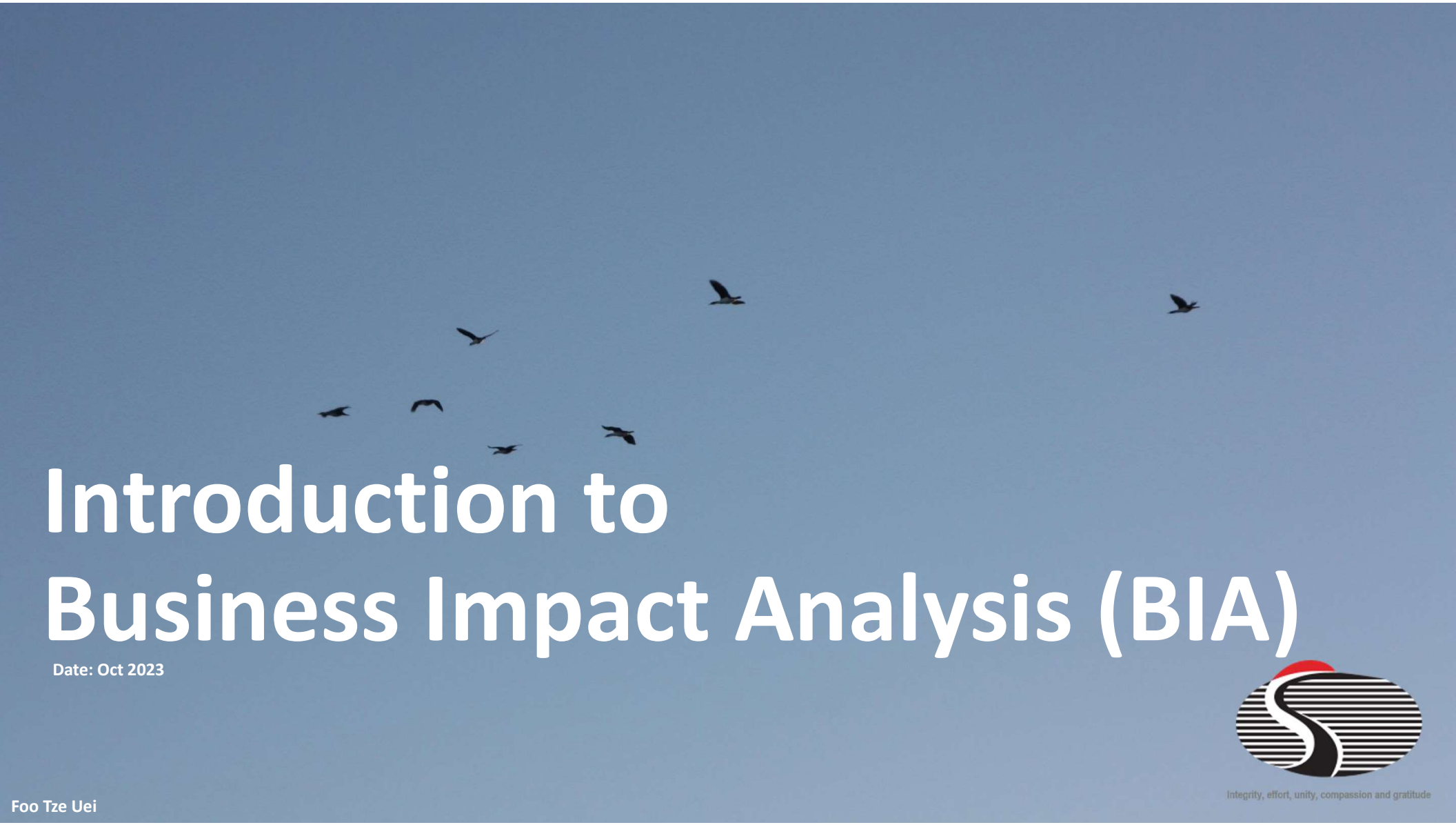


Introduction to Business Impact Analysis (BIA)

Date: Oct 2023

Foo Tze Uei

Integrity, effort, unity, compassion and gratitude

Topics

- Preface: Objectives of this exercise
- Preface: Scenario considered out of scope
- BIA Concepts
- Risk Management Impact Matrix
- Data Classification
- BIA Assessment Template Overview
- Weighted impact ratings
- Determining RTO/RPO
- Other examples of determining RTO/RPO

Preface: Objectives of this exercise

1. BIA discussed and presented herein focuses on how **UNAVAILABILITY** of the System/Application/Service that could be caused by various reasons which could impact the business.
2. Business to **gauge** their tolerance/ threshold level during duress and hardship.
3. BIA assessment by the business can determine the following.

System Recovery priority

Compliance & Legal

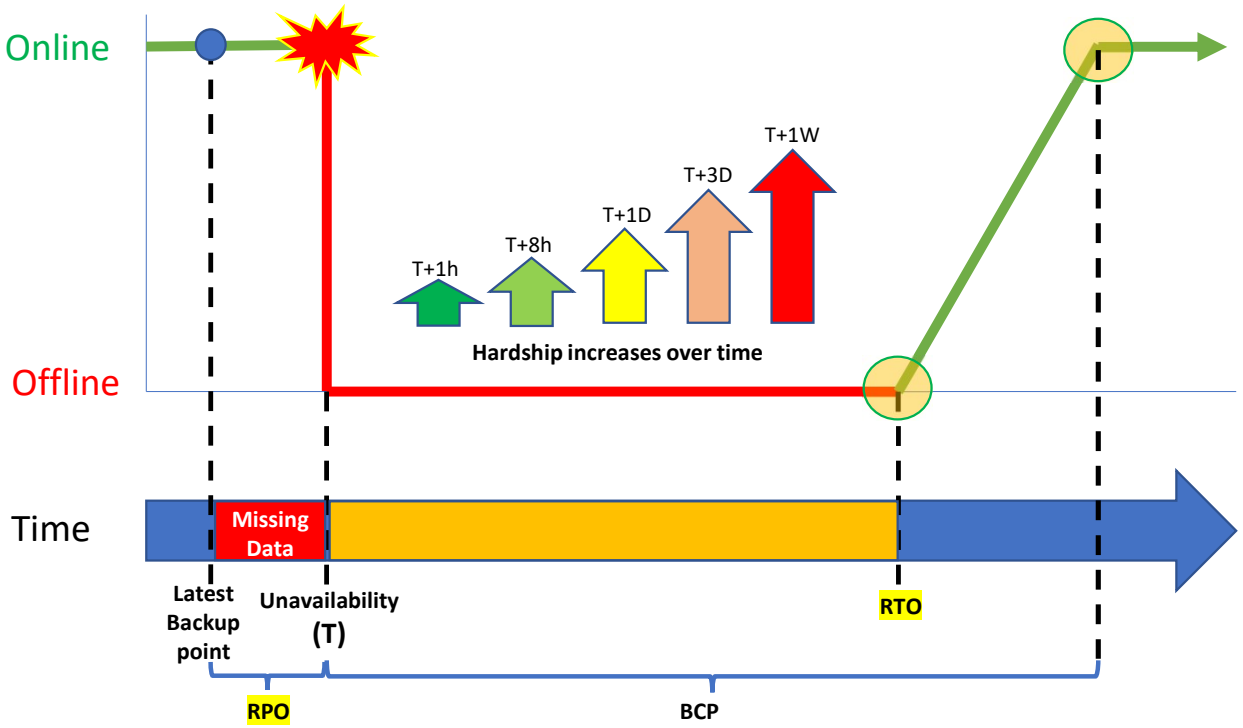
Company, business, operational strain

Recovery duration (RTO), Backup frequency (RPO)

Preface: Scenario considered OUT OF SCOPE

- Data Backup Corruption and complete loss of data
- CyberAttack (i.e. Ransomware, virus, etc.) rendering data irretrievable.
- Theft or espionage
- Events that involves uncontrollable circumstances such as warfare or calamity.
- This exercise is not about setting up the BCP but to estimate the RTO and RPO of the affected business/service.

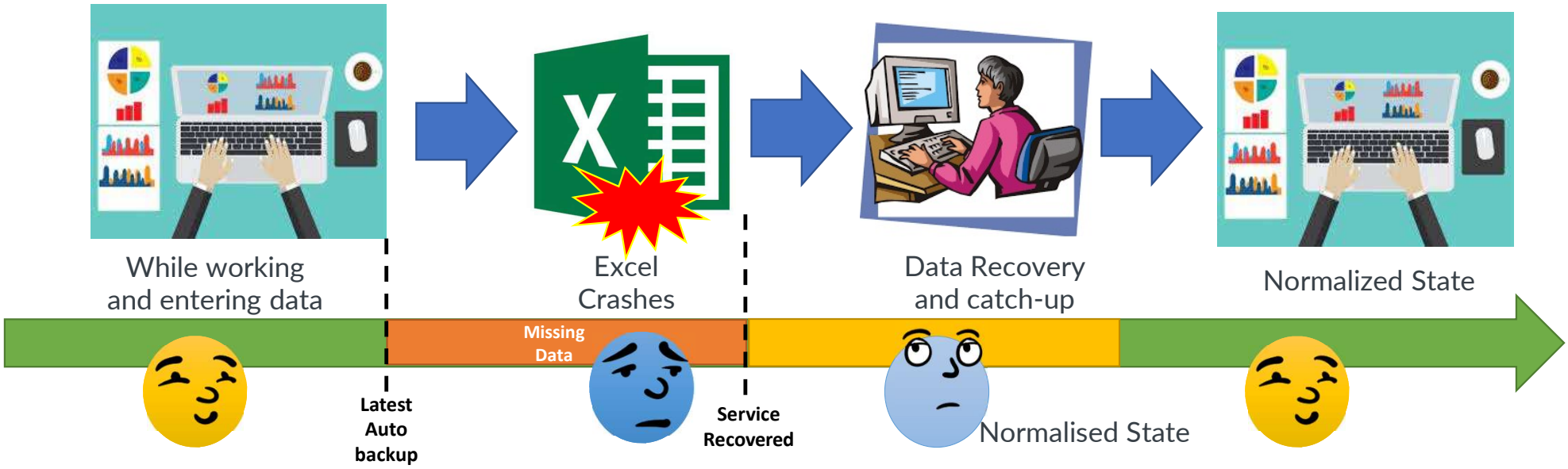
BIA Concepts



Key Terms	Definition
Online	System/Application/Service is connectable, available and operating as per normal.
Offline	System/Application/Service is unavailable for business use.
RPO	**R**ecovery **P**oint **O**bjective determines the data backup point **from which** the business identifies can afford to lose. This determines the backup frequency.
Missing Data	Data that is lost between last backup to time of disaster. The amount of data loss or missing during this period can be supplemented with BCP with tolerable impact to business.
Unavailability (T)	An incident that has affected the availability of the System/Application/Service impacting business.
RTO	**R**ecovery **T**ime **O**bjective determines the duration needed to restore System/Application/Service
BCP	Business Continuity Plan a set of plan and procedure from business to ensure it can function without the availability of System/Application/Service. (i.e. Manual workarounds)

Understanding RPO

RPO designates the variable amount of data that will be lost or will have to be re-entered upon service resumes.



Risk Management Impact Matrix (As defined by KSL ERM)

Impact categories/ thresholds	Insignificant	Minor	Moderate	Major	Severe
Financial (US$)**	**< $200K**	**$200K to < $2M**	**$2M to < $5M**	**$5M to < $10M**	**$10M & above**
Financial (% of variance from annual budget) – to specify the budget	**< 5%**	**5% - <10%**	**10% - <15%**	**15% - <30%**	**>30%**
Reputational Impact (Include • Media exposure, • Complaints • Customer loss, • Regulatory/ Contractual impact)	• Verbal or unofficial feedback received from external parties. • Reputational damage contained internally. • Do not impact customer relationships. • No impact to loss of market share	• Isolated letter of complaint. • Reputational damage limited to a few customers. • May lose customer relationships <5% of revenue. Can be recovered/re-built within the short term. • Loss of minimal market share but recoverable in the short term • Minor breaches with no liabilities or regulatory impact	• Several written complaints received. • Industry knowledge of incident but no media coverage. • Short term reputational impact. • May lose customers that may impact 5% - <10% of revenue in the short-to-medium term. Can be recovered/re-built within the medium term. • Loss of moderate market share but recoverable in the medium term. • Potential breach of any regulation/contract liabilities.	• 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. • Loss of significant market share • Potentially subject to regulatory scrutiny/ fines/ LDs/ penalties restrictive measures investigation / sanctions or legal actions against the company	• 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. • Loss of market share which results in a loss of its competitive edge in the long term. • Potentially subject to suspension of business activity, revocation of licenses, or large-scale legal action against the company and management (including any criminal charges)

**Standard metric will be based on EBITDA. Other metrics (e.g. revenue or costs) may alternatively be used, where justified.

Risk Management Impact Matrix (As defined by KSL ERM)

… continued from previous page

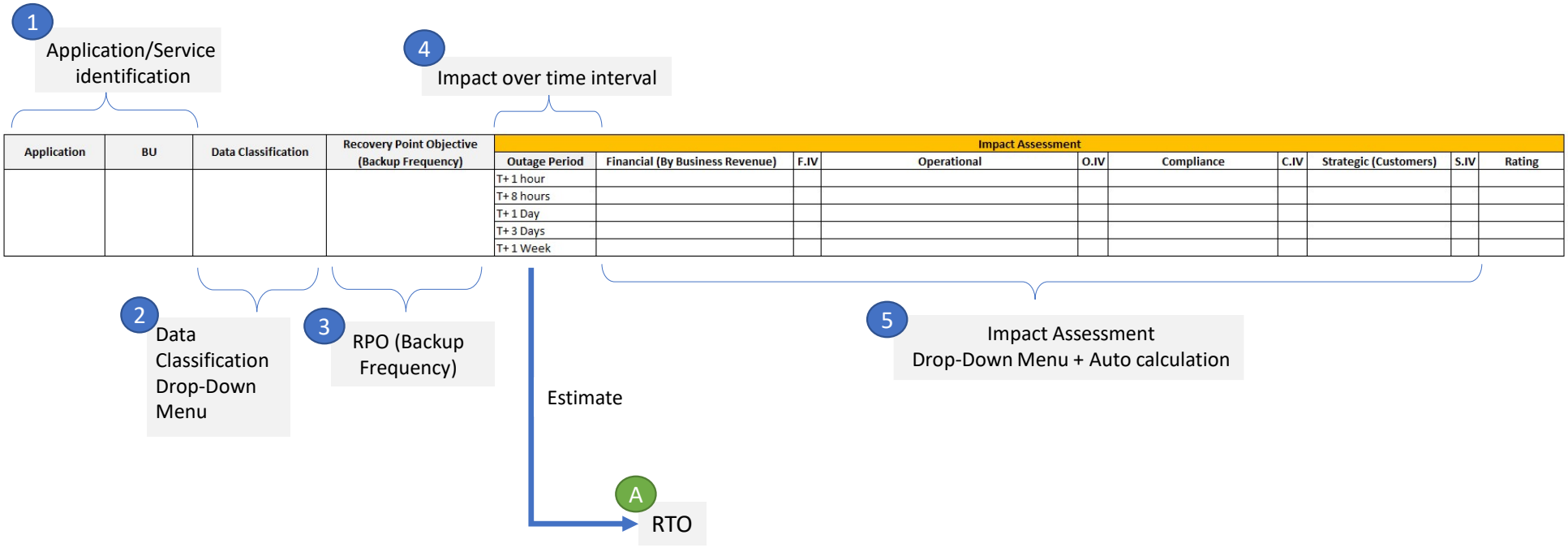
			Moderate	Major	Severe
Operational & HSSE Impact (Include impact to • People, • Operational downtime, • Environment, • Asset - Vessel/ Property loss & damage, Security, • Loss of business/ personnel info, • Regulatory/ Customer requirements & Contract liabilities)		Incident which could potentially cause:	Repeated incidents which could potentially indicate systemic issues.	Incident which could potentially cause:	Incident which could potentially cause:
	• First Aid cases/Minor Injuries	• Injuries requiring medical treatment.	Incident which could potentially cause: • RWC (Restricted Work Case) or LWC (Loss of Work Case)	• Permanent disabilities/ acute injuries/chronic effects.	• Fatality
	• No disruption/off hire days • Critical System Unavailability Time <= Recovery Time Objective and affects small group of users within a single BU	• 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	• 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 within 3 working days and affects 2 BUs	• 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	• 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
	• No impact to environment.	• Minor impact to environment, with impact contained internally.	• Short term environmental impact, with impact requiring a single external support.	• Medium term environment impact requiring multiple external support	• Long term/large scale environmental impact requiring multi-tiered response.
	• No asset loss • No loss of info	• Total asset/vessel/property loss/damage < 1% total assets (including incidents resulting from fire, pollution in water, collision, grounding, allision, security incidents)	• Total asset/vessel/property loss/damage 1-3% total assets ((including incidents resulting from fire, pollution in water, collision, grounding, allision, security incidents) • Loss of business info, which is not confidential/sensitive.	• Total asset/vessel/property loss/damage 4-5% total assets (including incidents resulting from fire, pollution in water, collision, grounding, allision, security incidents) • Loss of personnel/ confidential/ business sensitive info.	• Total asset/vessel/property loss/damage > 5% total assets (including incidents resulting from fire, pollution in water, collision, grounding, allision, security incidents) • Significant Loss of personnel/ confidential/ business sensitive info.
			• Breach of customer requirements & contract liabilities and/or regulations	• Reputational impact • Regulatory scrutiny/ fines/ LDs/ penalties restrictive measures/ investigation / sanctions • Legal actions against the company	• Suspension of business, Revocation of licenses, • Heavy regulatory fines/ penalty • Legal action against the company & management (including any criminal charges)

*Worksites refer to entire or significant portion of the work area. E.g. For PaxOcean, it refers to the entire or significant area of the shipyard and/or office. For Allgreen, refers to the entire or significant area of the malls, GWSA, office and/or project sites.

Data Classification

Data Classification	Description	Assessment Critieria						Examples
		Is it publicly available?	Distribution Group	Impacts individuals?	Impacts customers?	Financial Loss?	Regulatory penalties or litigation?	
• Level 0 - Public (or unclassified)	• Content readily and freely available to the public. • Content for public distribution; • Content is to wider audiences.	Yes	External	No	No	No	No	Marketing materials; job description; etc.
• Level 1 - Internal	• Internally circulated content that is meant for the staff or vendors with KSL. • Default setting for most information transacted within the company.	No	Internal	No	No	No	No	Internally circulated content or emails. Policies, procedure, etc.
• Level 2 - Confidential	• Content that contains sensitive information that directly impacts individual. • Could lead to escalation to senior management.	No	Internal	Yes	No	Possible	Possible	Personal details (i.e. NRIC, account details, medical details, birth certificate); payslip; Audit Reports; VA Scan reports; etc; Pricings.
• Level 3 - Sensitive	• Controlled information that is tightly controlled by the senior management. • Impacts the company substantially. • Very limited distribution and audience group.	No	Internal	Possible	Yes	Yes	Possible	M&A contracts; trade secrets; intellectual properties; etc.

BIA Assessment Template Overview



Template

Microsoft Excel Worksheet

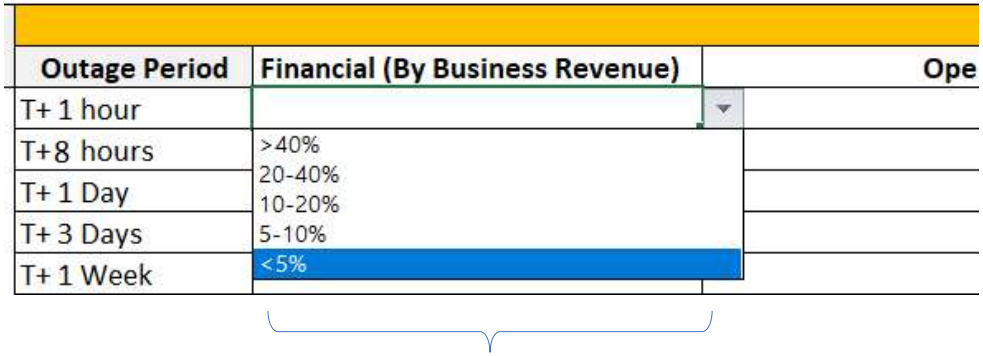
Data Classification Assessment

Application	BU	Data Classification	Recovery Point Objective (Backup Frequency)	Outage Period	Financial (By Business Revenue)	F.IV
				T+ 1 hour		
				T+ 8 hours		
				T+ 1 Day		
				T+ 3 Days		
				T+ 1 Week		

- Level 0 - Public (or unclassified)
- Level 1 - Internal
- Level 2 - Confidential
- Level 3 - Sensitive

- Drop-down menu selection of data classification
- Refer to the Data Classification table
- Please take the highest data classification where possible when accounting for all data classifications processed.

Impact Assessment

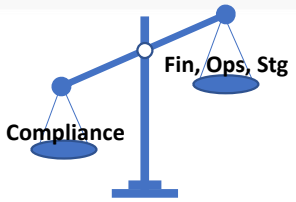


5x

- Impact over time assessment by each row
- Drop-down menu selection for Impact assessment.
- For no business impact, please select “<5%”
- Refer to Risk Management Impact Matrix table for guidance.
- Qualitative estimates by impact over time principle. Impact to business by the first hour, third hour and so on.

Weighted impact ratings

Impact Assessment					
Outage Period	Financial (By Business Revenue)	Operational	Compliance	Strategic (Customers)	Rating
T+ 1 hour	<5%	Insignificant or minimal interruptions to business operations within a single functional group < 1/2 day. No loss of internal information. Minimal to no impact to operational support and manual work can be sustained during outage.	Minor breaches with no liabilities or regulatory impact	Insignificant or minimal impact on customer relationships and contracts.	1
T+ 8 hours	<5%	A functional group Minor interruptions to business operations within a single functional group <1 day. Loss/corrupted internal information with low impact. Minimal impact to operational support and manual work can be sustained during outage.	Minor breaches with no liabilities or regulatory impact	Impact on <10% of customer relationships and contracts, which may be fully repaired in short term.	2
T+ 1 Day	<5%	Enterprise wide Inability to continue BAU across all functional groups > 3 days. Loss of confidential data that will incur financial losses. Significant impact to operational support and manual work can be difficult to sustain during outage.	Minor breaches with no liabilities or regulatory impact	Insignificant or minimal impact on customer relationships and contracts.	2
T+ 3 Days	<5%	Enterprise wide Significant interruptions (1-3 days) to BAU across all functional groups. Loss of confidential data with significant impact. Impacts operational support badly and operational support suffers hardship during outage.	Management unaffected Minor legal liabilities/restrictive measures Potential regulatory attention	Impact on 51 - 75% of customer relationships and contracts, requiring a long term recovery plan.	3
T+ 1 Week	<5%	Enterprise wide Inability to continue BAU across all functional groups > 3 days. Loss of confidential data that will incur financial losses. Significant impact to operational support and manual work can be difficult to sustain during outage.	Large Scale Legal Actions against the Company and Management Regulatory Sanctions Revoke of licenses/ suspension	Impact on 76 - 100% of customer relationships and contracts. Complete erosion of trust and confidence and potentially irreparable.	4
					3

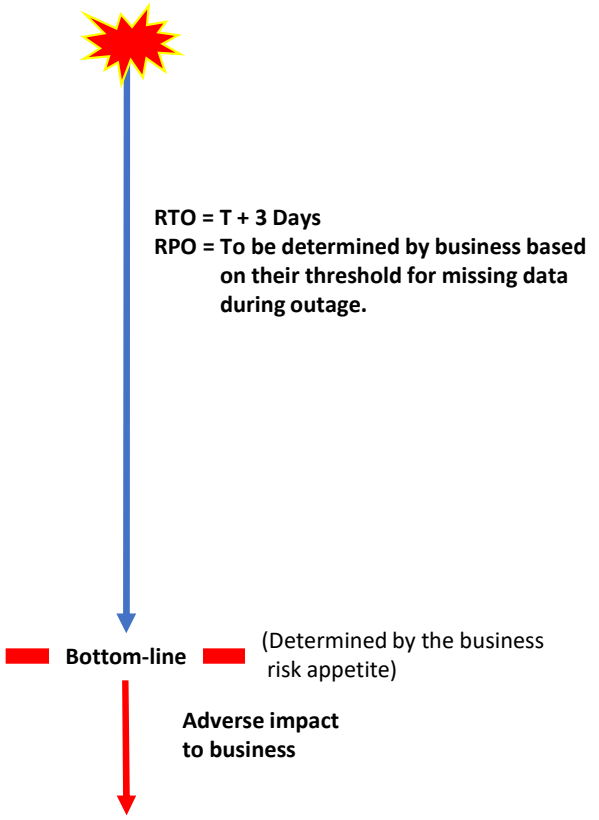


Weighted ratings with compliance weighted more than the others (i.e. Financial, Operations, Strategic)

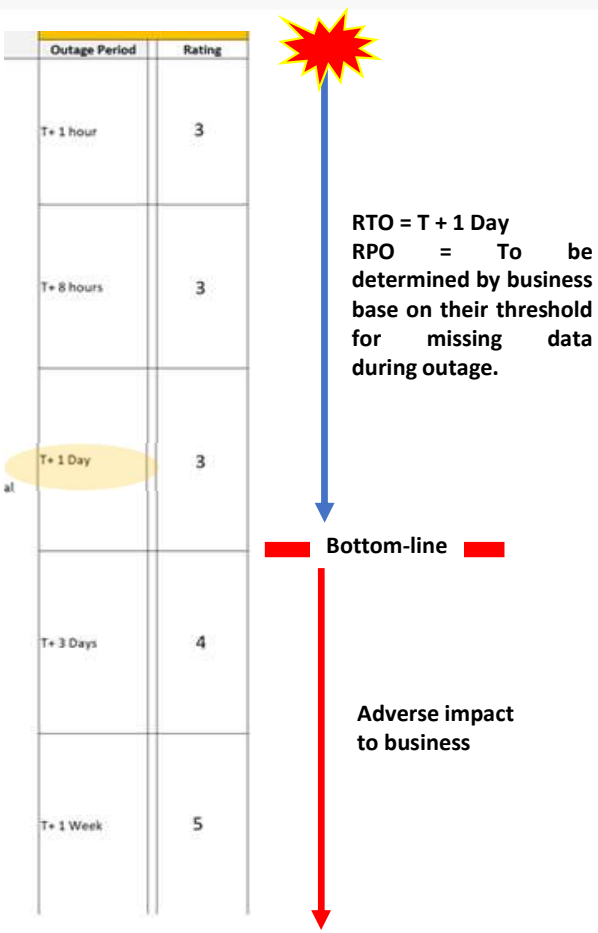
Average ratings from the assessment determines the overall criticality/priority of the application.

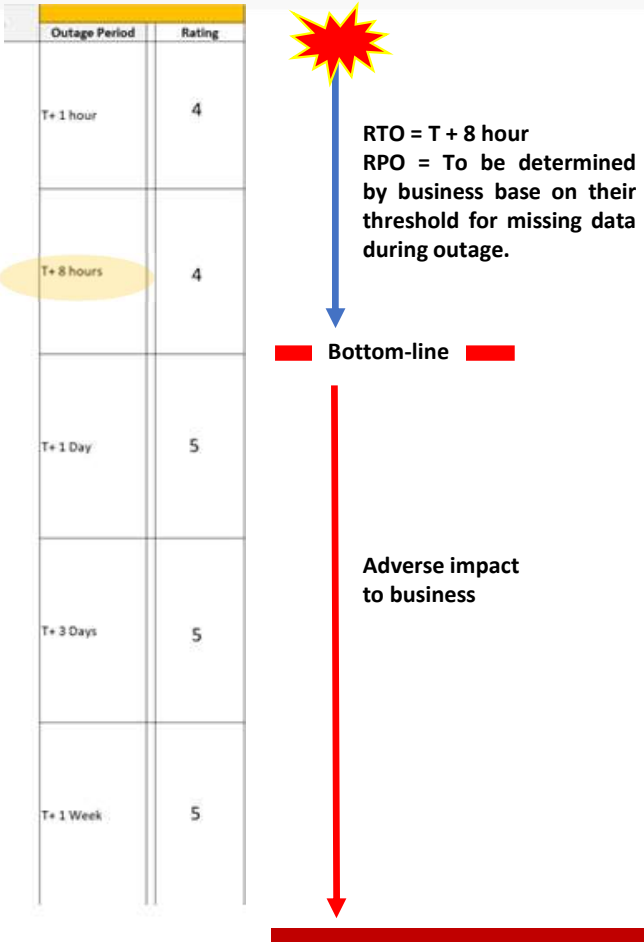
Determining RTO/RPO

Impact Assessment					
Outage Period	Financial (By Business Revenue)	Operational	Compliance	Strategic (Customers)	Rating
T+ 1 hour	<5%	Insignificant or minimal interruptions to business operations within a single functional group < 1/2 day. No loss of internal information. Minimal to no impact to operational support and manual work can be sustained during outage.	Minor breaches with no liabilities or regulatory impact	Insignificant or minimal impact on customer relationships and contracts.	1
T+ 8 hours	<5%	A functional group Minor interruptions to business operations within a single functional group <1 day. Loss/corrupted internal information with low impact. Minimal impact to operational support and manual work can be sustained during outage.	Minor breaches with no liabilities or regulatory impact	Impact on <10% of customer relationships and contracts, which may be fully repaired in short term.	2
T+ 1 Day	<5%	Enterprise wide Inability to continue BAU across all functional groups > 3 days. Loss of confidential data that will incur financial losses. Significant impact to operational support and manual work can be difficult to sustain during outage.	Minor breaches with no liabilities or regulatory impact	Insignificant or minimal impact on customer relationships and contracts.	2
T+ 3 Days	<5%	Enterprise wide Significant interruptions (1 3 days) to BAU across all functional groups. Loss of confidential data with significant impact. Impacts operational support badly and operational support suffers hardship during outage.	Management unaffected Minor legal liabilities/restrictive measures Potential regulatory attention	Impact on 51 - 75% of customer relationships and contracts, requiring a long term recovery plan.	3
T+ 1 Week	<5%	Enterprise wide Inability to continue BAU across all functional groups > 3 days. Loss of confidential data that will incur financial losses. Significant impact to operational support and manual work can be difficult to sustain during outage.	Large Scale Legal Actions against the Company and Management Regulatory Sanctions Revoke of licenses/ suspension	Impact on 76 - 100% of customer relationships and contracts. Complete erosion of trust and confidence and potentially irreparable.	4
					3

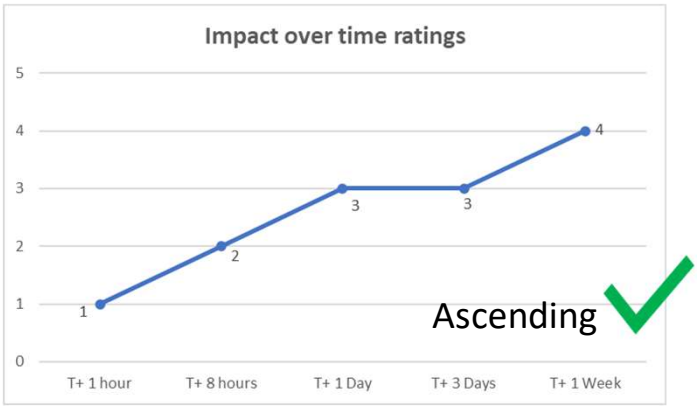


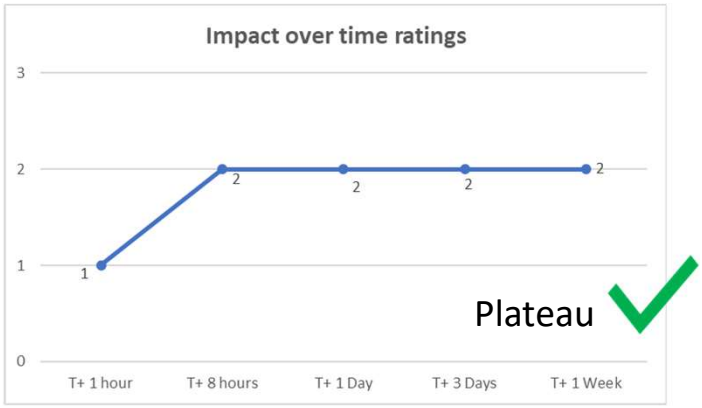
Other examples of determining RTO/RPO

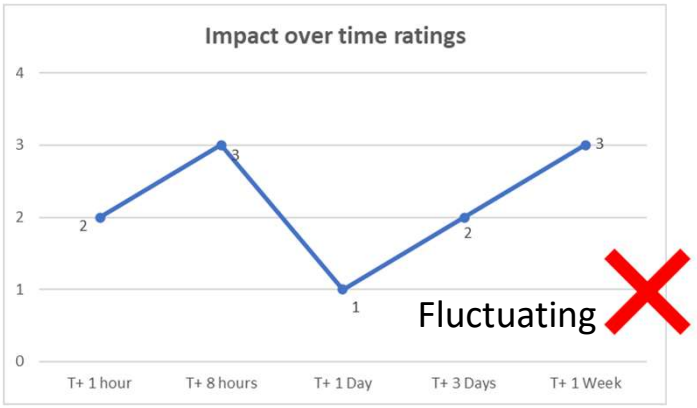


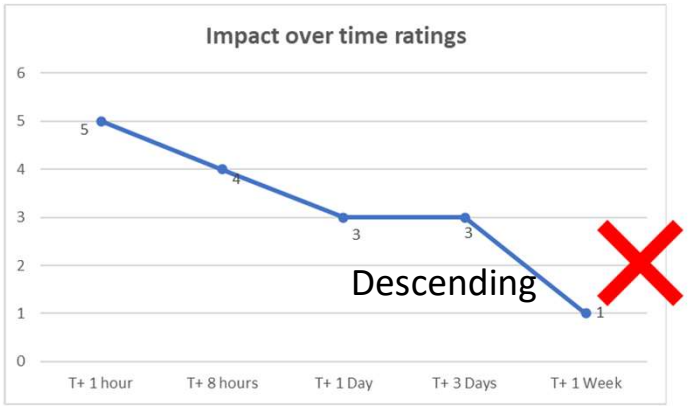


Impact over ratings samples

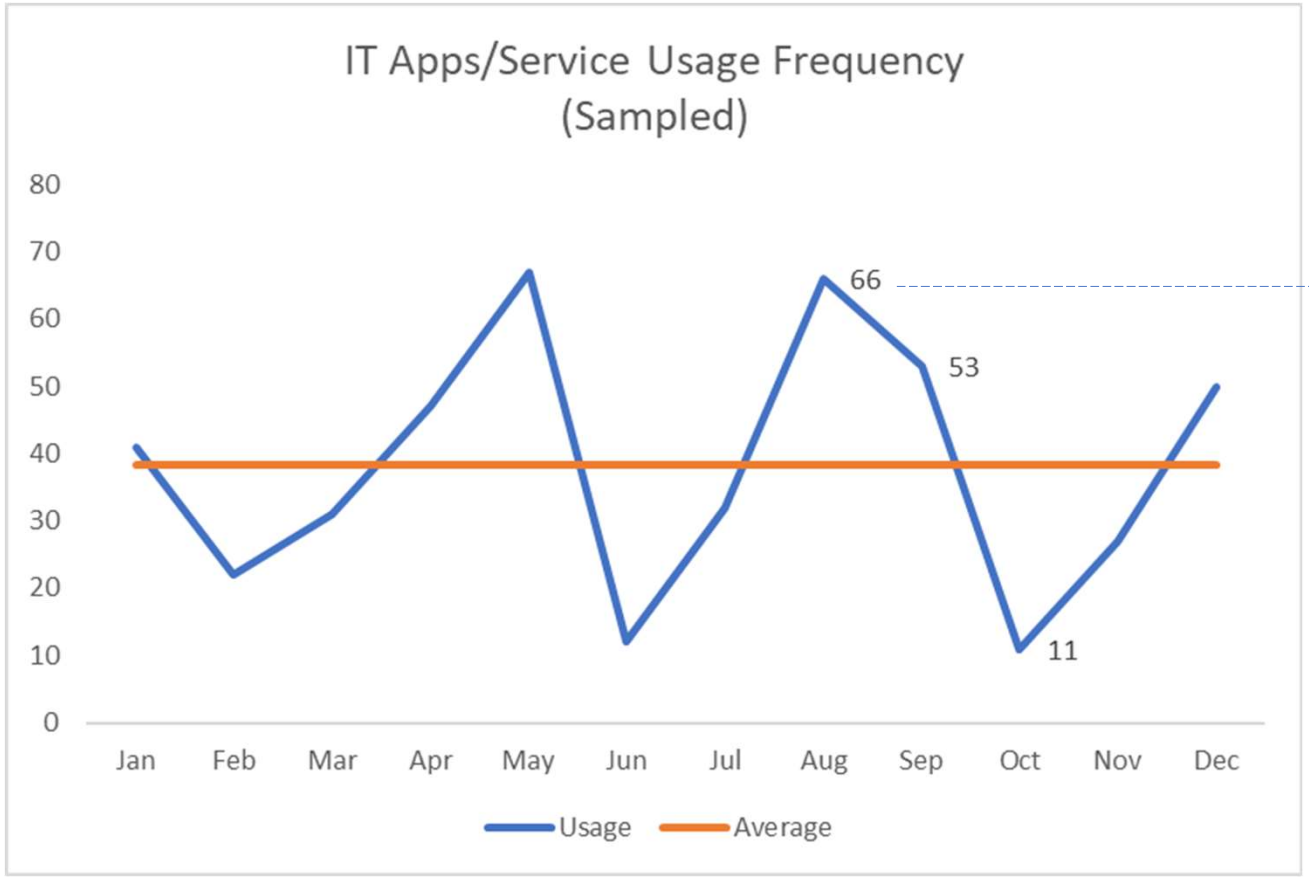








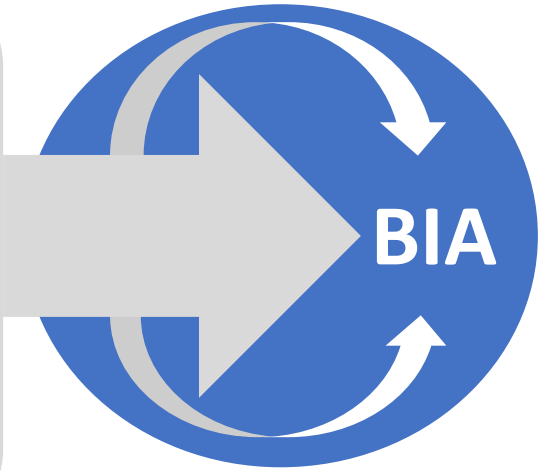
Which period to select for BIA assessment?



Pick this range for BIA assessment

When should BIA be done?

1. When you introduce a new Business; Process; System; etc.
2. When there is a major/ substantial change
3. Annual Review exercise



Thank you

Integrity, effort, unity, compassion and gratitude