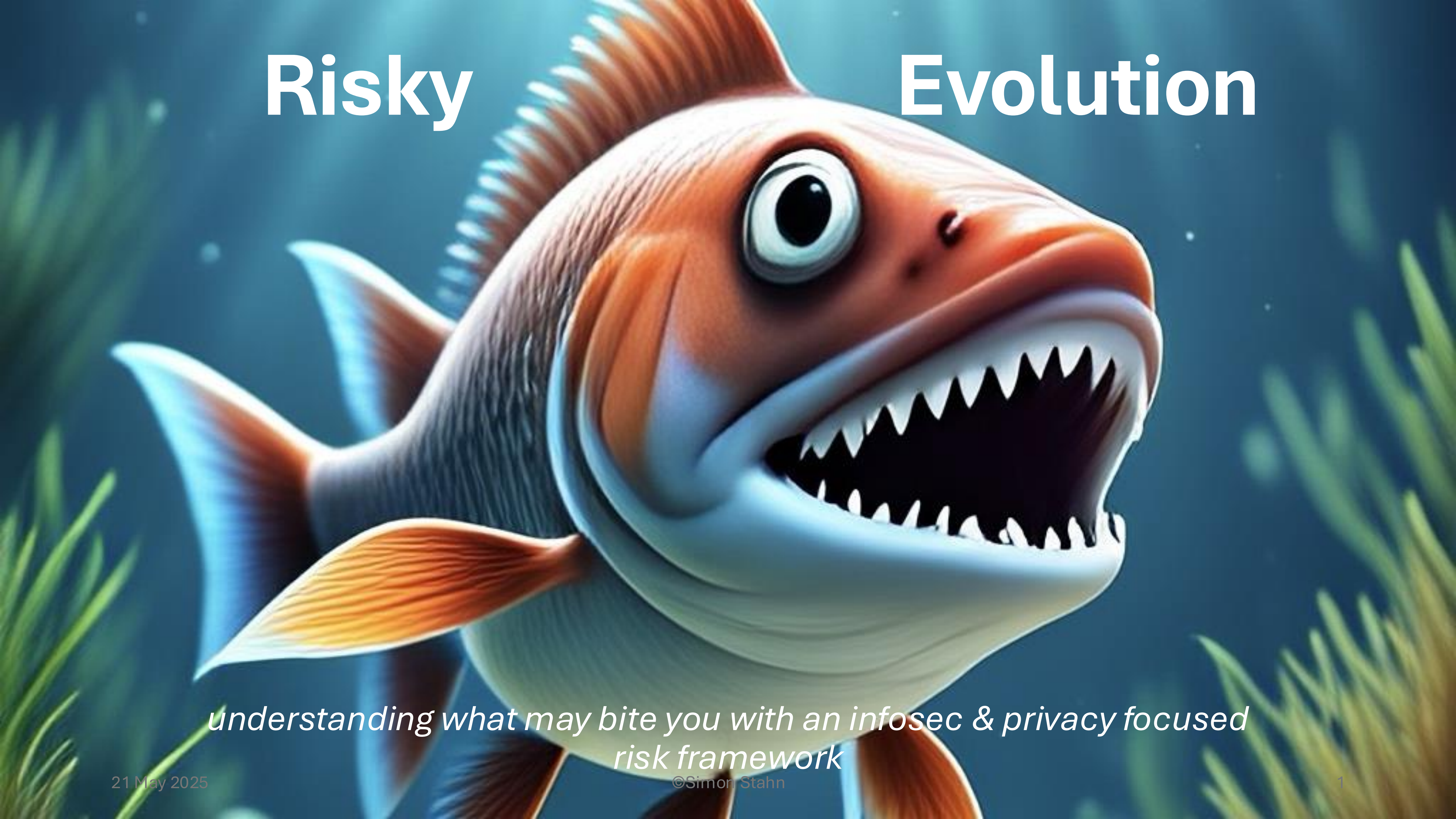
Risky Evolution



understanding what may bite you with an infosec & privacy focused risk framework

AusCERT 2025 Tutorial

Supporting slides and notes for attendees only

Contact

- Simon Stahn
- simon@adrenalan.com

Acknowledgement of Country

We acknowledge the traditional owners and custodians of country throughout Australia and acknowledge their continuing connection to land, waters and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

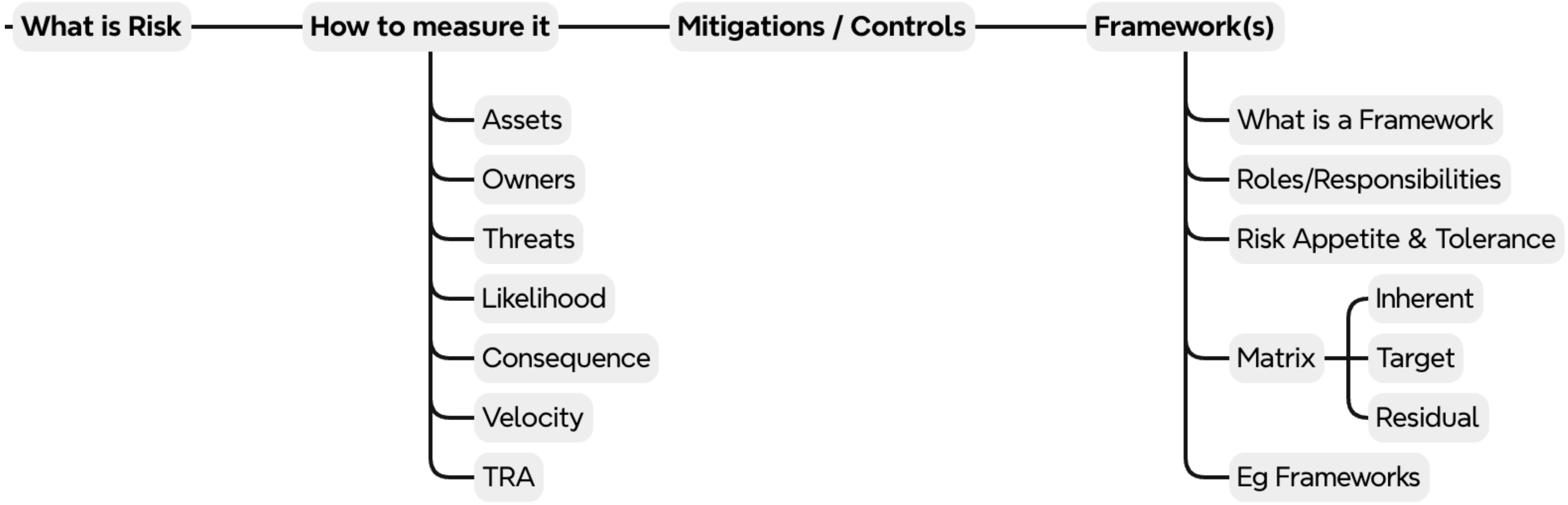
Guidelines for this session

- If you have questions or example to work through, note them and I’ll pause periodically in the first half for Q&A.
- If you need a clarification on something, please say it then and there.
- If I’m not loud enough, etc, let me know.
  I try and cater for all types of human-data-ingestion but don’t know your type… so let me know!
- Chatham house rules here – please respect each other’s privacy and confidentiality
- As always, let’s keep it polite between everyone.

Target Audience

- Already have an idea of cybersecurity and privacy concepts
- Want to **understand how** to either start/**build** a cybersec focused **risk framework** for their organization…
- …and (even if you already have one) use it well and integrate with the rest of the organisation

Agenda



- What is Risk
- How to measure it
  - Assets
  - Owners
  - Threats
  - Likelihood
  - Consequence
  - Velocity
  - TRA
- Mitigations / Controls
- Framework(s)
  - What is a Framework
  - Roles/Responsibilities
  - Risk Appetite & Tolerance
  - Matrix
    - Inherent
    - Target
    - Residual
  - Eg Frameworks

Terms of Reference

- cybersecurity - in these slides will just refer to cybersec / infosec / privacy, unless I'm clearly splitting them out
- Privacy is (of client, not of self)… we'll split it out as we come to it, mostly in the framework side of things

Policy

- Like the rest of infosec, if you don’t have it under a policy, you can’t do much about it.
- Check for clashes between infosec and other risk statements in policy throughout your organisation
- Policy and risk tolerance comes from Board level.

Why?

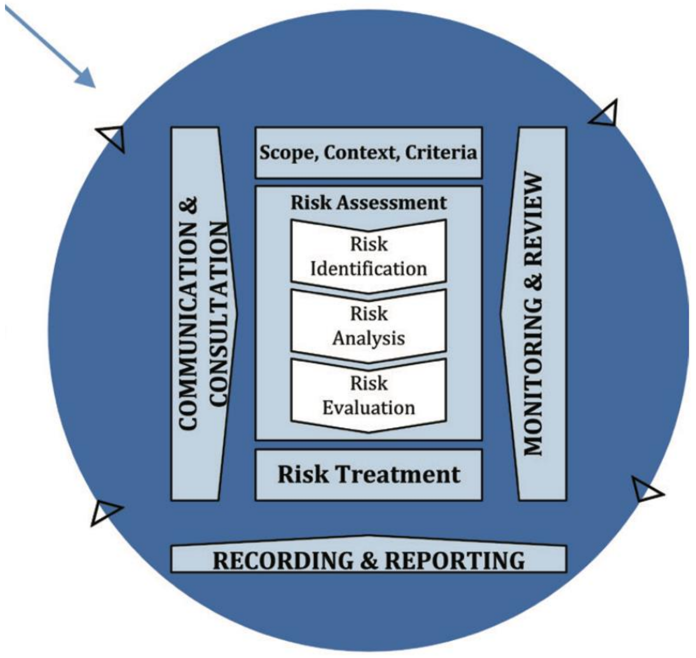
- Why do we want to quantify the risks?
  - We humans are pretty bad at identifying and quantifying risk
  - You can’t improve on something if you can’t measure it.
  - You can’t mitigate a risk if you can’t quantify it and break it down.
  - Prove you’re doing something about something
    - Regulatory
    - Audit
  - You can ask for money to fix things without a business case

What is risk?

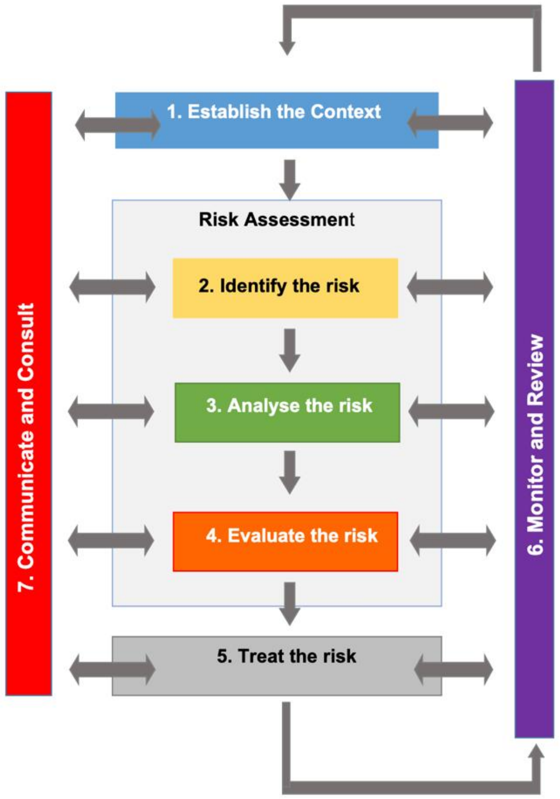
- Something bad happening
- The [possibility/chance] of [thing] being exposed to something (bad) happening and will be have a [consequence/impact]
  - What is ‘thing’ here… could be a person, the organization… but as infosec we can see it as “information asset”
- Exposed to risk as children… mostly parents guided your view of risk
- flip it, it’s an opportunity

Measure it

- Assets & owners
- Likelihoods
- Consequence & Impacts
- Velocity
- Threats

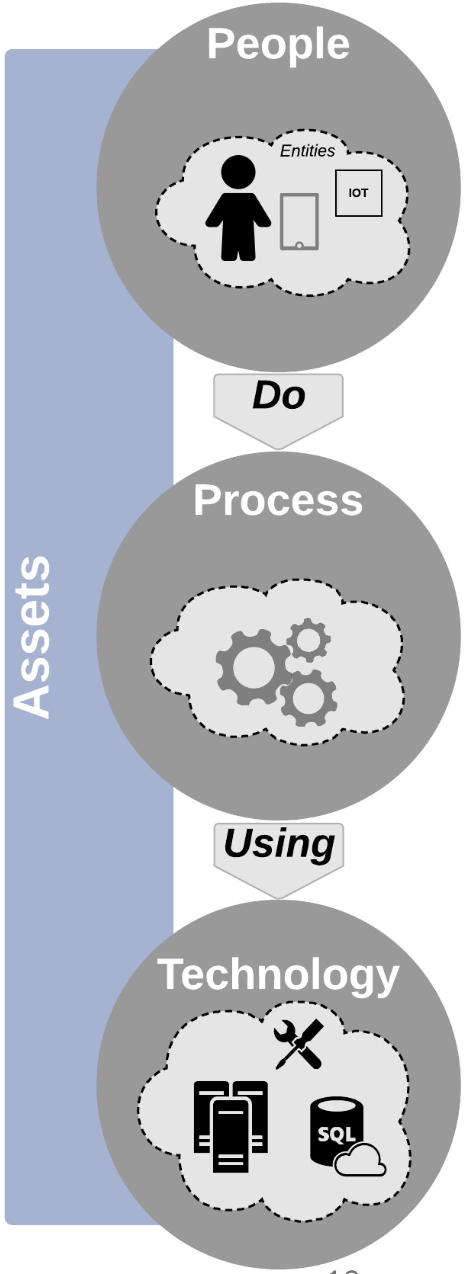


Process (clause 6)



Assets & Owners

- This slide left unintentionally blank?



Likelihood / Probability

- hmm

Likelihood	Probability	Description
Rare	< 15 %	Only likely in exceptional circumstatnces and unlikely to occur in the next five years
Unlikely	15 - 40 %	Not likely to occur, but may occur in the next three years
Possible	41 - 65 %	May occur within two years
Probable	66 - 85 %	Has happen in the past and/or could happen in the next year
Almost Certain	> 85 %	Happens from time to time and/or could happen in the next six months

Consequence / Impact

Risk Category	Descriptive Note
CATASTROPHIC	Critical event/circumstance with potentially disastrous impact on business sustainability
MAJOR	Critical event or circumstance that can be endured with proper management
MODERATE	Significant event or circumstance that can be managed under normal conditions
MINOR	Event with consequences that can be readily absorbed but requires management effort to minimise the impact
INSIGNIFICANT	Some loss but immaterial. Existing controls & procedures should cope with event or circumstance

Velocity

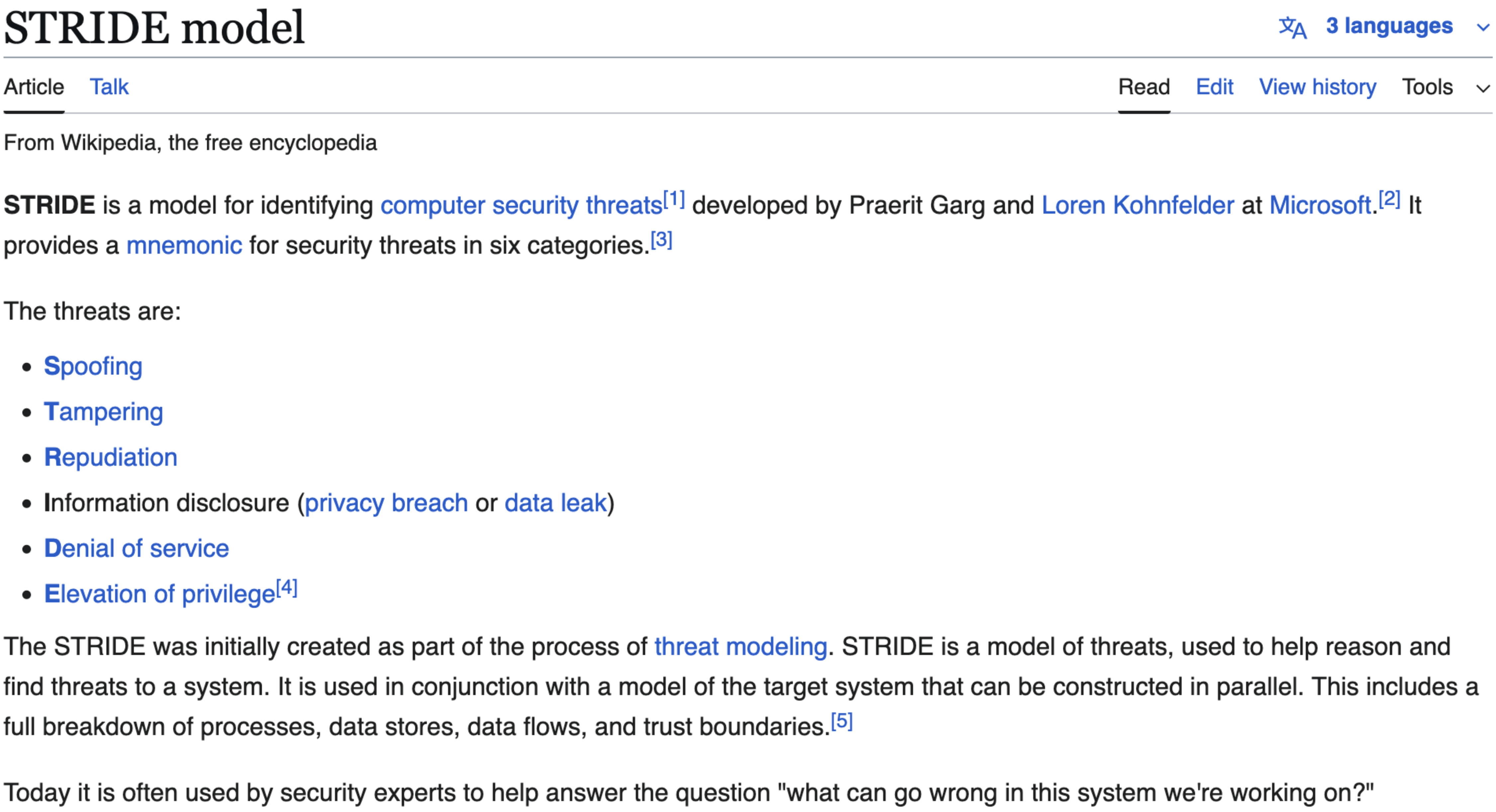
- Not so relevant in our industry, as most cybersecurity ‘events’ would be classed as “very rapid” in most enterprise risk velocity tables
- Included here to think about, as some consequences may take longer to manifest, or multiple instances, such as reputational damage.
- Definitely need to think to interface with Ent Risk Mgmt

Indication of the speed of onsite or the time it takes the organisation to feel the effects (consequence) once risk manifests

	Rating	Description
Velocity	Very Rapid	Very rapid onset, litte/no warning, or instantaneous
	Rapid	Onset occurs in hours/days to < few weeks
	Moderate	Onset occurs in 1-6 months
	Slow	6+ months
	Very Slow	Year onwards

Threats

(this slide left intentionally blank!)



STRIDE model

From Wikipedia, the free encyclopedia

STRIDE is a model for identifying computer security threats[1] developed by Praerit Garg and Loren Kohnfelder at Microsoft.[2] It provides a mnemonic for security threats in six categories.[3]

The threats are:

- Spoofing
- Tampering
- Repudiation
- Information disclosure (privacy breach or data leak)
- Denial of service
- Elevation of privilege[4]

The STRIDE was initially created as part of the process of threat modeling. STRIDE is a model of threats, used to help reason and find threats to a system. It is used in conjunction with a model of the target system that can be constructed in parallel. This includes a full breakdown of processes, data stores, data flows, and trust boundaries.[5]

Today it is often used by security experts to help answer the question "what can go wrong in this system we're working on?"

https://en.wikipedia.org/wiki/STRIDE_model

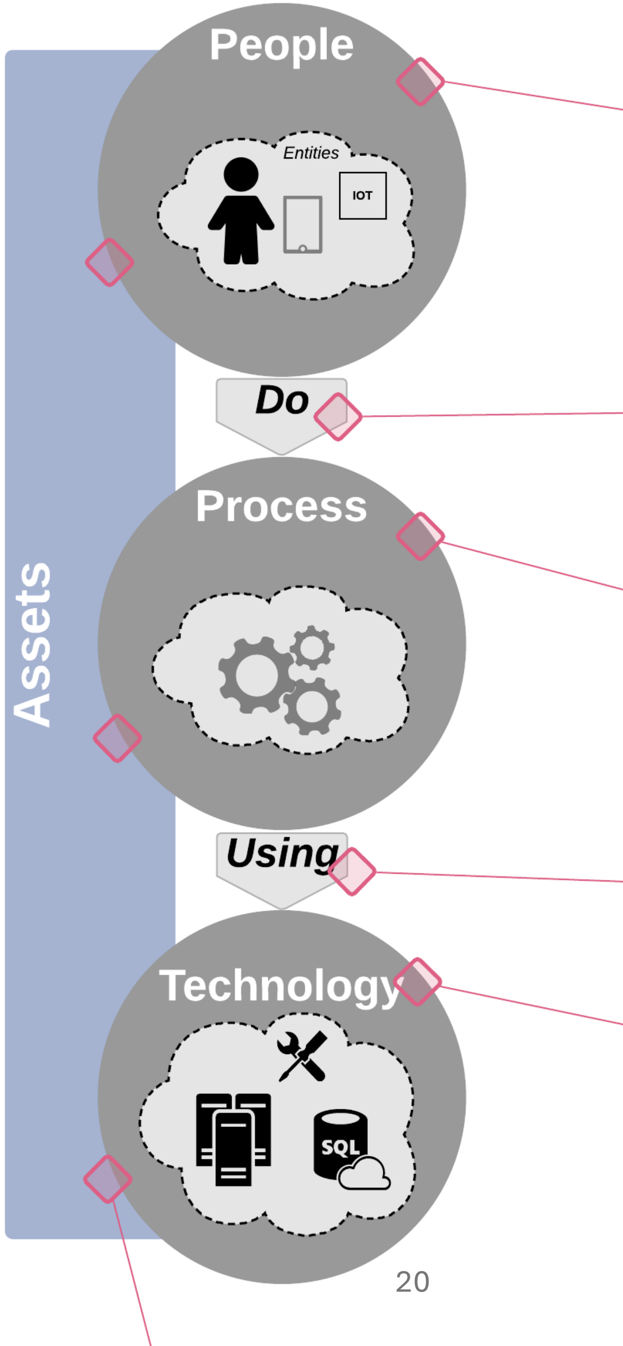
Stride

Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Someone obtaining information they are not authorized to access
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

https://en.wikipedia.org/wiki/STRIDE_model

Mitigations & Controls

- (Not going to try and suggest all the controls here today!)
- Look at all the levels – you have **natural control points between boundaries** such as between 'people' and 'process'.
- Also ask the question "**why** are we (doing project / doing this)?" and see if the benefits of the identified opportunities outweigh the risk 'costs'
- Build yourself a list of common controls for your organisation



Risk Frameworks

Framework

- A **framework** is a real or conceptual structure, or system of rules, intended to serve as a support or guide for the building of something that **expands** the structure **into something useful**

- Again, for those in the back, a framework is not a 'ready thing' that you can just use. It **needs to be formed** into something useful **for your organisation**.

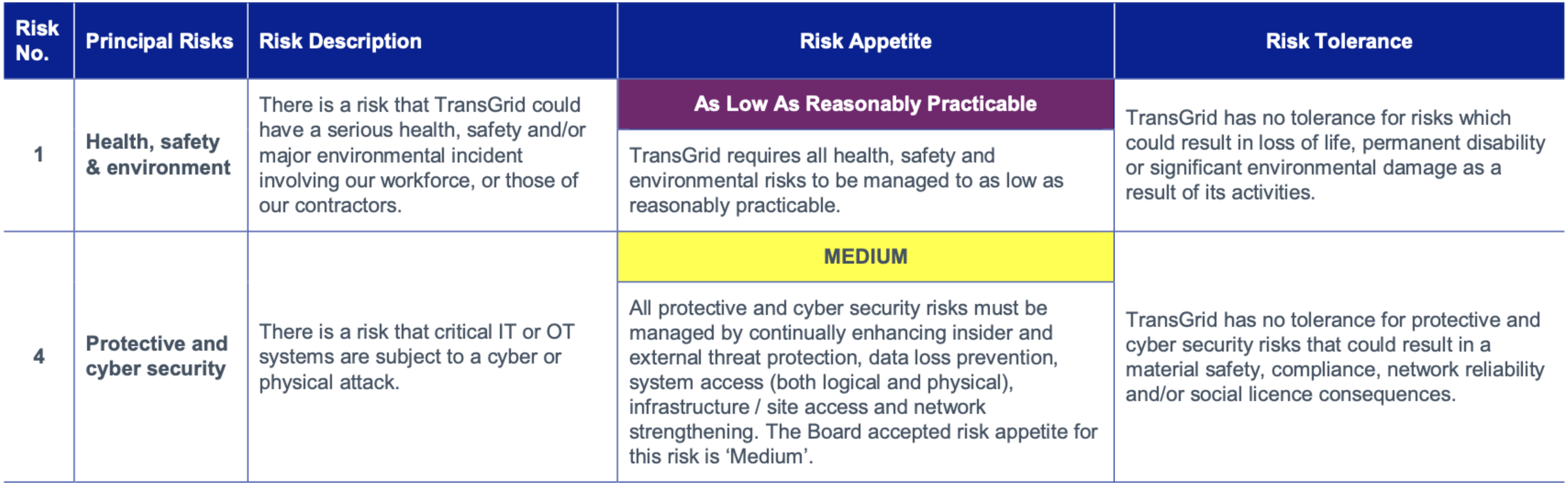
Roles & Responsibilities

Example Structure

Position	Responsibility
Board	• Sets, monitors and approves the organisation’s risk appetite statement(s)
Risk and Audit Committee	• Evaluates the adequacy and effectiveness of the organisation’s risk management and compliance framework • Advises Board on exposure and management of significant organisational risks
Governance area (Directors or Heads-of)	• Provides risk services (training, facilitation, advisory) to assist (management & staff) in their identification, assessment and treatment of risk • Informs and reports to RAC • Oversees the risk management framework
Management & Staff	• Manage risks in their areas of responsibility

Risk Appetite & Tolerance

- Board (or equivalent) sets the risk appetite & tolerance
  - Typically done for each RMF category – see example from TransGrid



Risk No.	Principal Risks	Risk Description	Risk Appetite	Risk Tolerance
1	**Health, safety & environment**	There is a risk that TransGrid could have a serious health, safety and/or major environmental incident involving our workforce, or those of our contractors.	**As Low As Reasonably Practicable** TransGrid requires all health, safety and environmental risks to be managed to as low as reasonably practicable.	TransGrid has no tolerance for risks which could result in loss of life, permanent disability or significant environmental damage as a result of its activities.
4	**Protective and cyber security**	There is a risk that critical IT or OT systems are subject to a cyber or physical attack.	**MEDIUM** All protective and cyber security risks must be managed by continually enhancing insider and external threat protection, data loss prevention, system access (both logical and physical), infrastructure / site access and network strengthening. The Board accepted risk appetite for this risk is 'Medium'.	TransGrid has no tolerance for protective and cyber security risks that could result in a material safety, compliance, network reliability and/or social licence consequences.

Risk Tolerance

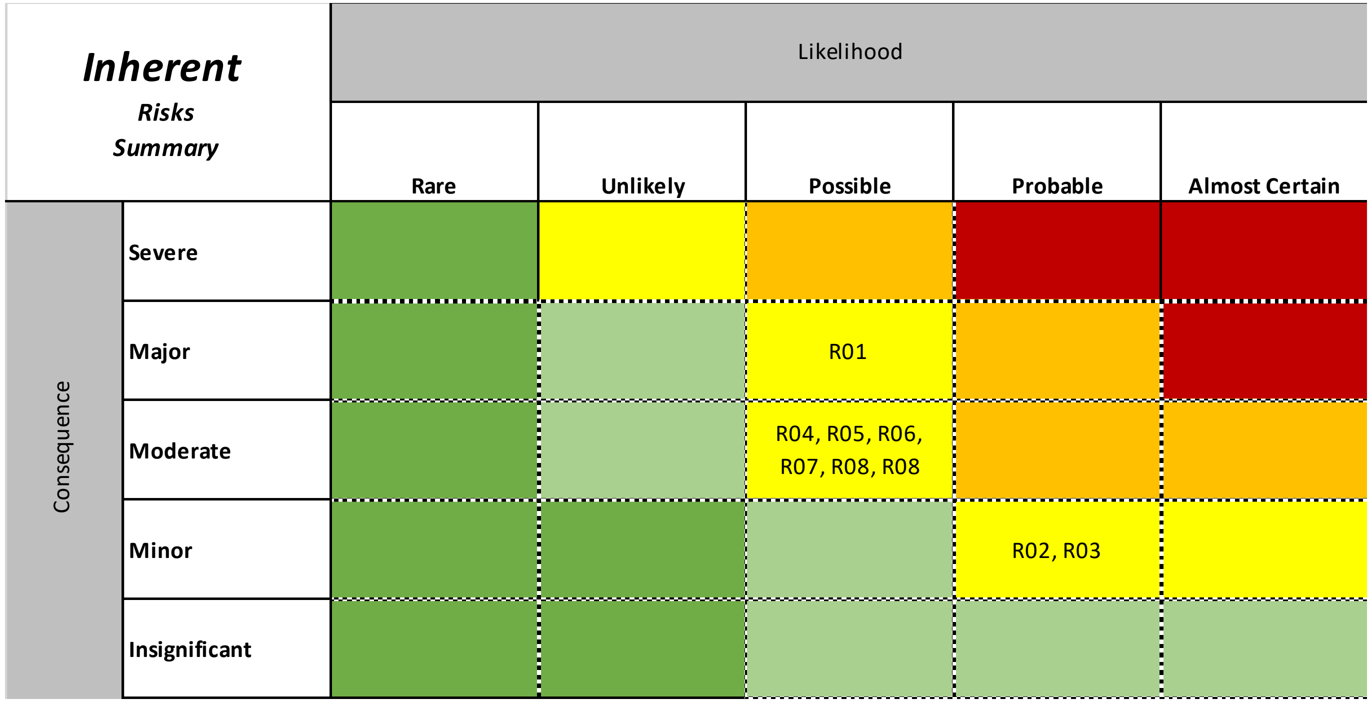
Risk Rating	Tolerance / Escalation
Very High	**Unacceptable** / No Tolerance Immediate / Urgent action required Escalate to the / Executive Group
High	**Highly Cautious** Within 3 months / Action plan required Requires escalation to Senior Management
Medium	**Tolerable** / Conservative Assess the risk and determine if current controls are adequate Management responsibility must be specified
Low	**Acceptable** Manage through routine procedures Unlikely to need specific application of resources.
Very Low	

Matrix

		Likelihood				
		Rare	**Unlikely**	**Possible**	**Probable**	**Almost Certain**
Consequence	**Severe**	Very Low	Medium	High	Very High	Very High
	Major	Very Low	Low	Medium	High	Very High
	Moderate	Very Low	Low	Medium	High	High
	Minor	Very Low	Very Low	Low	Medium	Medium
	Insignificant	Very Low	Very Low	Low	Low	Low

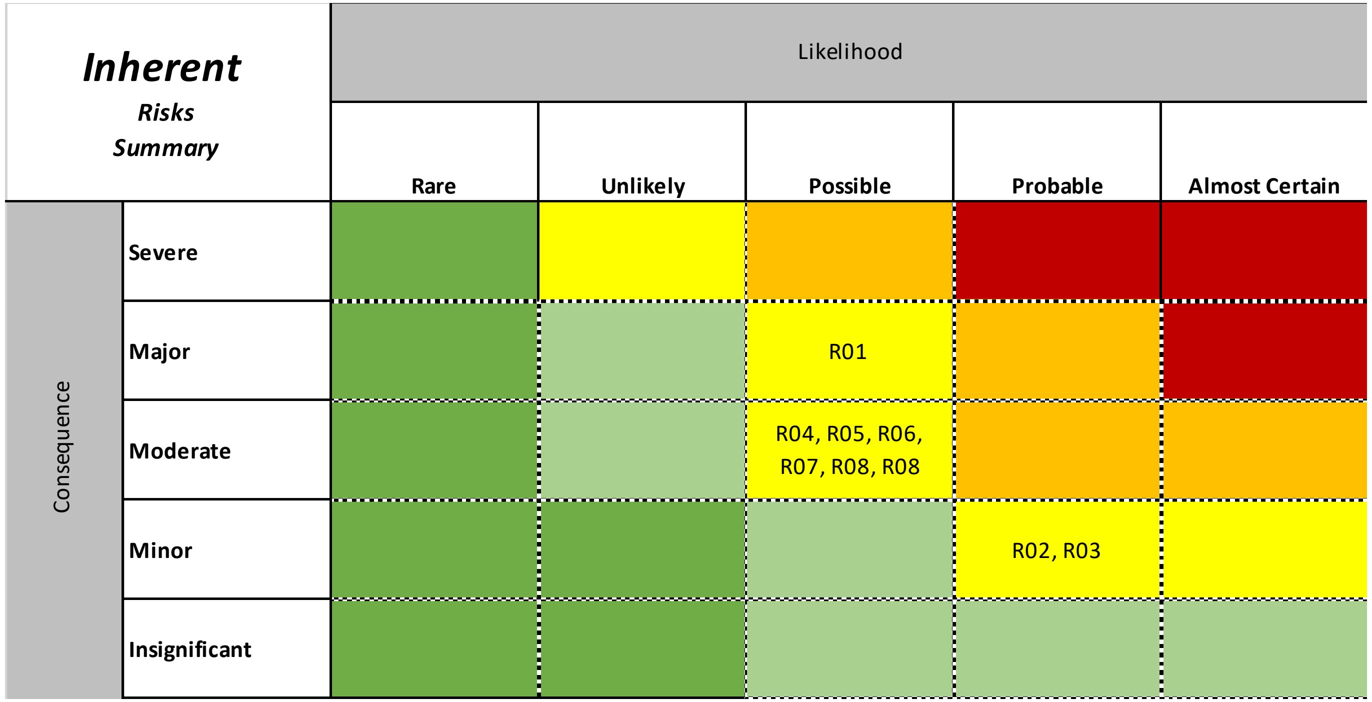
©Simon Stahn

Inherent Risk Summary



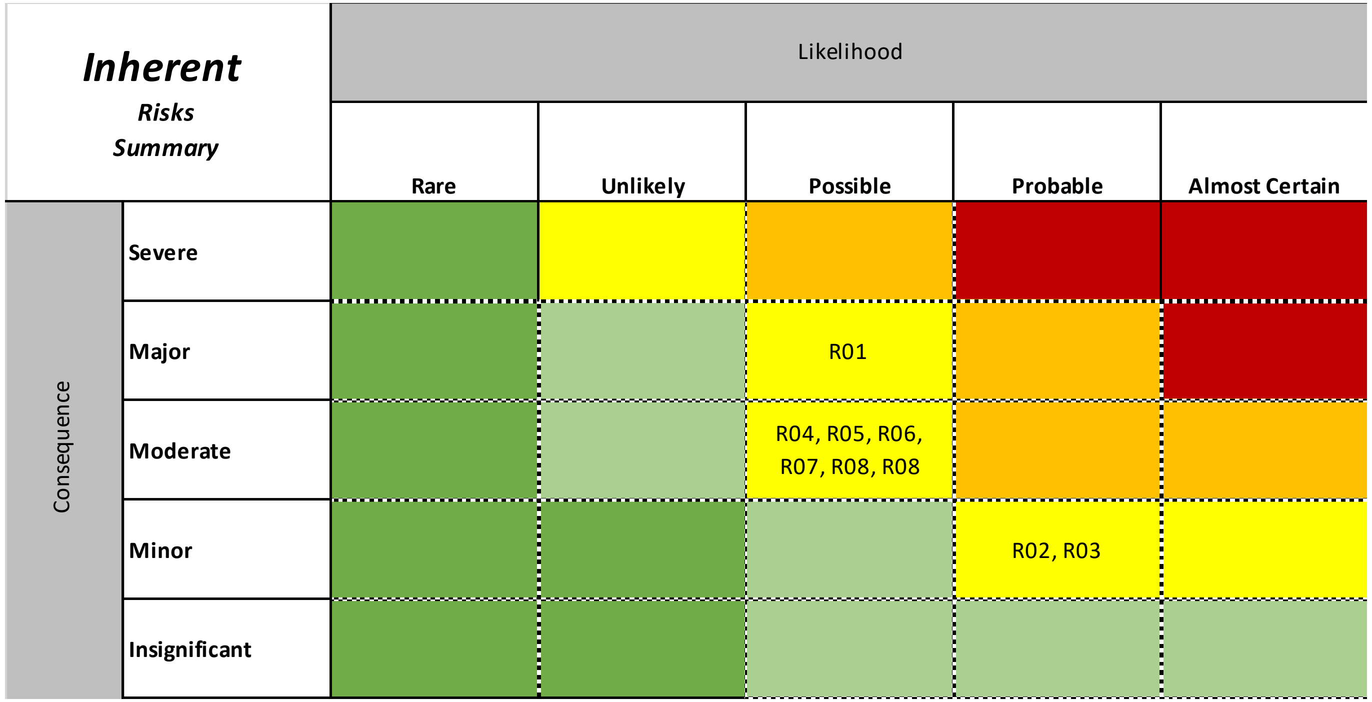
Inherent ***Risks Summary***		Likelihood				
		Rare	**Unlikely**	**Possible**	**Probable**	**Almost Certain**
Consequence	**Severe**					
	Major			R01		
	Moderate			R04, R05, R06, R07, R08, R08		
	Minor				R02, R03	
	Insignificant					

Target Risk Summary



Inherent ***Risks*** ***Summary***		Likelihood				
		Rare	**Unlikely**	**Possible**	**Probable**	**Almost Certain**
Consequence	**Severe**	🟩	🟨	🟧	🟥	🟥
	Major	🟩	🟩	🟨 R01	🟧	🟥
	Moderate	🟩	🟩	🟨 R04, R05, R06, R07, R08, R08	🟧	🟧
	Minor	🟩	🟩	🟩	🟨 R02, R03	🟨
	Insignificant	🟩	🟩	🟩	🟩	🟩

Residual Risk Summary



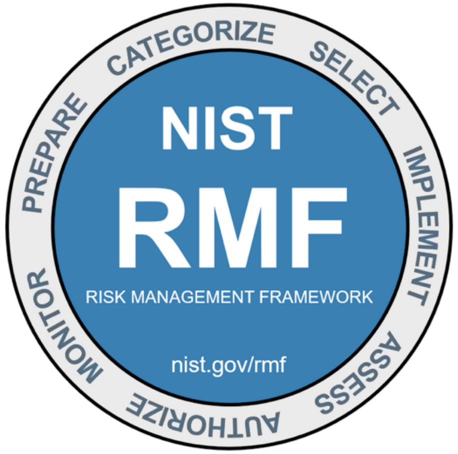
Inherent ***Risks*** ***Summary***		Likelihood				
		Rare	**Unlikely**	**Possible**	**Probable**	**Almost Certain**
Consequence	**Severe**					
	Major			R01		
	Moderate			R04, R05, R06, R07, R08, R08		
	Minor				R02, R03	
	Insignificant					

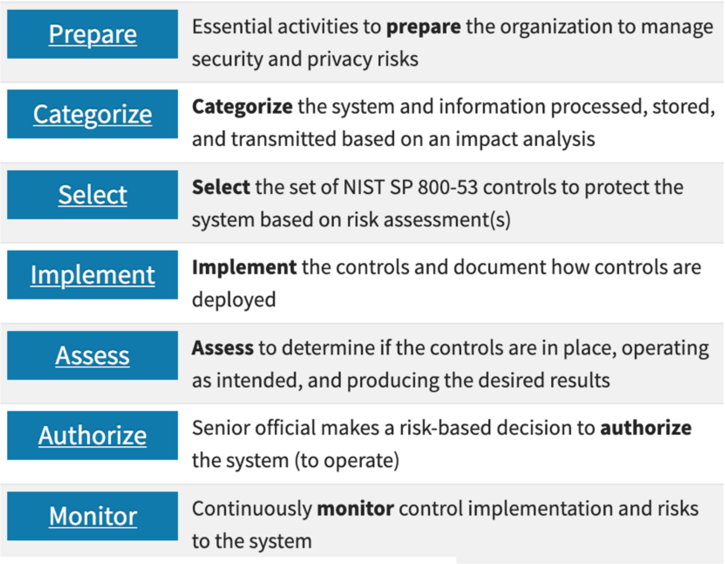
Some Risk Frameworks

- ISO 31000
- NIST.SP.800 Risk Management Framework
- COBIT 2019
- FAIR (Factor Analysis of Information Risk)
- TARA (Threat Assessment and Remediation Analysis)

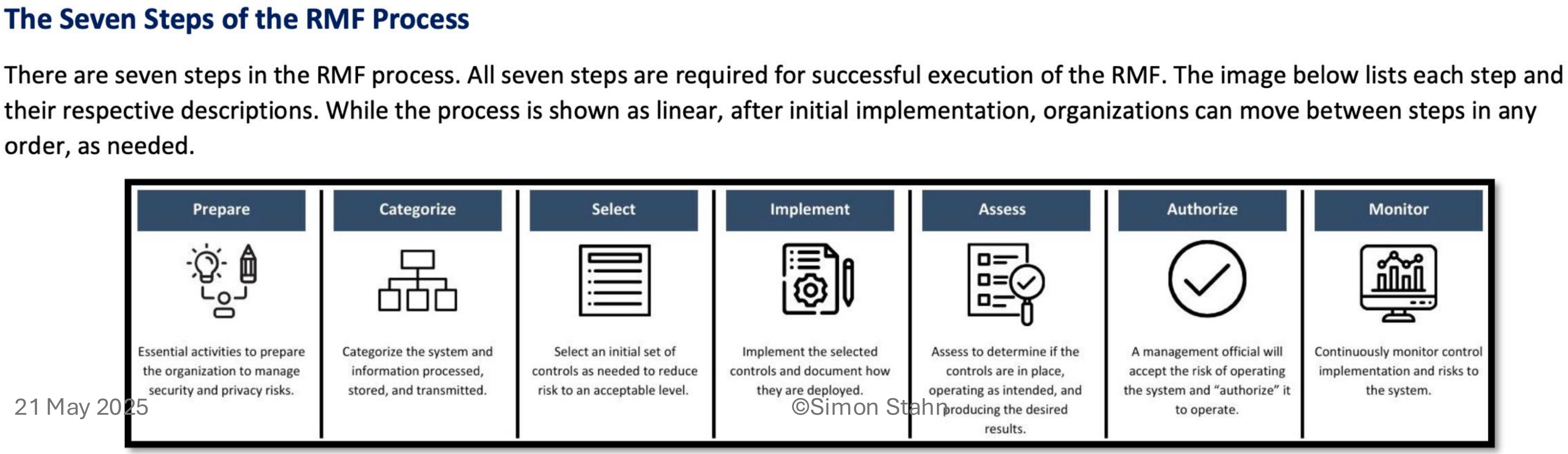
NIST Risk Management Framework

- https://csrc.nist.gov/projects/risk-management
- Has a good ‘quick start’ version for ‘small enterprise’





Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system



The Seven Steps of the RMF Process

There are seven steps in the RMF process. All seven steps are required for successful execution of the RMF. The image below lists each step and their respective descriptions. While the process is shown as linear, after initial implementation, organizations can move between steps in any order, as needed.

Prepare	Categorize	Select	Implement	Assess	Authorize	Monitor
Essential activities to prepare the organization to manage security and privacy risks.	Categorize the system and information processed, stored, and transmitted.	Select an initial set of controls as needed to reduce risk to an acceptable level.	Implement the selected controls and document how they are deployed.	Assess to determine if the controls are in place, operating as intended, and producing the desired results.	A management official will accept the risk of operating the system and “authorize” it to operate.	Continuously monitor control implementation and risks to the system.

Links / References

Materials from this session	https://github.com/adrenalan/AusCERT2025
STRIDE model	https://en.wikipedia.org/wiki/STRIDE_model
AICD cybersecurity risk links	https://www.aicd.com.au/risk-management/framework/cyber-security.html
AICD cybersecurity & privacy regulation notes for Directors / SMBs	https://www.aicd.com.au/risk-management/framework/cyber-security/new-cyber-security-and-privacy-regulation.html
ASIC note on Risk Appetite Statements	https://asic.gov.au/regulatory-resources/find-a-document/reports/corporate-governance-taskforce-director-and-officer-oversight-of-non-financial-risk-report/risk-appetite-statements
ISO 31000 (wiki)	https://en.wikipedia.org/wiki/ISO_31000
MITRE TARA	https://www.mitre.org/news-insights/publication/threat-assessment-and-remediation-analysis-tara
NIST Risk Mgmt Framework	https://csrc.nist.gov/projects/risk-management
ISACA COBIT	https://www.isaca.org/resources/cobit
FAIR institute	https://www.fairinstitute.org/what-is-fair
FAIR model PDF	https://cdn2.hubspot.net/hubfs/1616664/The%20FAIR%20Model_FINAL_Web%20Only.pdf