IT RISK MANAGEMENT FRAMEWORK & GUIDELINE

Version 1.1

FINAL

26-Jul-2023

Foo Tze Uei

Topics

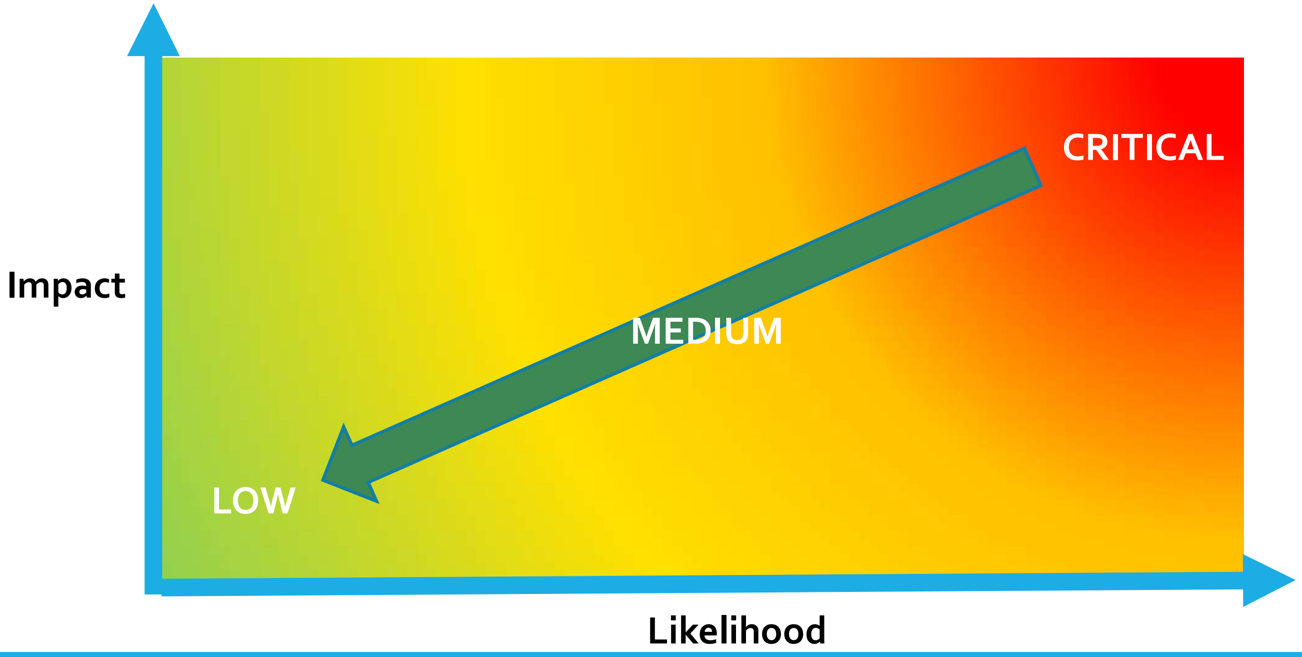
- IT Risk Management Objectives
- IT Risk Management Framework
- IT Risk Roles, Responsibilities and Team structure
- IT Risk Filtering Guidelines
- IT Risk Assessment Methodology and Process
    - ❑Step 1 – Risk Identification (Activity 1, 15mins)
    - ❑Step 2 – Risk Analysis (Activity 2, 10 mins)
    - ❑Step 3 – Risk Evaluation (Activity 3, 15 mins)
- IT Risk Register Components
- Risk Types ,Threat Sources and Impact Areas Catalogue
- What's next? (Open discussion)

Workshop Timings and Workflow

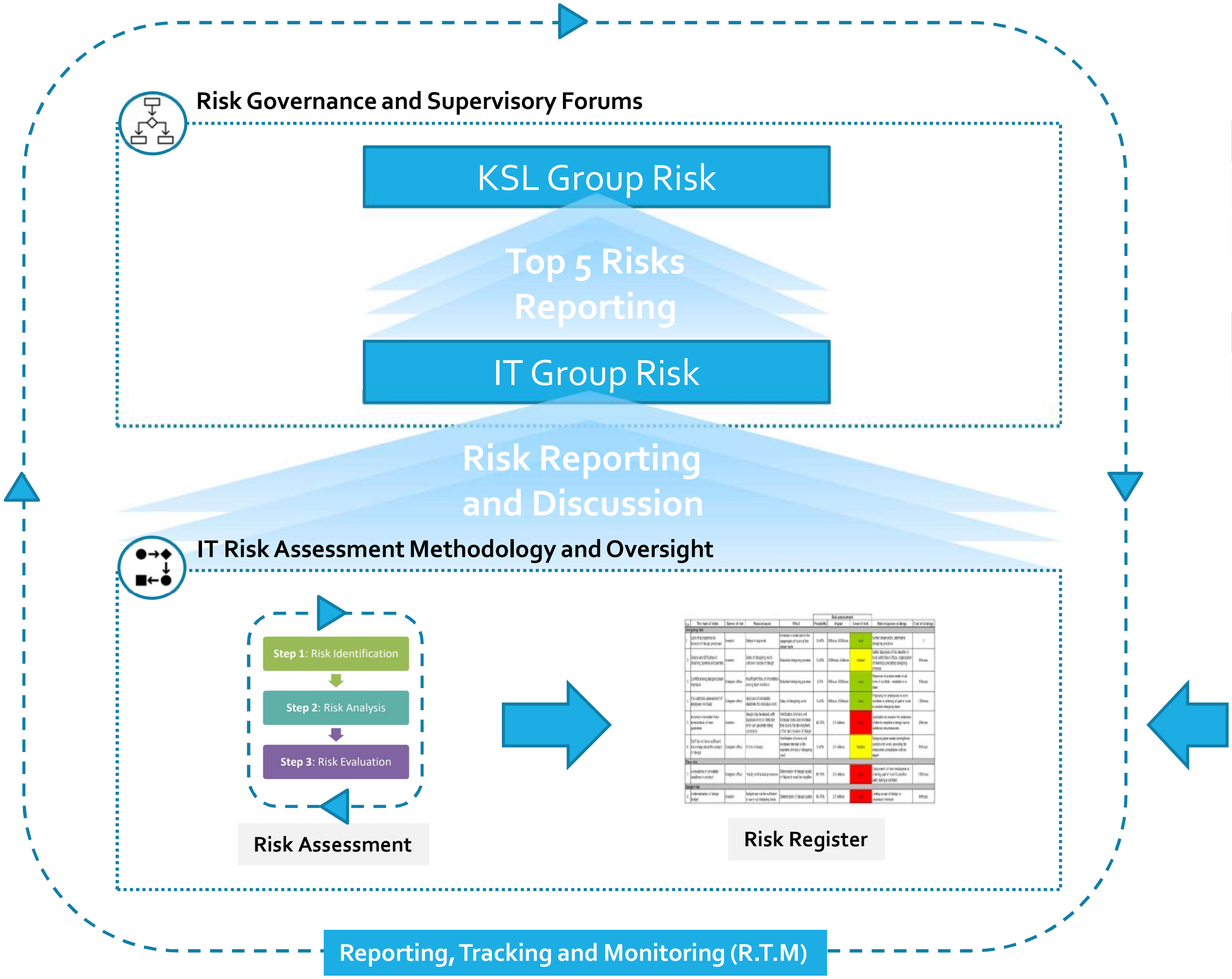
No.	Topics	Duration (Mins)
1	IT Risk Management Objectives (5 mins)	30
2	IT Risk Management Framework (10 mins)	
3	IT Risk Roles, Responsibilities and Team structure (5 mins)	
4	IT Risk Filtering Guidelines (5 mins)	
5	IT Risk Assessment Methodology and Process (5 mins)	
6	Step 1 – Risk Identification (Activity 1, 15mins)	90
	Present their information (10 mins)	
	Break (10 mins)	
7	Step 2 – Risk Analysis (Activity 2, 10 mins) UPDATED	
	Present their information (10 mins)	
	Break (10 mins)	
8	Step 3 – Risk Evaluation (Activity 3, 15 mins)	
	Present their information (10 mins)	
9	IT Risk Register Components (5 mins)	30
10	Risk Types ,Threat Sources and Impact Areas Catalogue (5 mins)	
11	What’s next? (Open discussion, 10 mins)	
12	Wrap up (SMT Closing, 10 mins)	
		150 (2.5 hrs)

IT Risk Management Key Objectives

- Resource is FINITE! Know your risks and know which areas to commit resources (i.e. Manpower, time, costs) and prioritize effort efficiently.
- Able to systematically identify, analyze and surface risks to management.
- Exposing the risks to a wider audience for their attention, acknowledgement and help
- Report; Track and Monitor all risks centrally.
- Key building block for ISO27001
- Reduce overall risk posture to LOW as much as possible.



IT Risk Management Framework



Risk Governance and Supervisory Forums

KSL Group Risk

Top 5 Risks Reporting

IT Group Risk

Risk Reporting and Discussion

IT Risk Assessment Methodology and Oversight

Step 1: Risk Identification

Step 2: Risk Analysis

Step 3: Risk Evaluation

Risk Assessment

Risk Register

Reporting, Tracking and Monitoring (R.T.M)

Groups/ Forums	Reporting Frequency
KSL Group Risk	Twice yearly
IT Group Risk	Bi-monthly

Risk Register	Review Frequency
All Active Risks	Once yearly

IT Risk Sources

- Operations
- Deviations
- Audits

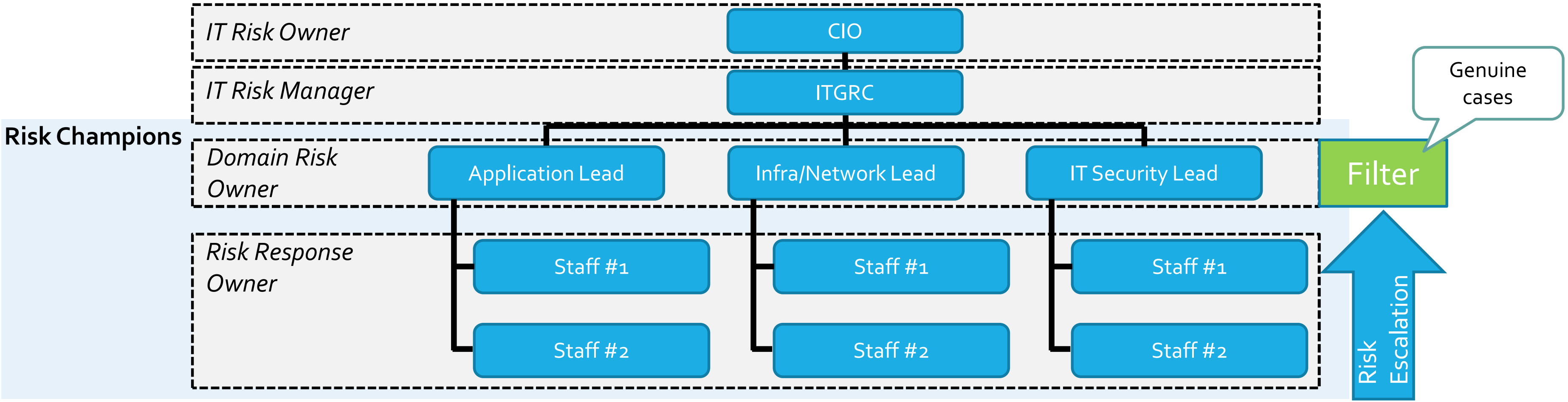
Risk Roles and Groups

- IT Risk Owner
- Domain Risk Owner
- Risk Response Owner
- Risk Champions

IT Risk Roles, Responsibilities and Team Structure

Roles	Responsibilities	
IT Risk Owner	• Ultimate risk owner of Group IT.	
IT Risk Manager	• Chairperson to ensure all reported risk are registered. • Facilitator of the risk forum	• Tracking of risk response plan to closure
Domain Risk Owner	• Overall risk owner of the domain (i.e. Application, Security, Infra/Net, Operations) • Responsible for ensuring that the residual risks remain within the organization's tolerance level.	• Filter escalated risk cases and ensure genuine cases. • Ensure the treatment and response plan is adequately addressing the risk directly. • Ensure timely completion of risk response plan
Risk Response Owner	• Provide risk treatment and response plan • Ensure timely completion of risk response plan	
Risk Champions	• Support the risk management framework • Generate risk awareness and instill risk culture amongst staff.	• Actively participating in the discussion and brainstorming of response plan.

<u>Sample</u> *Risk Team Structure*



IT Risk Owner

CIO

IT Risk Manager

ITGRC

Risk Champions

Domain Risk Owner

Application Lead

Infra/Network Lead

IT Security Lead

Risk Response Owner

Staff #1

Staff #2

Staff #1

Staff #2

Staff #1

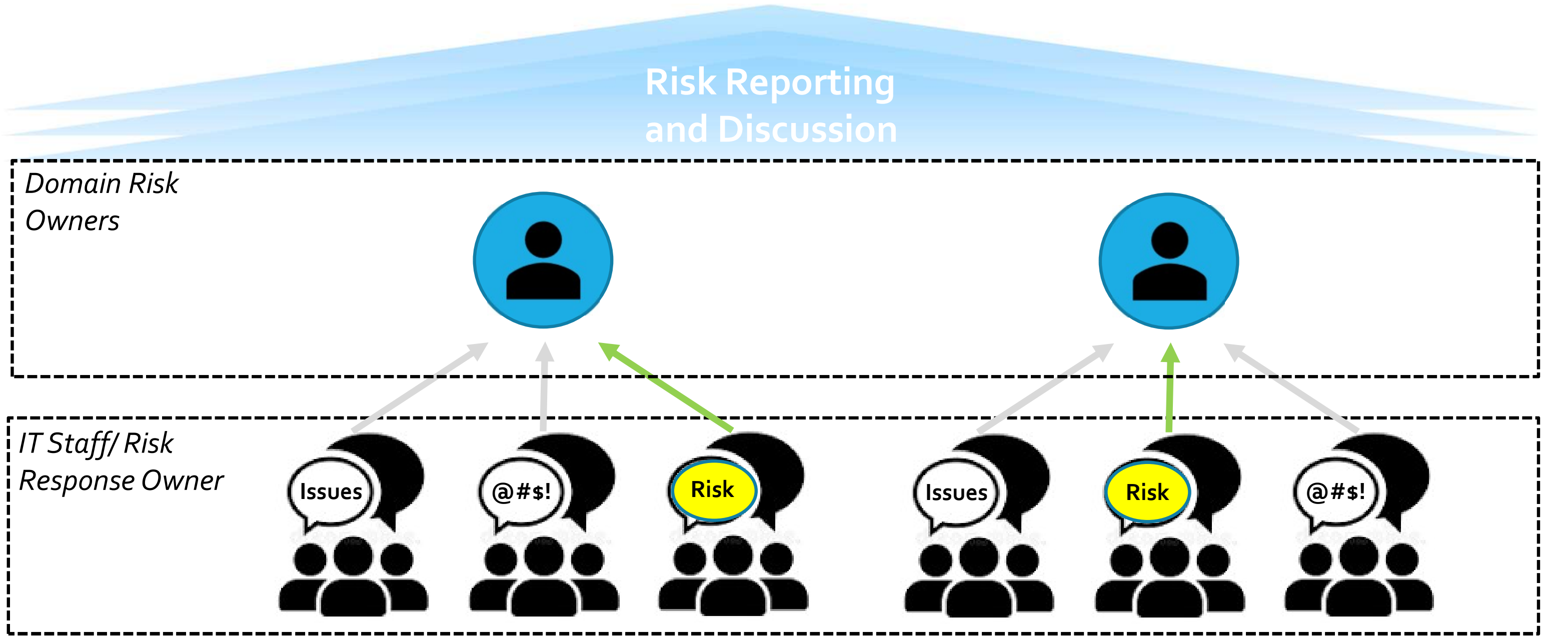
Staff #2

Filter

Genuine cases

Risk Escalation

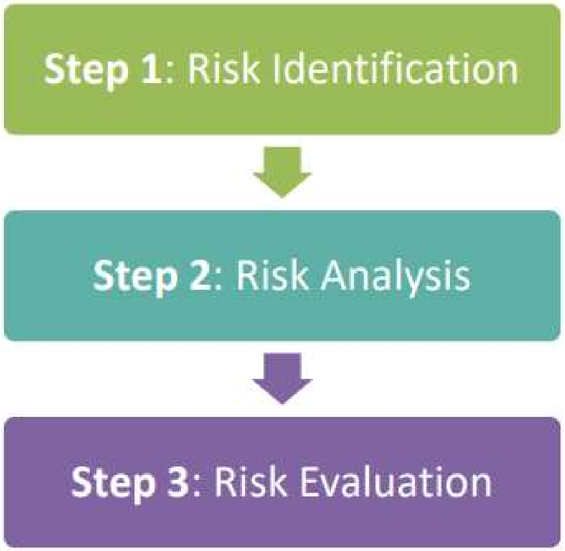
IT Risk Filtering Guidelines



- It is important to differentiate risk from noises (e.g. Complaints, issues, etc.) or end up with “dirty” risk register.
- Genuine risk cases should be identified and tabled for discussions.
  - Risk that affects business.
  - Risk that affects operation.
  - Risk cannot be resolved by the domain and needs the help from other domains to mitigate the risks.
  - Risk is ever persistent and cannot be resolved within risk tolerance level.

IT Risk Assessment Methodology and Process

Risk assessment is about identifying risks that are specific to the environment and determining the level of identified risks.



Step 1: Risk Identification

Step 2: Risk Analysis

Step 3: Risk Evaluation

Risk Identification: The process of finding and framing the risk scenario that can potentially impact the company while ensuring the risk statement which everyone can understand.

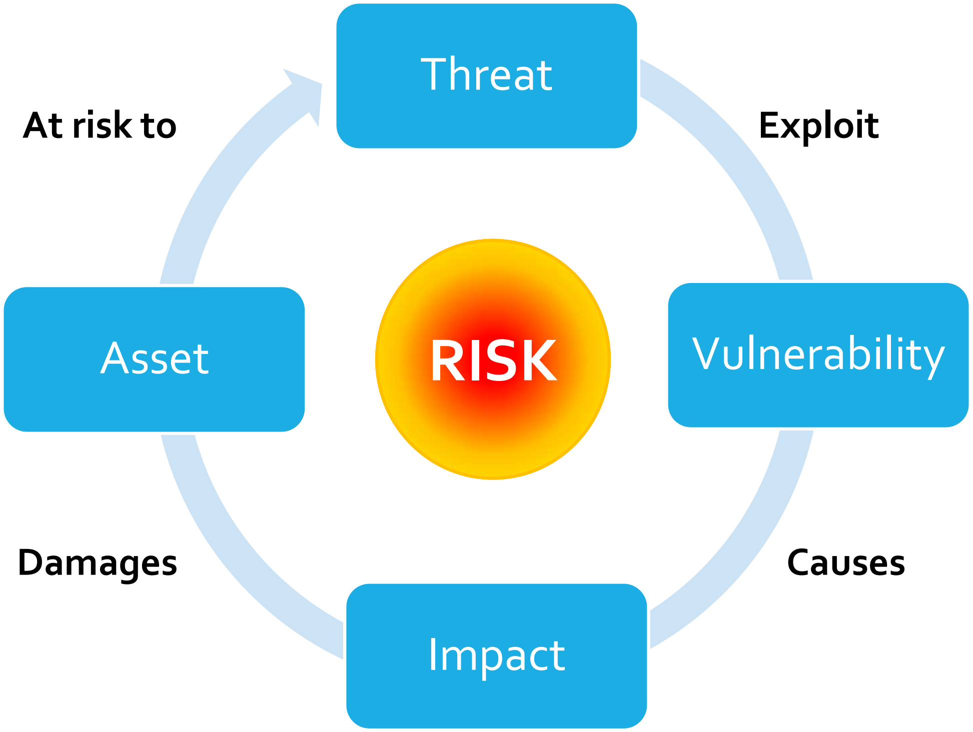
Risk Analysis: Understanding the nature of the risk with assessment on its likelihood, existing controls and residual risk.

Risk Evaluation: Knowing the weightage of all the risks, prioritize resources and select the appropriate risk treatment. (i.e. Accept, Mitigate, Avoid or Transfer)

Adapted from CSA Guide to conducting cybersecurity risk assessment for critical information infrastructure (Feb 2021)

STEP 1: Risk Identification

STEP 1 – Risk Identification: Understanding risk and establishing risk context



Context!!!
Context!!!
Context!!!

Components	Description
Risk	Scenario with the possibility of suffering harm or loss.
Threat	Any source or event that has the potential to cause harm to asset
Vulnerability	Weakness in the design, implementation and operation of an asset.
Impact Areas	Magnitude of harm resulting from a threat event exploiting a vulnerability
Asset	An object or resource of value to the company

Adapted from NIST SP 800-30R1

STEP 1 – Risk Identification: Risk scenario framing (Examples)

Risk Type	Threat	Vulnerability	Impact Areas	Asset
Intentional	Privilege User/ Administrator	With elevated privilege access	**Integrity:** Deletes or tamper logs and changes all audit traces of activities	All Servers
Structural	Controller	• Because of poor or no maintenance • Business also not agreeable to finance the upgrade or extend support contracts.	**Availability:** Crashes and loses access to key OT systems **Resources:** Frequent instability causes IT staff to be overworked	SCADA Master Station Building controls systems and other EMS equipment
Environment	Fire	Burns flammables (e.g. card boxes)	**Availability:** Can destroy the computers and equipment which impacts site services	Computer Room

Please refer to Appendix A-1 for information

Adapted from NIST SP 800-30R1

Activity 1

(15 mins)

Look HERE

Microsoft Excel Worksheet

Keep it simple and understandable

- Let's construct risk scenario you experienced in your domain and want the rest to know or help?
- Was there a case of concern you know, regardless what you do there's no possibility of changing?
- Try to provide risk scenario for each of the impacted areas (C.I.A.A.R.O).

Risk Type	Threat	Vulnerability	Impact Areas	Asset

Please refer to Appendix A-1 for risk, threat, vulnerability and impact area references

Examples of IT Risk Topics

BU

AD

Vendors

Products

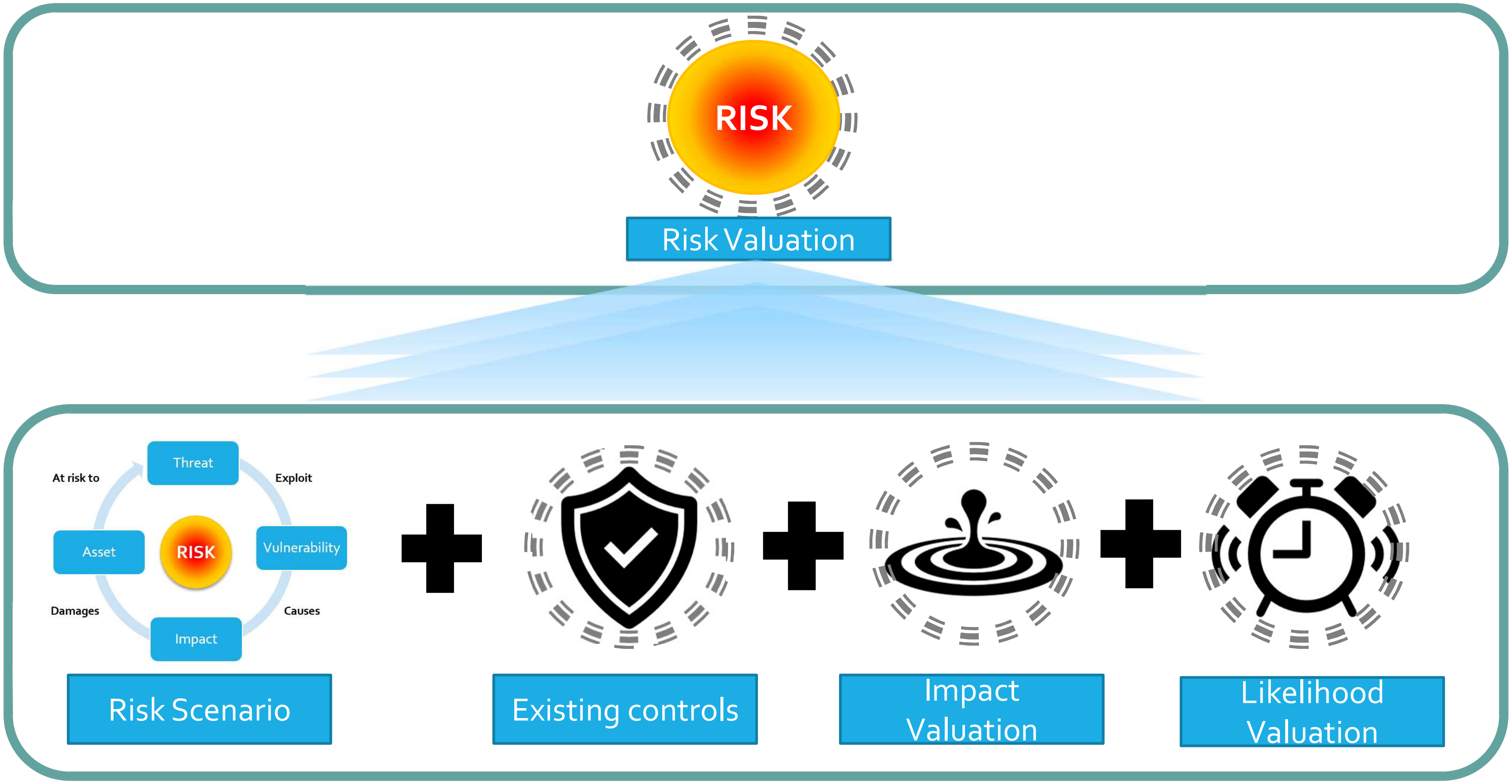
Cyber Security

Geopolitical Tensions

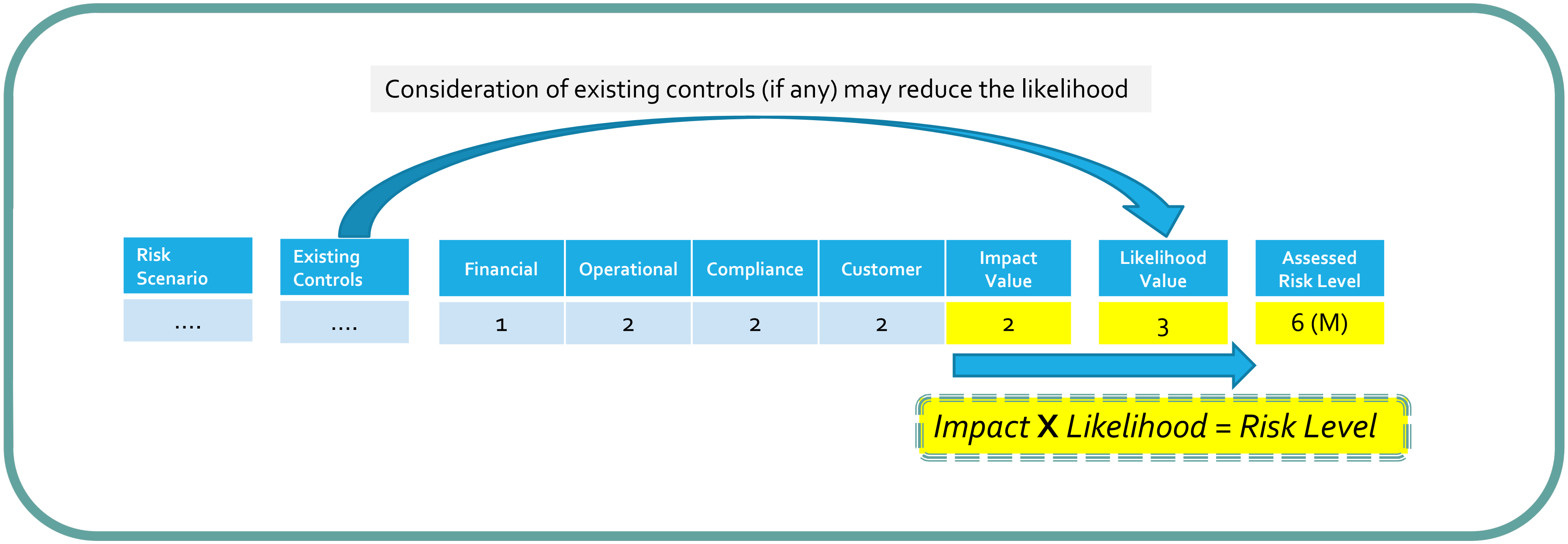
Remote Offices

STEP 2: Risk Analysis

STEP 2 – Risk Analysis: Knowing existing controls in place



STEP 2 – Risk Analysis: Knowing existing controls in place



Consideration of existing controls (if any) may reduce the likelihood

Risk Scenario	Existing Controls	Financial	Operational	Compliance	Customer	Impact Value	Likelihood Value	Assessed Risk Level
….	….	1	2	2	2	2	3	6 (M)

Impact **X** *Likelihood = Risk Level*

STEP 2 – Risk Analysis: Enterprise IMPACT Matrix (UPDATED JULY 2023)

Valuation	Type	Financial (By Business Revenue)	Operational	Compliance	Strategic (Customer)
5	Severe	$10M & above > 30%	Incident which could potentially cause: • Fatality • Unplanned Operational Downtime for vessel > 4 weeks. • Unplanned Operational downtime for shore office/ worksites* > 2 weeks • Unplanned Operational downtime for data center/site > 1 days • Critical System Unavailability Time > Recovery Time Objective by > 1 week and affects Enterprise wide.	• Significant Loss of personnel/ confidential/ business sensitive info. • Suspension of business, Revocation of licenses, • Heavy regulatory fines/ penalty • Legal action against the company & management (including any criminal charges)	• International media exposure. • Significant public concern • Long term reputational impact. • May lose customers that may impact > 20% of revenue in the short-to-medium term.
4	Major	$5M to < $10M 15% - < 30%	Incident which could potentially cause: • Permanent disabilities/ acute injuries/chronic effects. • Unplanned Operational Downtime for vessel 2 weeks – 4 weeks • Unplanned Operational downtime for shore office/worksites* 1 week – 2 weeks • Unplanned Operational downtime data center/site 12 hours – 24 hours • Critical System Unavailability Time > Recovery Time Objective by > 3 working days and affects more than 2 Bus.	• Loss of personnel/ confidential/ business sensitive info. • Reputational impact • Regulatory scrutiny/ fines/ LDs/ penalties restrictive measures/ investigation / sanctions • Legal actions against the company	• National media exposure. • Some public concern • Medium term reputational impact. • May lose customers that may impact 10% - 20% of revenue in the short-to-medium term.
3	Moderate	$2M to < $5M 10% - < 15%	Incident which could potentially cause: • RWC (Restricted Work Case) or LWC (Loss of Work Case) • Unplanned Operational Downtime for vessel 2 days – < 2 weeks • Unplanned Operational downtime for shore office/worksites* 1 day – < 1 week • Unplanned Operational downtime for data center/site 1 hour – < 12 hours • Critical System Unavailability Time > Recovery Time Objective.	• Potential breach of any regulation/contract liabilities • Loss of business info, which is not confidential/sensitive	• Several written complaints received. • Industry knowledge of incident but no media coverage. Short term reputational impact. • May lose customers that may impact 5% -
2	Minor	$200K to < $2M 5% - < 10%	Incident which could potentially cause: • Injuries requiring medical treatment • Unplanned Operational Downtime for vessel < 2 days • Unplanned Operational downtime for shore office/worksites* < 1 day • Unplanned Operational downtime for data center/site < 1 hour • Critical System Unavailability Time > Recovery Time Objective within 8 office hours and affects a single BU.	• Minor breaches with no liabilities or regulatory impact	• Isolated letter of complaint. • Reputational damage limited to a few customers. • May lose customer relationships
1	Insignificant	< $200K < 5%	Incident which could potentially cause: • First Aid cases/Minor Injuries • No disruption/off hire days • Critical System Unavailability Time <= Recovery Time Objective and affects small group of users within a single BU.	• No impact to environment, contract liabilities and/or regulations	• Verbal or unofficial feedback received from external parties. • Reputational damage contained internally. • Do not impact customer relationships.

STEP 2 – Risk Analysis: LIKELIHOOD Matrix (UPDATED JULY 2023)

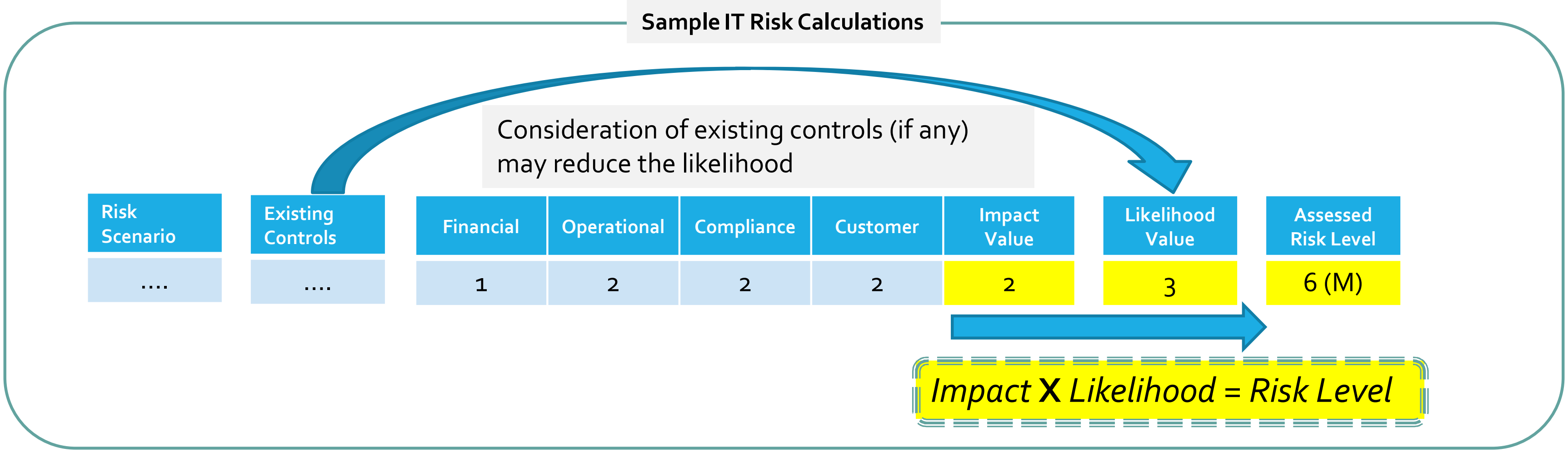
Valuation	Type	Quantitative Estimation	Qualitative Estimation
5	Almost certain	• Known to occur several times a year • >75% chance of happening.	• Nature / business environment is highly susceptible to the risk; • Occurrence is highly probable; • Situation is expected to occur in most circumstances or is already occurring. • Happens several times per year at organisation/ worksites/ vessel
4	Likely	• Likely to occur several times a year. • >50% chance of happening.	• Nature / business environment is susceptible to the risk; • Occurrence is probable; • Situation is expected to occur in some circumstances. • Happens several times per year in our organisation / industry
3	Possible	• Historically happening between 1 time annually or every 1-3 years. • >20% - 50% chance of happening.	• Nature / business environment is susceptible to the risk; • Occurrence may be reasonably possible; Situation will probably occur in some circumstances. • Occurred within our organisation.
2	Unlikely	• Historically happening only once annually and/or sporadically over last 5 years. • <20% chance of happening.	• Nature / business environment is minimally susceptible to the risk, but occurrence is low; Occurred in the industry, at least once.
1	Highly Unlikely	• Historically happening sporadically over last 10 years. • May not have sufficient data to back the frequency • ≤1% chance of occurring.	• Nature / business environment is minimally susceptible to the risk, but occurrence is remote. Situation will probably occur in very exceptional circumstances. • No knowledge / never heard of such situation in the organisation/ industry.

Activity 2

(10 mins)

Keeping it real and honest

- Following Activity 1, do you think we have some existing controls of relevance to the risk scenario?
- Let’s estimate the impact and likelihood
- What do you think is the actual risk level at this point? Do you think it’s fair or needs adjustments?



Sample IT Risk Calculations

Consideration of existing controls (if any) may reduce the likelihood

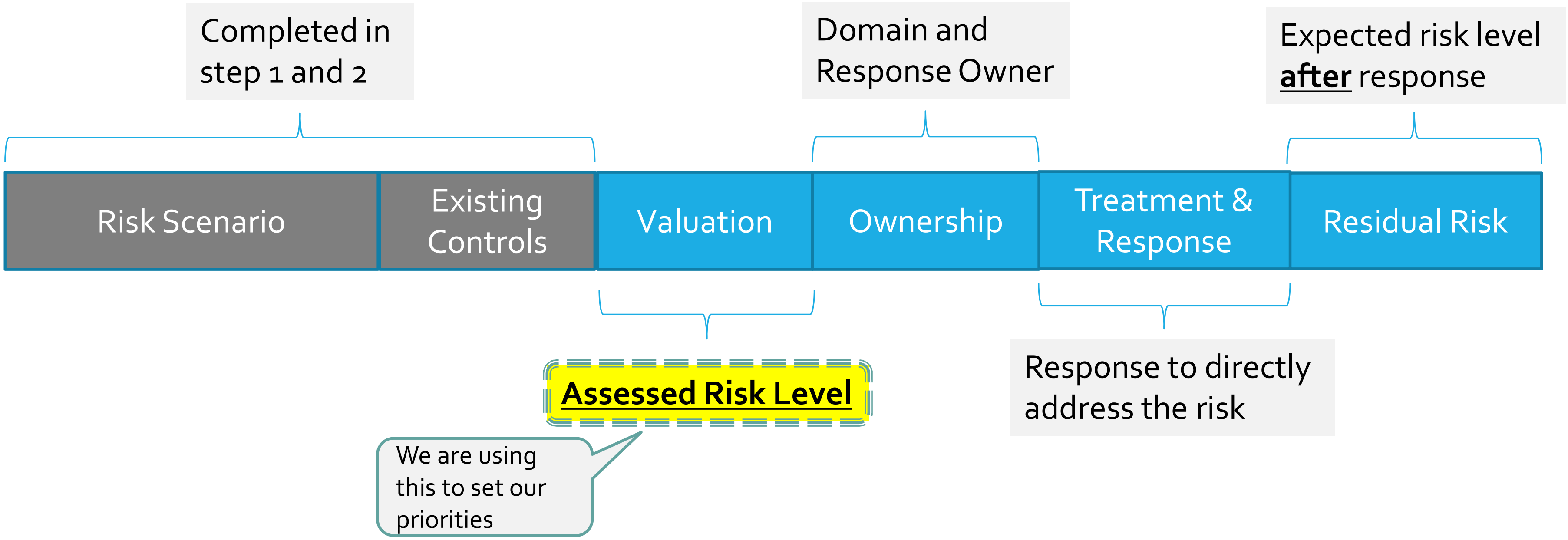
Risk Scenario	Existing Controls	Financial	Operational	Compliance	Customer	Impact Value	Likelihood Value	Assessed Risk Level
....	....	1	2	2	2	2	3	6 (M)

Impact **X** *Likelihood = Risk Level*

STEP 3: Risk Evaluation

STEP 3 – Risk Evaluation

Risk Evaluation – Measuring risk against the company's risk appetite and tolerance level to determine and understand the significance of risk level. Once that is established, we can prioritize which risk to action upon first and if the response is adequate.



Completed in step 1 and 2

Domain and Response Owner

Expected risk level **<u>after</u>** response

Risk Scenario | Existing Controls | Valuation | Ownership | Treatment & Response | Residual Risk

<u>Assessed Risk Level</u>

Response to directly address the risk

We are using this to set our priorities

Adapted from CSA Guide to conducting cybersecurity risk assessment for critical information infrastructure (Feb 2021)

STEP 3 – Risk Evaluation: Prioritisation through Risk Matrix

CATASTROPHIC (5)	Low(5)	Medium(10)	High(15)	High(20)	Critical(25)
MAJOR (4)	Low(4)	Medium(8)	Medium(12)	High(16)	High(20)
MODERATE (3)	Low(3)	Medium(6)	Medium(9)	Medium(12)	High(15)
MINOR (2)	Low(2)	Low(4)	Medium(6)	Medium(8)	Medium(10)
INSIGNIFICANT (1)	Low(1)	Low(2)	Low(3)	Low(4)	Low(5)
	Highly Unlikely (1)	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Almost certain (5)**

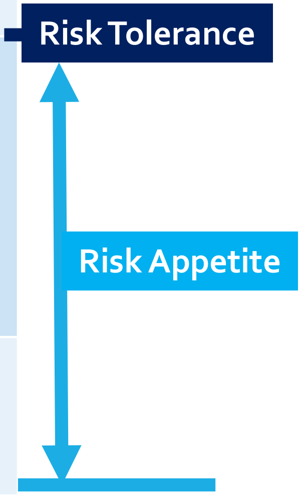
Risk Level	Range	Timeframe
Low	1 to 5	KIV or 12 months
Medium	6 to 12	3 - 6 months
High	15 to 20	1 - 3 months
Critical	25	ASAP – 1 month

Timeframe stipulated here serve as a generic guide; IT Security or Cyber Security (e.g. Pen-test, product patching, etc.) will reference from Patch Management Standards.

Adapted from NIST SP 800-30R1

STEP 3 – Risk Evaluation: Group IT's Risk Tolerance and Appetite that help us set priorities

Risk Level	Description	Risk Appetite
Critical	This level of risk **cannot be accepted** and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken **immediately or as soon as possible**.	Unacceptable
High	This level of risk **cannot be accepted**. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 to 3 months or when *achievable.	Unacceptable
Medium	This level of risk **can be accepted IF** there are no treatment strategies that can be easily and/or economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately. Where possible treatment strategies aimed at reducing the risk level should be developed in the next 6 to 12 months or when *achievable.	Conditional Acceptance
Low	This level of risk can be accepted and if the risk level remains unchanged over a period of time it can be closed especially when there are no reported cases recently.	Accepted



Risk Tolerance

Risk Appetite

*Achievable means when all needed resources are available as sometimes there are cases with delay or events delay (e.g. Supply shortage; pandemic; etc.)

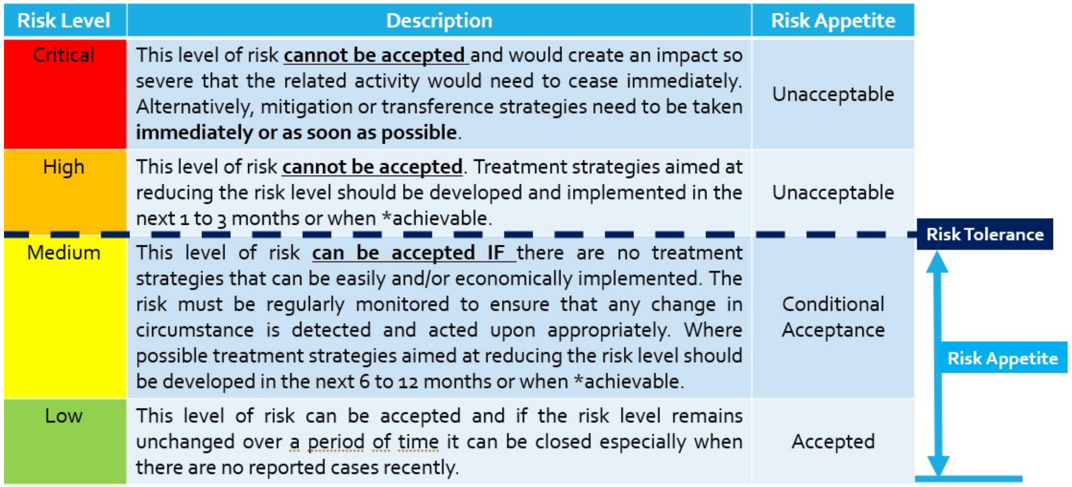
Adapted from CSA Guide to conducting cybersecurity risk assessment for critical information infrastructure (Feb 2021)

Activity 3

(15 mins)

Let’s go!!!

- Following Activity 2, we to look at those critical and high priorities.
- What do you think is our treatment and response plan?
- Are we able to lower their residual risk to acceptable levels?
- Let’s get the right resources and work on them.



Risk Level	Description	Risk Appetite
Critical	This level of risk **cannot be accepted** and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken **immediately or as soon as possible**.	Unacceptable
High	This level of risk **cannot be accepted**. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 to 3 months or when *achievable.	Unacceptable
Medium	This level of risk **can be accepted IF** there are no treatment strategies that can be easily and/or economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately. Where possible treatment strategies aimed at reducing the risk level should be developed in the next 6 to 12 months or when *achievable.	Conditional Acceptance
Low	This level of risk can be accepted and if the risk level remains unchanged over a period of time it can be closed especially when there are no reported cases recently.	Accepted

IT Risk Register Components

Risk register a centralized repository to document and track all identified risk.

Components	Description
Date of Entry	The date of risk has been reported/ filed.
Risk ID	Risk numbering for ease of reporting and tracking
Status	Current Status (Open, Closed, In-progress)
Risk Owner	The ultimate owner or domain owner of the IT risk
Risk Scenario	Risk scenario framing of how it affects the company
Risk Source	Source of reporting for this risk (e.g. Audit, Ops, Deviation, etc.)
Risk Type	Refer to A1
Existing controls	All existing controls that can reduce the likelihood
Assessed Risk Level (Impact and Likelihood)	Refer to Step 2 (Low, Medium, High, Critical)
Risk Action/ Response Owner	The assigned person/team to respond to risk reported
Risk Treatment Type	Treatment type (Avoid, Mitigate, Transfer, Accept)
Response Description	Detailed information of response
Residual Risk Level	Expected risk level **after** suggested response
Target Date	Expected completion date of response
Notes	Any other notes, including delay or change log

Status	Description
Open	New open risk case for discussion
Closed	Nothing to follow-up and/or risk not shown over last 12 months
In-progress	Risk management in progress
Active	Risk is active and monitored
Rejected	Risk is rejected after assessment

Treatment	Description
Avoid	Stop the action/ activity to evade the risk
Mitigate	Reduction of risk level within tolerance; Default and preferred method
Transfer	Move the risk to another entity to offset the risk impact; Accountability is not moved.
Accept	Do nothing as there are no treatment strategies that can be easily and/or economically implemented to further address risk.

WHAT'S NEXT?

APPENDIX

A1 – Risk Types ,Threat Sources and Impact Areas Catalogue

	Risk Type	Threat Sources		Impact Areas	Description
Adversarial	**Intentional**	**Individual** • Outsider • Insider • Trusted Insider • Privileged Insider **Group** • Ad hoc • Established	**Organization** • Competitor • Supplier/ Vendor • Partner/ JV • Customer • Nation-State	• Confidentiality • Integrity • Availability • Authentication • Resources • Others	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).
Non-adversarial	**Accidental**	• User • Privileged User/Administrator	**Organization** • Competitor • Supplier/ Vendor • Partner/ JV		Erroneous actions taken by individuals in the course of executing their everyday responsibilities.
	Structural	**Information Technology (IT) Equipment** • Servers/ Devices • Storage • Processing • Communications • Sensor (OT) • Controller (OT)	**Environmental Controls** • Temperature/Humidity Controls • Power Supply **Software and Services** • Operating System • Networking • General-Purpose Application • Mission-Specific Application • Cloud Computing (e.g. IAAS/PAAS/SAAS)		Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
	Environmental	**Natural or man-made disaster** • Fire • Flood/Tsunami • Windstorm/Tornado • Hurricane • Earthquake • War/ Bombing/ Riots/ Protests • Geopolitical tensions	**Unusual Natural Event** • Sunspots **Infrastructure Failure/Outage** • Telecommunications • Electrical Power		Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.

Adapted from NIST SP 800-30R1

THE END