

CENTRAL MINDANAO UNIVERSITY (CMU)

Lab Midterm Examination

Members:

Karl Kinji S. Landicho

Klent Denzel Baylosis

Rosette Ayunar

Ted Bryan Razonado

Jay Ranes

Nieven Charles Tagactac

Dave Edward Chavez

Cedrick Capuyan

- Proof the letter received by the DTO Director Mr. Jeremy Yves Capili
 - Signed by Sir Capili

March 14, 2023

THRU: CAPILI, JEREMY YVES
DTO DIRECTOR

SUBJECT: IT SECURITY AUDIT OF CENTRAL MINDANAO UNIVERSITY

Dear Sir/Mr.,

I hope this letter finds you well. I am writing to express our intention to conduct a study on the audit of the Digital Transformation Office (DTO) at Central Mindanao University, in fulfillment of our subject Information Assurance and Security.

Our study aims to assess the practices of your security measures, data integrity, compliance with relevant standards and regulations in the DTO of your institution, and effectiveness in supporting the university's operation.

We understand the critical role that the DTO plays in supporting the university's operations, decision-making processes, and strategic initiatives. Therefore, our audit will be conducted with the utmost confidentiality, and respect for your institution's policies and procedures.

We would appreciate your cooperation in facilitating this audit by providing access to relevant documentation, systems, and personnel as needed. Our team is committed to working closely with your staff to minimize disruption to daily operations and to ensure a smooth audit process.

If you have any questions or require further clarification regarding our intent to audit the Central Mindanao University DTO, please do not hesitate to contact us through our mobile number 09366492175, or email us at landicho.karlkinji22@gmail.com. We look forward to the opportunity to collaborate with you and contribute to the ongoing improvement of your institution's information management systems.

Thank you for considering our request, and we look forward to your favorable response.

Very Sincerely,

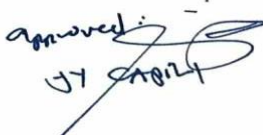

KARL KINJI LANDICHO
PROJECT MANAGER

Attested By:

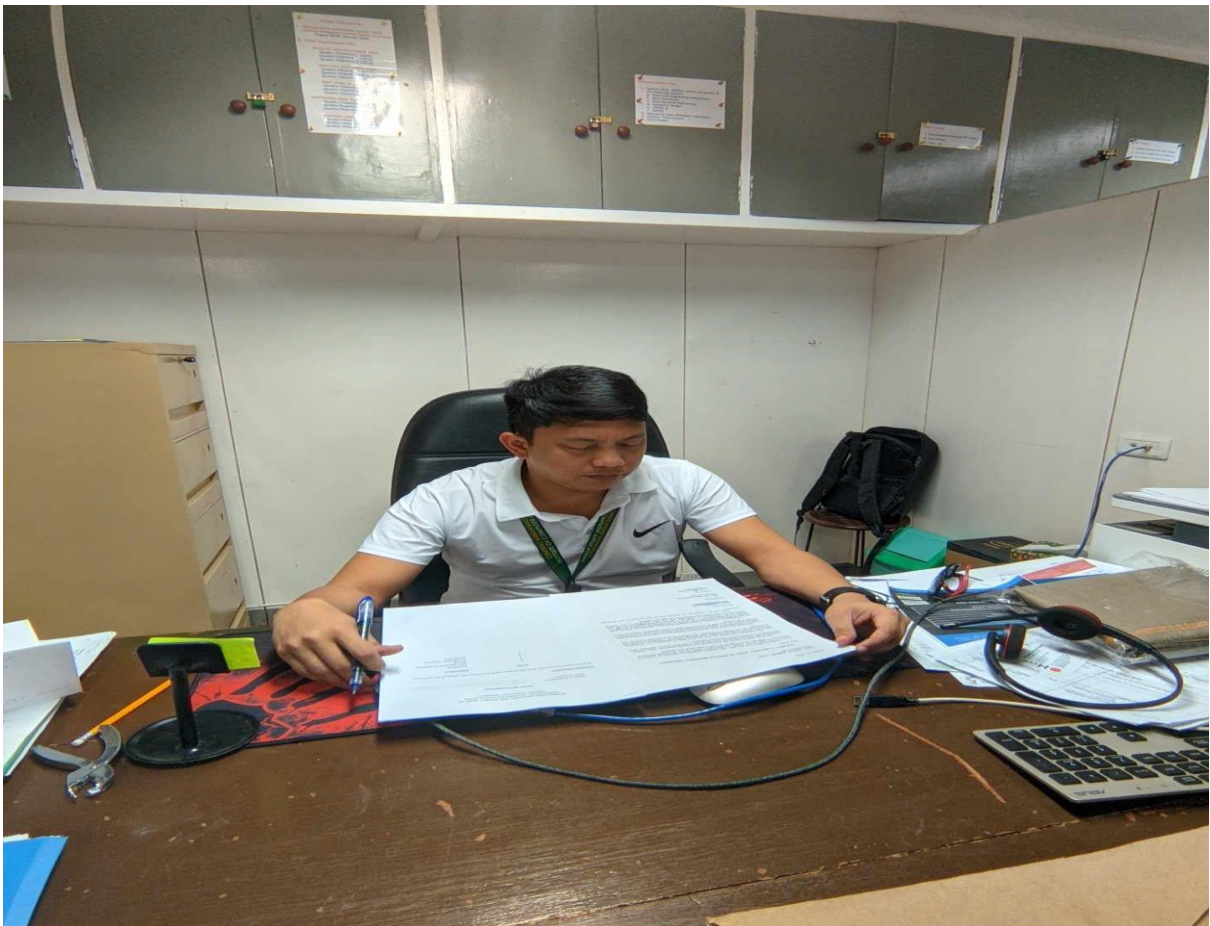

SGD. DR. MEL HAYAG JR.
Course Instructor

NOTED BY:


JOHN DUTAJONES
College Dean


approved
JY Capili

- Proof of questionnaire answered by the respondent



• Answered Questionnaire

No.	Items	Scale				
1	How well does the MIS office in Central Mindanao University follow industry standards with regards cyber security policies, procedures, and standards based on industry standards	5	4	3	2	1
2	To what extent does the MIS office protect sensitive information received from a third- as well as other parties with whom that data is shared (i.e. Encryption, SSL/TLS connections)? party firm during transmission between the owning third-party	5	4	3	2	1
3	How effectively are all devices within the MIS office that store or process a third-party firm's sensitive information protected from the Internet by a firewall?	5	4	3	2	1
4	In terms of relevance and effectiveness, how well-defined are the roles of designated Cyber-security personnel within the MIS office	5	4	3	2	1
5	How consistent and relevant is the cyber-security user education and awareness program conducted by the MIS office or other relevant departments within the university	5	4	3	2	1
6	How relevant is the performance of cyber-security audits by external 3rd parties by the MIS office	5	4	3	2	1
7	How effectively do all devices within the MIS office that store or process sensitive information utilize anti-malware software with current signature Files	5	4	3	2	1
8	In terms of relevance, do users that can access devices that store or process sensitive information have a unique user name and complex password to access the system	5	4	3	2	1
9	In terms of relevance, do all devices within the MIS office that store or process sensitive information at a minimum have access control that is configured on a least privilege model? (A person only has access to the data/device that they need)?	5	4	3	2	1
10	How effectively is the performance of the vulnerability scans on all the devices that store or process sensitive information within the MIS office	5	4	3	2	1
11	How well are the vulnerabilities being remediated in a risk based priority manner within the MIS office	5	4	3	2	1
12	How relevant is the configuration of all devices that store or process sensitive information to have all unnecessary ports and services disabled and are they used for limited functions	5	4	3	2	1

ISO certified

Network Security
Data Privacy
Encryption
SSL/TLS
Firewall

Wia Mc
Security

13	How promptly are patches deployed for high-risk operating system and third-party application vulnerabilities on all devices storing or processing sensitive information, in accordance with industry best practices (i.e., within 48 hours), and medium/low-risk patches within <= 30 days	5	4	3	2	1
14	How well encrypted is the sensitive information stored in all computer devices within the MIS office	5	4	3	2	1
15	To what extent do all mobile devices (e.g., smartphones, tablets) storing sensitive information have configuration management provided by the MIS office's centrally managed infrastructure, including the ability to remote wipe the device	5	4	3	2	1
16	To what degree do all mobile devices in the MIS office that store sensitive information at a minimum have access control to the device	5	4	3	2	1
17	How skilfully is the MIS office Computer Incident Response Team (CIRT) with a formal process to respond to cyber-attacks?	5	4	3	2	1
18	When you must share sensitive information with other companies, do you require those companies to follow policies, and procedures for cyber security based on industry standards?	5	4	3	2	1
19	Does the MIS office require 2-factor authentication for remote access (e.g. token used in addition to a username and password for VPN login)?	5	4	3	2	1
20	Does the MIS office perform industry standard logging and monitoring on devices that store or process sensitive information?	5	4	3	2	1
21	Does the MIS office control web access based on the risk (e.g. reputation, content, and security) of the sites being visited (e.g. Web Proxy Controls)?	5	4	3	2	1
22	How effectively does the capabilities of the MIS office of detecting and blocking malicious e-mail prior to delivery to the end user?	5	4	3	2	1
23	Does the MIS office actively participate in a cyber-intel sharing forum	5	4	3	2	1
24	How often does the MIS office perform phishing email testing of its employees	5	4	3	2	1

As long as the updates/patches are available

Session

ISO standard

Subscription type

- Other Documentation

