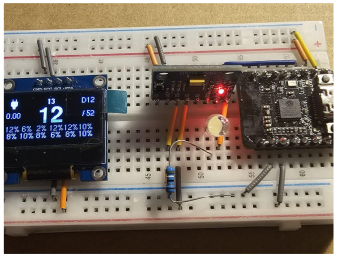
Risk Management

We wear hoodies. Why should we care?

- Brief introduction.
- Introduce some necessary tools.

** Any opinions are my own and from my own work/life experience. Any feedback/agreement/disagreement welcome!*

Me



Toit

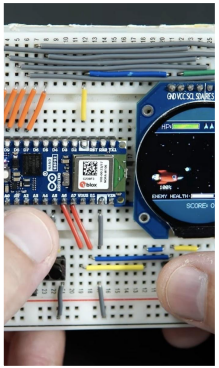
You

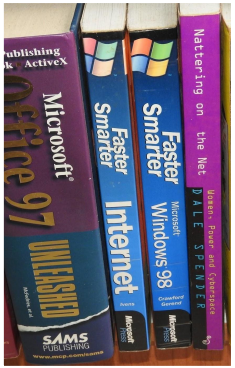
You build and break things, for fun or for a living.

You've probably seen things (like security) done badly, or been left out where it mattered.

Maybe you haven’t…

But you want your work, now (and in the future) to matter.





Risk Management

…isn't paperwork. It's the API between IT and the business.

…isn’t a weapon to be beaten by. It’s a weapon to wield.

Either learn this language, or accept that someone less technical than you is making your decisions for you.

What are we doing?

‘Risk Management’ sells a unified approach to identify, assess, treat and monitor risks, across an entire company.

- Identifying
- Assessing
- Treating
- Monitoring

Why are we doing it?

Both **external** and **internal** pressures, aside from being plain useful

- ISO, NIS2, ISA/IEC, require ‘risk based’ and ‘appropriate and proportionate’
- NIS2 made it **personal** for the management body… and they need us to do the work.
- The CRA reporting clock is **already** running for products we ship.
- Supply chain is now in scope: we're somebody else's supplier.

Compliance Based

Success = Every box ticked

- *Treats all risks as equal. Can result in over-investment in low-risk areas and under-investment in high-risk areas.*
- *Creates a false sense of security: "we're compliant" doesn't mean "we're secure."*
- *Becomes a paper exercise that encourages resentment rather than engagement.*
- *Doesn't really adapt when new threats emerge or when the business changes.*
- *Auditors see through it.*

What does 'Risk-Based' Mean?

"The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives."

Risk Based

Success = Risk reduced to an acceptable level

- *Requires genuine engagement from people who understand the business.*
- *Risk assessments are only as good as the input, without participation, frameworks are built on assumptions.*
- *Takes more effort upfront than ticking boxes.*
- *Can feel uncomfortable initially because it requires explicit decisions being attributable (e.g., subtly forces accountability).*

REPEAT

NIS2/CSL

EUs baseline CS law for critical sectors - broader, stricter, and more enforceable

A real life example of external pressure

Breaks down into Important Entities and Essential Entities

OT explicitly in scope - no ambiguity

Stricter *minimum* requirements in OT

Mandatory incident reporting

Senior leaders personally accountable

REPEAT

ISA/IEC62443 Security Levels

Helps to understand & categorise the response (& how far we go).

This is a worked example of Risk Management

SL1 - Casual/Accidental Disclosure, opportunistic interference.

SL2 - Some skill, basic tools, intention.

SL3 - Good skill, specialist system knowledge, moderate resources.

SL4 - High skill, significant resources, high motivation.

“Risk-based”

ISO 27001, ISO 22301, ISO 31000, & IEC 62443 all anchor their requirements to risk. This isn't coincidental — it's how the standards avoid prescribing one-size-fits-all controls.

Cyclical

The ISO frameworks are explicitly a loop: integrate, design, implement, evaluate, improve.

Supply Chain

…is everyone’s problem. NIS2 explicitly calls out supply chain security as a required measure. Capture Energy's dual role as a supplier and a service provider means we are a producer and consumer and sit on both sides for stakeholders.

Accountability

*…stays at the top. NIS2 takes this further: management can be held **personally** liable, and critically, that accountability **cannot** be delegated downward.*

Ownership

…requires authority to make change, not just proximity. The process of recording/attributing decisions forces us to be more mindful.

IT/OT are ‘different’

In IT environments, confidentiality is key. In IACS/OT, availability & safety come first.

The standards explicitly warn against taking IT security solutions and applying them to IACS without an understanding of consequence.

Fix things

Learn the rules of the game. Then make the system do what it should.

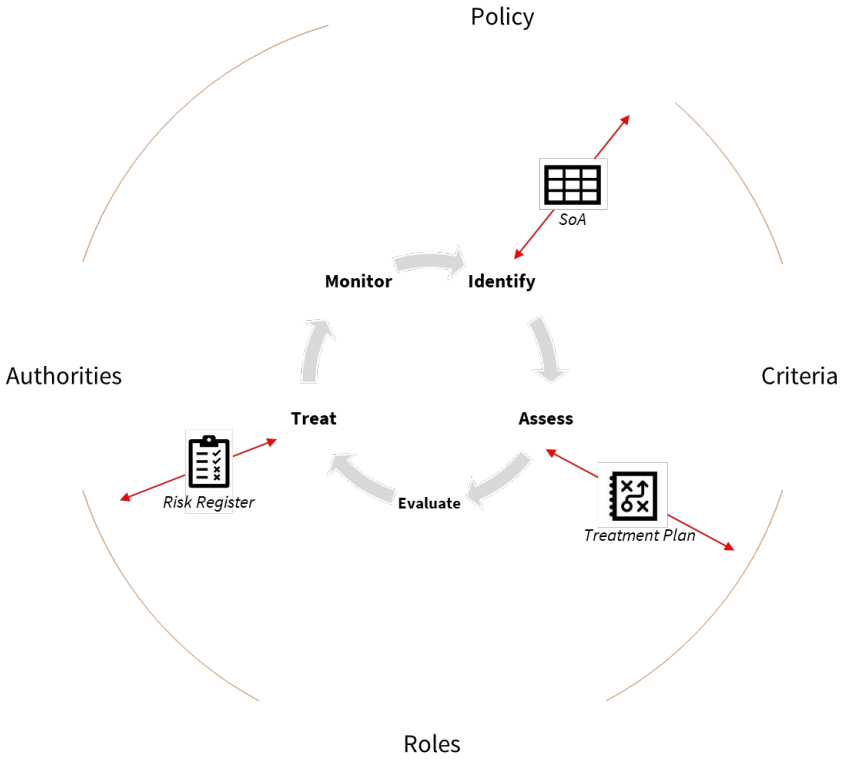
Just like you already do.

The Moving Parts

Rome wasn't built in a day, but one day, we might move there.

- **Governance**
- **Process**
- **Artifacts**
- **Cadence**
- **Linkage**

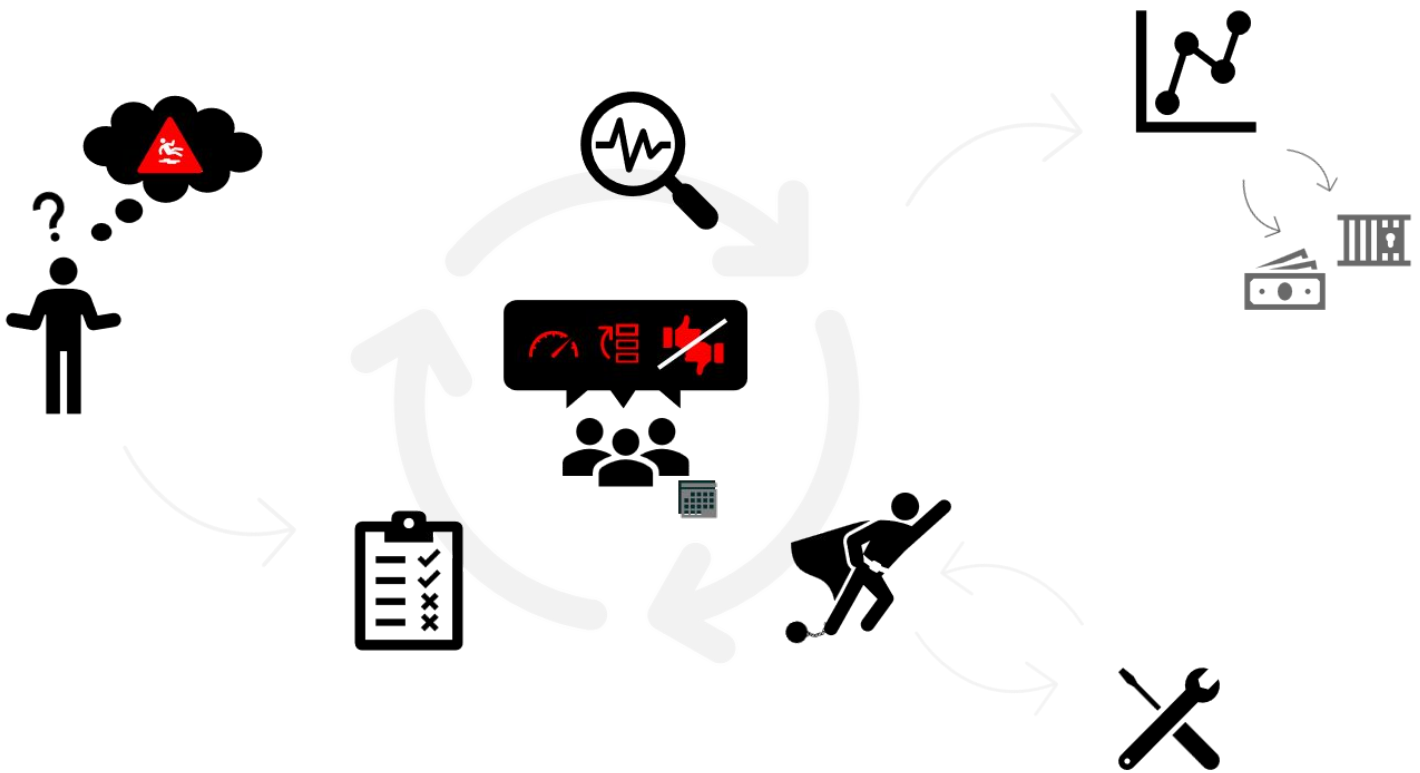
Moving Parts



Risk Cycle

Key to effective risk management is ownership of, and action on, identified risks.

Two major elements exist to handle these: the **Risk Register** to track them, and the **Risk Register Review** process to see that they're addressed.



Tools: Risk Matrix

The Risk Matrix is the function that maps a written risk statement to a comparable score. Without it, every risk is an opinion, re-evaluated every time it's read.

Likelihood and Severity definitions are set by the business itself, often with more than one domain perspective, and relative to its industry. The matrix is something of a fuzzer: it intends to be less specific. It's the company's risk appetite written down as a lookup table.

If a risk doesn't have an obvious place in the table, the rule definitions likely need adjustment. Getting more specific about percentage definitions makes it worse.

		Impact / Consequence				
		1: Negligible	**2: Minor**	**3: Moderate**	**4: Major**	**5: Catastrophic**
Likelihood / Probability	**5: Certain**	5	10	15	20	25
	4: Likely	4	8	12	16	20
	3: Possible	3	6	9	12	15
	2: Unlikely	2	4	6	8	10
	1: Rare	1	2	3	4	5

Tools: People (Roles)

Top Management

Overall accountability. Approves policy, decides risk appetite, reviews escalations.

Risk Owner

Owns individual risks. Identifies, assesses, approves treatment plans.

Risk Officer

Operational coordinator. Runs reviews, tracks training, maintains SoA.

Control Owner

Ensures assigned controls are implemented and operational.

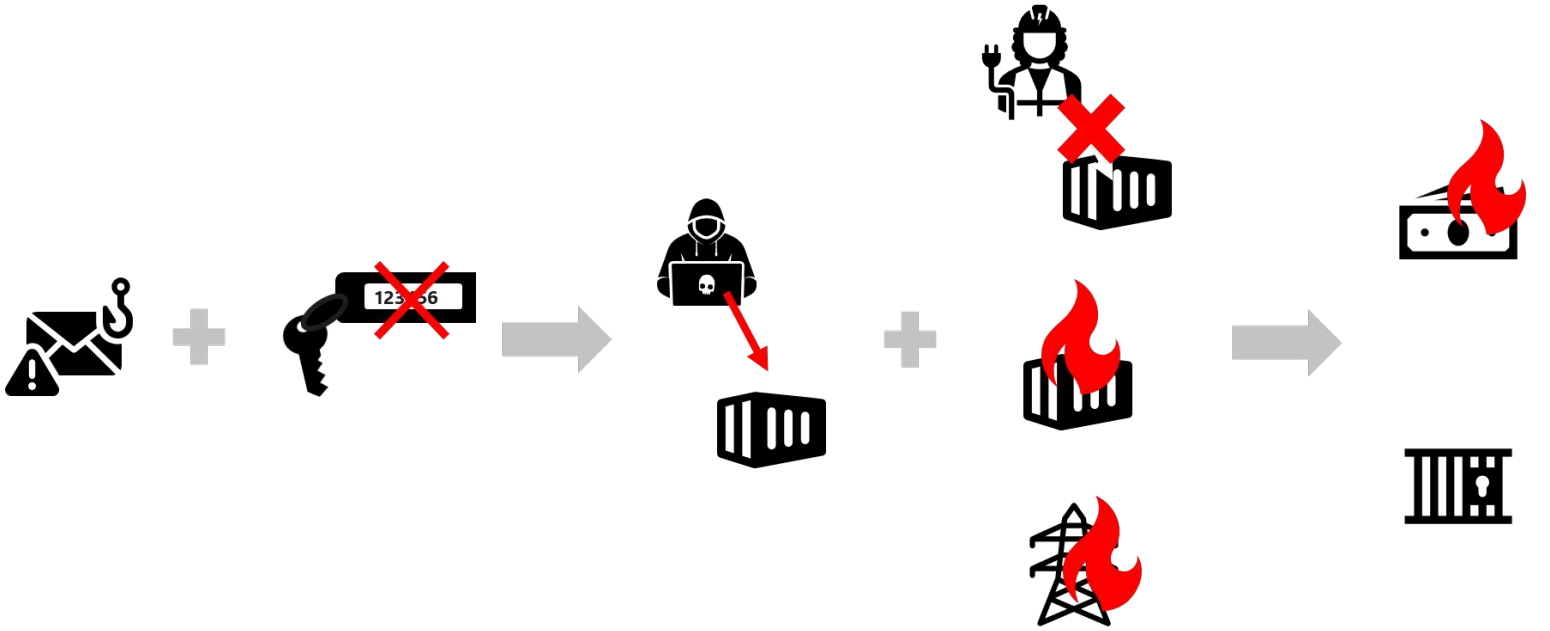
All Employees

Follow controls, report risks, participate in awareness training.

Treatment Owner

Temporary role: designs/executes a specific treatment plan.

Tools: Structured Risk Statement



IF

I go out without a raincoat

AND

It rains

THEN

I will arrive at the interview wet, potentially with my laptop (containing my presentation) soaked in my backpack/handbag

WHICH WOULD RESULT IN

- *visible discomfort at the meeting*
- *potential water ingress to the laptop*

CAUSING

- *Reduced chances of success*
- *Having to shell out for a new laptop*

Tools:
The Structured Risk Statement

If you want attention for your issue, you need to ensure that management clearly understand.

This is why the Structured Risk Statement exists.

IF: *[threat/event occurs]*

Describe the specific action, event, or threat actor activity that could initiate the risk, such as an attacker action, system failure, human error, or external event.

AND: *[vulnerability or condition exists / control fails]*

Describe the technical, procedural, or control weakness that would allow the threat event to lead to exploitation.

THEN: *[unwanted event happens]*

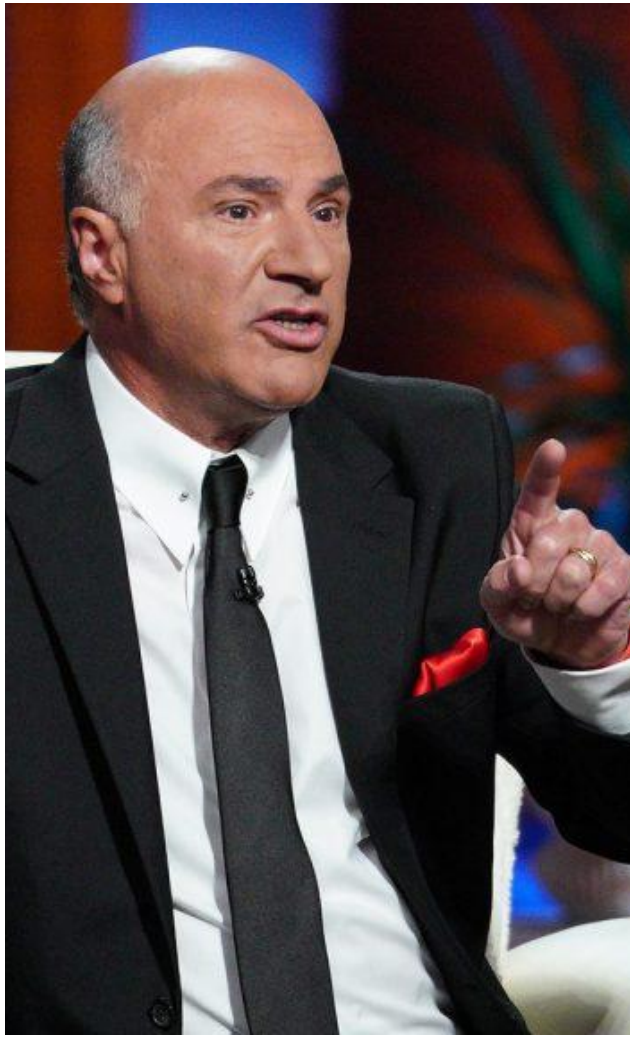
Describe the direct unwanted event or compromise that occurs when the threat exploits the vulnerability.

WHICH WOULD RESULT IN: *[consequence to the organisation]*

Describe the direct consequence to the system, service, or data following the unwanted event.

CAUSING: *[ultimate business impact]*

Describe the ultimate business impact, such as financial loss, regulatory breach, contractual failure, operational disruption, or reputational damage.



IF *servers are not patched regularly*

AND *an attacker gains access to the internal network*

THEN *malware could be installed on systems*

WHICH WOULD RESULT IN *system outages*

CAUSING *service disruption*

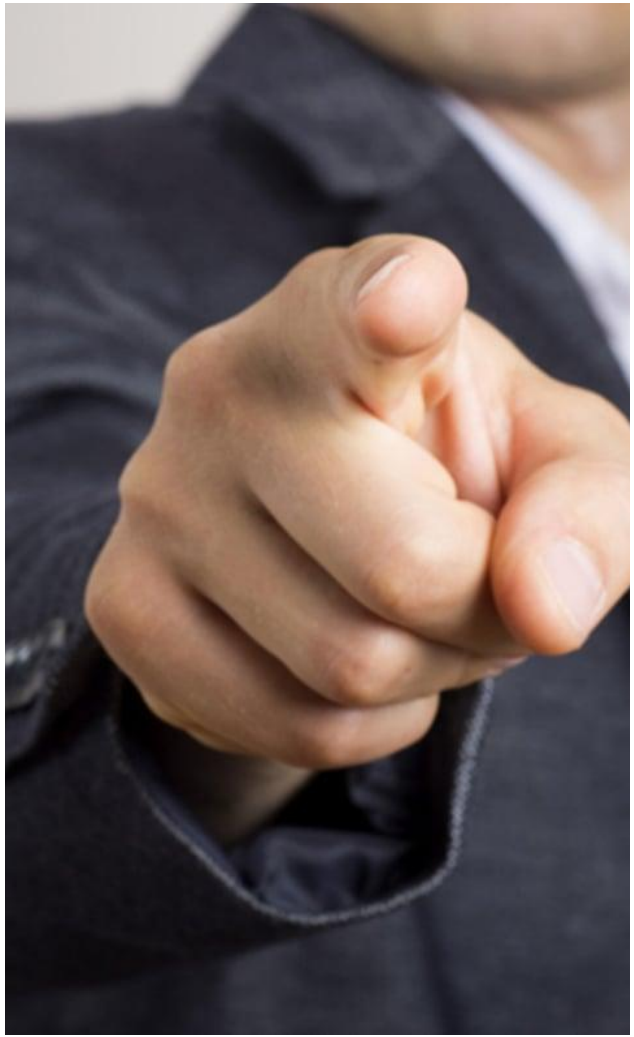
IF *An attacker identifies that our website is using NPM packages with publicly known vulnerabilities*

AND *those vulnerable packages have not been patched or replaced*

THEN *the attacker may exploit those vulnerabilities to execute malicious code in our environments*

WHICH WOULD RESULT IN *loss or disruption of our most critical service*

CAUSING *missed contractual obligations with customers*



IF

Describe the specific action, event, or threat actor activity that could initiate the risk, such as an attacker action, system failure, human error, or external event.

AND

Describe the circumstances, technical, procedural, or control weakness that would allow the threat event to lead to exploitation.

THEN

Describe the direct unwanted event or compromise that occurs when the threat exploits the vulnerability.

WHICH WOULD RESULT IN

Describe the direct consequence to the system, service, or data following the unwanted event.

CAUSING

Describe the ultimate business impact, such as financial loss, regulatory breach, contractual failure, operational disruption, or reputational damage.

REPEAT

But How?

Use the resources available. (standards, etc!)

Don’t be afraid to get advice/ help/ second opinion.

Use Risk Management.

Take time & do homework.

Go back to basics:

- Zero trust principles
- BIA and Risk Management

Connectivity is one of the chief vectors of cyber incidents.

Incidents are often multifaceted and not always technical.

Links

Me:

/milkmansson

@milkmansson

milkmansson