Selected KA required	Identify Cyber Risks	Protect Resources	Detect Cyber Risk Occurrences	Response to Cyber Risk Occurrences Incidents	Recover from High Impact Risk Incidents
Scope Management					
Plan Scope Mgt	Identify project resources that need to be protected. E.g. NIST catogories - Asset Management - Business Environment - Governance - Risk Assessment - Risk Management Strategy	Identify the methods/tools/strategies to protect the project resources. E.g. NIST catogories - Access Control - Awareness and Training - Data Security - Information Protection Processes and Procedures - Maintenance - Protective Technology	Identify the risk detection scheme. E.g. NIST catogories - Anomalies and Events - Security Continuous Monitoring - Detection Processes	Identify the response methods that can be used. E.g. NIST catogories - Response Planning - Communications - Analysis - Mitigation - Improvements	Identify the recover measures when university's critical infrastructures faceing loss, modification, damage. E.g. NIST catogories - Recovery Planning - Improvements - Communications
Collect Requirements	Collect and confirm with the clients about their requirements for resources securing	Collect and confirm with the clients about their protection methods requirements	Collect and confirm with the clients about their risks detection requirements	Collect and confirm with the clients about their preferred risks response mechanism	Collect and confirm with the clients about their preferred infrastructures recovery mechanism
Define(Product) Scope	Identify which project assets are exposed to danger in product design phase	Implement protection in functional and non-functional scope of product	Code killswitch detection in product design phase	Code killswitch response in product design phase	List the recovery plan for university in the situation when code killswitch is turned on
Create WBS	Create WBS for identifying project resources that need to be protected	Create WBS for protecting project resources	Create WBS for detecting cyber risk occurrences	Create WBS for responding to cyber risk occurrences incidents	Create WBS for recovering university's critical infrastructures from high impact risk incidents
Validates Scope	Make Test plan for efficiently and completely identifying project resources	Write test scripts for testing project resources protection	Write test scripts for testing risk detection	Write test scripts for testing risk response	Write test scripts for testing recovery from disaster
Control Scope	Manage changes to project resouces	Manage changes to project resouces protection methods	Manage changes to risk detection scheme	Manage changes to response methods	Manage changes to recovery mechanism
Stakeholders Management					
Identify Stakeholders	Identify people involved in the project and their resources	- Identify the vulnerability brought by people's lack of awareness of cybersecurity - List the potential chances that people can be hacked by social engineering	- Identify the detection scheme to detect potential external hacking on employees and employers - Specify how to detect social engineering	Identify the risk response to social engineering	Identify the recovery mechanism after being attacked by social engineering or other people perspective cyber attacks
Plan Stakeholder Engagement	Recruit employees that already have some sense and awareness of cybersecurity	- Recruit cybersecurity specialist to train the general employees - Recruit cybersecurity specialist to protect potential vulnerability caused by general employees	Recruit cybersecurity specialist to implement the detection mechanism	Recruit cybersecurity specialist to analyze and respond to the happening cyber attacked that goals for stakeholders	Recruit cybersecurity specialist and assets manager that can quickly recover the critical infrastructures of university
Manage Stakeholder Engagement	Train employees and managers regularly on cybersecurity awareness and mitigation methods	Train employees and managers regularly on the procedure of protecting project resources	Train employees and managers regularly on detecting potencial social engineering risks	Train employees and managers regularly on reporting the cyber attacks for cybersecurity specialist to respond to the attacks	Train employees and managers regularly on how to recover the critical infrastructrues and project resources after a high impact incidents already happened

Monitor Stakeholder Engagement	- Monitor and record any malicious or suspicious behaviour of internal stakeholders - Monitor and record any vulnerability of peope management	Monitor and record the whole protection process on preventing cyber attacks on people involved	Monitor and record any detected suspicious logs from internal people	Monitor and record responses of social engineering attacks from stakeholders	Monitor and record the recover operation from stakeholders each time
Communication Management					
Plan Communication Management	Identify the stakeholder communications requirements	All stakeholders (such as suppliers, customers, partners) understand the roles and responsibilities.	Stakeholders and responsibilities for detection are well defined to ensure accountability.	Personnel know their roles and order of operations when a response is needed.	Public relations are managed.
Manage Communication	Identify the Stakeholders.	Communications and control networks are protected.	Establish and manage a baseline of communication operations and expected data flows for stakeholders and systems.	Events are reported consistent with established criteria.	Reputation after an event is repaired.
Monitor Communication	Identify stakeholders' information needs.	Identify the flow of information.	The communication environment is monitored to detect potential cybersecurity events.	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecuritysituational awareness.	Recovery activities are communicated to internal stakeholders and executive and management teams.
Project Team Resource Management	Identify the definition of team resources, the allocation of personnel in different situations, the management plan within the team, and recource release based on roles and responsibilities of individuals	Identify the staffs responsible for risk protection and distribute the team resources(e.g., tools, equipment, and supplies)	Identify the staffs responsible for risk detection and security vulnerabilities that may be caused by internal personnel's improper behavior	Identify staffs and resources will be deployed to response to cyber risk	Identify staffs and resources for executed recovery processes and procedures
Plan Resource Management	Identify the information security roles and responsibilities of the team members, aligned with internal roles and external partners	Identify which team resources will be allocated to staff who is responsible to protect, including: - maintenance - organizational assets - controlled tools - vulnerability management	Identify which team resources will be allocated to staff who is responsible to detect cybersecurity incidents	Identify which team resources and staffs will be deployed when cyber risks occur	Identify which team resources and staffs will be applied for recovery strageties after a cybersecurity incident
Estimate Activity Resources	Estimate the type and quantities of resources necessary to specific cyber risk	Team resources for protection of certain risk should be estimated	Team resources for detecting vulnerabilities should be estimated	Estimate how much the deployment of respond plan would cost	Estimate how much would the recovery strategies cost
Acquire (Recruit) Resources	Analyze and organize the requirement list of team resources for different cyber risks	Obtain open source software and useful data resources from reliable third parties	Check the effectiveness of the tools and resources used in the vulnerability detection plan	Ensure that the recruited staffs involved in the response work have sufficient capabilities to deal with different cybersecurity incidents	Some data storage devices for backup and repair tools are available to staffs
Develop Team (Training)	Train staffs to identify security risks and get familiar with different functional tools and resources	Provide the staffs with cybersecurity awareness education, cybersecurity- related duties and responsibilities consistent with related policies, procedures, and agreements.	Teach staffs how to use various tools to analyze and detect possible vulnerabilities	Teach staffs how to deal with different cybersecurity incidents, and incorporate the lessons learned into the plan	Train staffs on the use of repair tools and methods of executing repair plans

Manage Team	Staffs are clearly allocated to related department and team resources are inventoried	Set the content related to team discipline in the team charter, and clarify the sensitive information and resources that need authenticated access	Monitoring for unauthorized personnel, connections, devices, and software is performed	Establish good connection with the detection department to ensure that cybersecurity incidents can be reported to the response department in time	Ask staffs to use storage devices that comply with the organization's specifications in a safe manner for data backup when necessary
Procurement Management	Identify if the procured resources have lower cyber risk	Identify the resources are procured from a secured seller	Identify security vulnerabilities of procured resources	Identify the efficiency of procured resources in response to cybersecurity incidents	Identify the recovery capabilities of procured resources
Plan Procurement Management	Identify the organization’s requirements for reasonable cybersecurity resources and pontential sellers	Identify the necessary protection level of procured software and hardware	Identify the necessary tools and data resources for detection	Identify what equipment can guarantee an efficient response to cybersecurity incidents and third-party services that can be relied on	Identify the secured and reliable storage devices for the recovery
Conduct Procurement	Choose a trusted seller to trade, identify the potential business impacts and likelihoods	Make sure the procured resources comply with cybersecurity standards	Make sure the seller has not concealed product defects and potential vulnerabilities	Make sure the seller can response with necessary security risk information in time	Make sure the procured resources could be recovered
Control Procurement	Confirm that the content in the contract complies with laws and standards, and analyze whether the seller’s product has cyber risks	In the contract, procurer should ask seller to prove that the product has passed the integrity check mechanism	In the contract, procurer should clarify possible security vulnerabilities in the seller’s products and the attribution of responsibilities	In the contract, the seller should agree with voluntarily share information about security risks and respond to the purchaser in time	Reach an agreement with the seller on after-sales service to guarantee the maintenance and repair of the procurement