools and frameworks, and limited cybersecurity training in key areas (e.g., incident response, threat intelligence, malware analysis), few technical staff with the necessary skills.

5. Cross-cutting weaknesses. Insufficient budget for IT and cybersecurity initiatives, general lack of support from management for IT resilience efforts.

Integrating both the Strengths and Weaknesses identified, we can summarize the information as follows and determine the level of maturity in the CERT-RMM.

Table 1: Strengths and Weaknesses

CERT-RMM Domain	Strengths	Weaknesses	Maturity Level	Rationale
Governance	- Legislative measures and executive orders (E.O. No. 189, s. 2015) - Bangsamoro e-Government Master Plan - IT policies and frameworks.	- No established ICT policies. - No mandate for CERT. - Lack of appreciation by BARMM leadership. - No Parliament Bill for CERT.	Performed (Level 1)	Despite the strong legislative foundation, the absence of critical policies and the lack of leadership support hinder the institutionalization of governance processes.
Process Maturity	- Initiatives like BICTO BCERT. - Support from partners and stakeholders. - Consultant engagement.	- Lack of technical personnel and skills. - Lack of structured CERT. - Bureaucratic delays. - No focal person for CERT processes.	Performed (Level 1)	Processes are reactive and dependent on external support (e.g., consultants). Weak internal capabilities and bureaucratic inefficiencies prevent consistent execution.
Infrastructure Readiness	- Data centers established in some ministries. - CERTCLOUD law for infrastructure. - Autonomous region status.	- Poor IT infrastructure (e.g., SME-grade equipment). - No monitoring tools (e.g., SIEM). - Unsecured IT assets. - Unconsolidated IT resources.	Performed (Level 1)	While some infrastructure exists, significant deficiencies in visibility, monitoring, and equipment quality limit operational readiness and resilience.
Response Capability	- Quick and reliable responses to cyber incidents. - BICTO BCERT initiatives.	- Unpreparedness for cyber threats. - Limited cybersecurity training. - No incident response framework. - Few skilled personnel.	Performed (Level 1)	Response capability relies on isolated initiatives but lacks structured frameworks, skilled teams, and essential cybersecurity tools.

With the ongoing BARMM Government transition, the required processes for the institutionalized CERT in the region have not yet come to fruition. The concerned MOAs are still setting up the policies, frameworks, and plans. While the strategies have already been identified in the Bangsamoro Development Plan for 2023-2028, the implementation is another story.

The first domain is Governance. These measures establish roles, responsibilities, policies, and strategies for managing resilience and aligning with organizational goals. In relation to the establishment of CERT, the BARMM Government has identified the need to establish the CERT. It has acknowledged the need for collaboration, setting up policies and guidelines on protocols, and sharing capabilities. However, these have not been institutionalized and are still in ongoing transition. As an autonomous region, it has the capability to create its own regional laws subject to the provisions of the Constitution. Based on the description of the maturity levels, it is apparent based on the SWOT Analysis workshop that the BARMM Government is generally still in Level 1 in the governance domain. This means that the basic processes are in place and executed. The MOAs are aware of the requirements and standards of the CERT. However, the activities are reactive, informal, and not standardized. Thus, the results depend on individual efforts and are not repeatable. Moreover, despite the strong legislative foundation, the absence of critical policies and the lack of leadership support hinder the institutionalization of governance processes. While existing legislative measures (e.g., E.O. 189) provide a foundation, the absence of key policies, lack of CERT mandates, and limited leadership appreciation weaken the ability to institutionalize processes across BARMM.

The second domain is on the Process Maturity. This evaluates processes' design, implementation, and standardization to ensure they support resilience objectives consistently. With the ongoing transition and capacity improvements in ICT infrastructure, manpower, structures, and institutionalized cooperation, the processes are more reactive. Moreover, these processes are reactive and dependent on external support (e.g., consultants). There is also an observation that weak internal capabilities and bureaucratic inefficiencies prevent consistent execution. With this supporting information, as identified in the workshop, we can say that the Bangsamoro Government is still on Level 1 in terms of process maturity. This means that the basic processes are in place and executed, but their activities are reactive, informal, and not standardized. The strengths, such as stakeholder support and consultant engagement, outweigh weaknesses like skill gaps, lack of roles, and no focal point for CERT processes. These issues make processes inconsistent and reactive, placing process maturity at Performed (Level 1).

Infrastructure readiness, which assesses the adequacy, availability, and resilience of technology, facilities, and resources that support critical operations, can be determined based on the information provided in the SWOT Analysis workshop that it is still on Level 1. This indicates that while some infrastructure exists, significant deficiencies in visibility, monitoring, and equipment quality limit operational readiness and resilience. This is caused by several factors, such as poor IT infrastructure (e.g., SME-grade equipment), no monitoring tools (e.g., SIEM), unsecured IT assets, and unconsolidated IT resources. Despite some ministries having data centers, the weaknesses in IT asset consolidation, poor infrastructure quality, and lack of visibility tools (e.g., SIEM) indicate readiness is still ad hoc and reactive, reducing maturity to Performed (Level 1).

Moving on with the Response Capability domain, we can observe that the information provided describes a Level 1 maturity. Response capability measures the ability to detect, mitigate, and recover from incidents effectively, ensuring continuity of operations. The workshop participants perceive that there is unpreparedness for cyber threats, limited cybersecurity training, no incident response framework, and few skilled personnel. Response capability relies on isolated initiatives but lacks structured frameworks, skilled teams, and essential cybersecurity tools. Although some response initiatives (e.g., quick responses to incidents) exist, unstructured processes, limited training, and the absence of incident response tools mean response capability remains reactive and inconsistent. This limits the maturity to Performed (Level 1).

The identified weaknesses are barriers to the advancement of the region to the next level of maturity. These can be leveraged and addressed to make way for advancement. Moreover, with the identified weaknesses and opportunities, the BARMM Government can enhance its Cybersecurity Plan by focusing on the CERT RMM domains and advancing in the maturity level. The opportunities can be considered as part of the strategic initiatives and the BARMM Government can mitigate threats by addressing gaps highlighted in weaknesses.

Opportunities and Threats

Opportunities can be turned into strategic initiatives. These opportunities can facilitate the advancement in the maturity level by identifying the thematic areas that can be improved with the inflow of outside enabling factors. These can assist and define the actions to achieve more strategic results.

The lack of awareness, skill gaps, and capacity constraints identified in weaknesses align with the threats of leadership instability, resistance to change, and cyberattacks. Addressing these issues through training, role clarification, and infrastructure upgrades mitigates risks and will strengthen the CERT maturity level. Further, improving process maturity and governance reduces dependencies on third parties and minimizes misunderstandings within CERT teams.

Advancing the organization's CERT-RMM maturity level requires a comprehensive integration of strengths,

Table 2: Opportunities and Threats

CERT-RMM Domain	Threats Identified	Analysis	Possible Actions
Governance	- Change of leadership after BARMM elections. - Political instability. - Resistance to change in terms of cybersecurity. - Public criticism. - Misunderstanding among CERT members. - Lack of awareness by constituents.	Governance-related threats arise from political dynamics, leadership changes, and lack of awareness by stakeholders. These weaken long-term strategic direction.	1. Institutionalize CERT governance structures and policies to ensure continuity, independent of leadership changes. 2. Conduct stakeholder engagement campaigns to build awareness of cybersecurity initiatives and their benefits. 3. Establish a cross-agency oversight body for CERT governance to reduce political influence.
Process Maturity	- Misunderstanding among CERT members. - Dependency on third parties. - Resistance to change in terms of cybersecurity.	These threats reflect a lack of coordination, reliance on external actors, and resistance to adopting structured cybersecurity processes.	1. Create clear roles, responsibilities, and communication processes within CERT. 2. Build internal capabilities to reduce third-party reliance. 3. Offer training programs to overcome resistance to new cybersecurity workflows.
Infrastructure Readiness	- Scalability issues. - Lack of control over cloud assets (e.g., web hosting). - Access control issues.	-Infrastructure-related threats highlight gaps in managing cloud resources, scalability, and controlling access to IT systems.	1. Implement access control mechanisms such as multi-factor authentication (MFA) and role-based permissions. 2. Conduct audits of cloud and web-hosted assets to identify vulnerabilities. 3. Adopt scalable cloud solutions with built-in security features.
Response Capability	- Changing nature of cyber threats (e.g., sophisticated attacks). - Proliferation of government threat actors. - Increased cyberattacks. - Lack of awareness among employees and top management.	Response-related threats underscore the need for proactive monitoring, threat intelligence, and trained personnel to handle incidents effectively.	1. Establish a Security Operations Center (SOC) to monitor threats in real-time. 2. Provide regular cybersecurity awareness training for all staff and leadership. 3. Develop incident response playbooks for new and emerging cyber threats.

weaknesses, opportunities, and threats. Strengths such as legislative measures, existing IT policies, and strong partnerships provide a foundational advantage. However, weaknesses like skill gaps, limited resources, and the lack of cybersecurity awareness hinder operational consistency and require targeted interventions. Opportunities in training, collaboration with public and private entities, and the adoption of advanced technologies offer pathways for improvement. Threats such as evolving cyber risks, political instability, and resistance to change necessitate robust governance frameworks and proactive mitigation strategies. By institutionalizing governance processes, standardizing workflows, upgrading infrastructure with tools such as SIEM and vulnerability assessment platforms, and improving response capabilities through training and incident response playbooks, the organization can progress to a Managed (Level 2) maturity level, aligning its operational resilience with CERT-RMM standards.

CONCLUSIONS

The CERT Resilience Management Model (CERT-RMM) was utilized as a guiding framework to integrate SWOT analysis for assessing and advancing the maturity of the organization's operational resilience. Strengths, such as established legislative measures, strategic IT policies, and strong partnerships, were foundational to current capabilities, while weaknesses, including skill gaps, insufficient resources, and the absence of key policies, were identified as critical barriers to consistency and institutionalization. Opportunities, such as collaboration,

training, and technology adoption, highlighted clear pathways to address gaps, while threats, including political instability, sophisticated cyber risks, and resistance to change, emphasized the need for proactive governance and infrastructure upgrades.

The integration of SWOT analysis within the CERT-RMM domains—Governance, Process Maturity, Infrastructure Readiness, and Response Capability—enabled the identification of the current maturity level as Performed (Level 1) across the domains. Recommendations were provided to progress to Managed (Level 2), including the institutionalization of governance processes, development of standardized and repeatable workflows, investment in scalable and secure infrastructure, and the establishment of structured incident response frameworks supported by regular training and awareness campaigns.

This approach demonstrates the practical application of CERT-RMM in aligning resilience capabilities with organizational goals while providing actionable insights for advancing maturity. By systematically addressing weaknesses, leveraging strengths, and capitalizing on opportunities, the organization can enhance its operational resilience and prepare to meet evolving cybersecurity challenges effectively.

REFERENCES

Ahmed, A. A., & Al Dabbagh, N. B. (2023). Web Attacks and Defenses: Review Paper. *Journal of Education and Science,* 30(1), 45-62. https://doi.org/10.33899/edusj.2023.137855.1319

Anwar, S., & Yunus, K. (2024, February 09). *A comprehensive guide to CIEMs: Mastering cloud security in limited resource settings*. Bitdefender. https://www.bitdefender.com/en-us/blog/businessinsights/a-comprehensive-guide-to-ciems-mastering-cloud-security-in-limited-resource-settings

APAC State of Incident Response: Philippines. (2022). *Retrieved November 18*, 2024, from Kroll: https://www.kroll.com/en/insights/publications/cyber/apac-state-incident-response/philippines

Arora, V. (2010). *Comparing Different Information Security Standards: COBIT vs. ISO 27001*. Doha, Qatar: Carnegie Mellon University.

Bangsamoro Transition Authority. (2020, October 28). Retrieved from Bangsamoro Autonomy Act Number 13 (Bangsamoro Administrative Code): https://parliament.bangsamoro.gov.ph/bta-acts/an-act-providing-the-bangsamoro-administrative-code-and-for-other-related-purposes

Bangsamoro Development Plan. (2023). *Cotabato City: Bangsamoro Planning and Development Authority-BARMM*.

Budapest Convention on Cybercrime. (2021). Retrieved November 18, 2024, from https://www.coe.int/en/web/cybercrime

Caralli, R., Knight, M., & Montgomery, A. (2012). *"Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability*. White paper (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University). Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58916

CERT Resilience Management Model (CERT-RMM) Version 1.2. (2016). (Carnegie Mellon University, Software Engineering Institute) Retrieved from https://insights.sei.cmu.edu/library/cert-resilience-management-model-cert-rmm-version-12/

Chammem, M., Hamdi, M., & Kim, T. H. (2014). Extending advanced evasion techniques using combinatorial search. *2014 7th International Conference on Security Technology (SecTech),* (pp. 41-46).

Cornell, A., & Waits, T. (2013). The CERT assessment tool: Increasing a security incident responder's ability to assess risk. *2013 IEEE International Conference on Technologies for Homeland Security* (HST), 236-240. https://doi.org/10.1109/THS.2013.6699006

Cybercrime Prevention Act of 2012, Republic Act No. 10175. (n.d.). Retrieved from https://www.doj.gov.ph.

Data Privacy Act of 2012 (Republic Act No. 10173). (n.d.). Retrieved from https://www.privacy.gov.ph.

De Salins, G. D., Collett, G. C., & James, R. (2024). *Digital First Responders - The Role of Computer Security Incident Response Teams (CSIRTS) in Developing Countries*. World Bank. Retrieved from https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099060824112023473/p177852158c0330d51a71613967bd98edc4

DICT. (n.d.). Retrieved November 18, 2024, from https://dict.gov.ph/about-us/our-mandate/

DICT CERT Manual. (n.d.). Retrieved from https://www.ncert.gov.ph/cert-manual/dictcertmanual.pdf

Etuh, E., & Bakpo, F. (n.d.). *Social Media Networks Attacks and their Preventive Mechanisms: A Review*.

Government-citizen collaboration key to BARMM's digital future, BICTO says. (n.d.). Retrieved November 18, 2024, from Bangsamoro Official Website: https://bangsamoro.gov.ph/news/latest-news/government-citizen-collaboration-key-to-barmms-digital-future-bicto-says/

Grobler, M., & Bryk, H. (2010). *Common Challenges Faced During the Establishment*. https://doi.org/10.1109/ISSA.2010.5588307

Guide on Local Governance in Fragile and Conflict-Affected Settings: Building a Resilient Foundation for Peace and Development. (2016). Retrieved November 18, 2024, from United Nations Development Programme (UNDP): https://www.undp.org/publications/local-governance-fragile-and-conflict-affected-settings

Gulla, V. (2023). 3,000 high-level cyberattacks in PH in 2022: DICT. Retrieved November 18, 2024, from *ABS-CBN News*: https://news.abs-cbn.com/business/04/12/23/3000-high-level-cyberattacks-in-ph-in-2022-dict

Helia, H. (2017). Secure web development Pankaj Pant.

Haaga-Helia Univ. *Appl. Sci, 8*(5), 2003-2005.

Kumar, A. N. (2023). Next-generation Firewalls And Application Layer Security: Protecting Against Advanced Threats. Retrieved November 18, 2024, from Influencer: https://influencermagazine.uk/2023/01/next-generation-firewalls-and-application-layer-security-protecting-against-advanced-threats/

LawPhil Project- RA 10175. (n.d.). Retrieved Noovember 18, 2024, from https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html

Leveraging digital technologies to enable program monitoring in remote fragile and conflict-affected areas. (2023). Retrieved November 18, 2024, from World Bank: https://www.worldbank.org/en/results/2023/03/07/leveraging-digital-technologies-to-enable-program-monitoring-in-remote-fragile-and-conflict-affected-areas

Managing Risks with Limited Resources. (n.d.). Retrieved November 18, 2024, from CSO Online: https://www.csoonline.com/article/567649/managing-risks-with-limited-resources.html

Mangelen, B. J. Z., Bawa, L. S., Untong, L. P., & Mohamad, H. A. (2023). Maguindanaon Love Songs as Tool and Springboard in Teaching Figurative Language for Maguindanaon Culture Preservation. *Journal of Natural Language and Linguistics, 1*(1), 31–41. https://doi.org/10.54536/jnll.v1i1.2035

Mohamad, H. A. (2021). *The lived experiences of english language learners' on sakalam expression.*

Mohamad, H., & Parcon, M. (2022). Unfolding Stories of English Teachers with Multiple Ancillary Functions in Maguindanao-1 Division: A Phenomenological Study. *Psychology and Education: A Multidisciplinary Journal, 2*(6), 496-501.

Panalangin, M. L., Mantikayan, J. M., Abdulgani, M. A., & Mohamad, H. A. (2024). Integration of IoT-Knowledge-Based Architecture in the Development of the Daily Time Records System for the Ministry of Science and Technology, Philippines. *American Journal of Innovation in Science and Engineering, 4*(1), 9-20. https://doi.org/10.54536/ajise.v4i1.3947

Pulindao, F. L., & Mohamad, H. A. (2023). Learners' View of English Language Learning Through Modular Approach-A Phenomenology. *American Journal of Interdisciplinary Research and Innovation, 2*(4), 20-35.

Reyes, F. M., Abdulgani, M., Aliuden, M. F., Mantikayan, J., Guiamalon, T., Dilna, S., Mohamad, H., & Nawal, S. Z. (2022). Event Management System With SMS Notification for Mindanao People's Care Foundation, Inc. *Psychology and Education: A Multidisciplinary Journal, 3*(7), 600-609.

Salah, H., Abdulgani, M., Aliuden, M. F., Mantikayan, J., Guiamalon, T., Dilna, S., … & Ferolino, M. F. (2022). Adopting Human Resource Information System (HRIS)-Enabled Government Transformation: Perspective of MBHTE Employees. *Psychology and Education: A Multidisciplinary Journal, 3*(7), 610-615.

Sinsuat, D. R. R., Abdulgani, M., Mantikayan, J., & Mohamad, H. (2022). The Effectiveness of Augmented Reality (AR) as a Tool of Office for Ministry of Basic, Higher, and Technical Education in Bangsamoro Autonomous Region in Muslim Mindanao. *Psychology and Education: A Multidisciplinary Journal, 3*(5),468-479.

Usman-Kaibat, S., Kaibat, M., Maguid, A., Mohamad, H., Alim, T., (2025). The Status of K-12 Science and Mathematics Spiral Curriculum: A Case Study. *Psychology and Education: A Multidisciplinary Journal, 30*(2), 209-217. https://doi.org/10.5281/zenodo.14602606

Usman, S. M., Abdulgani, M. A., Faheem, M., Aliuden, M., Mantikayan, J. M., Abdulgani, R. A., .. & Mohamad, H. A. (2022). Inventory and Monitoring System on Logistic Vehicles and Passengers Loading Plan for Offiice of the Presidential Adviser on the Peace Process (OPAPP). *Psychology and Education: A Multidisciplinary Journal.*