Connecting Up

techsoup NEW ZEALAND

Connecting Up is a not-for-profit organisation. Our purpose is to help fellow not-for-profits leverage the digital world to positively impact their communities. The digital world is expanding beyond IT software-hardware and digital marketing to new innovative service delivery and measuring social impact.

Connecting Up believe that not-for-profits with the right tools and skills can and do achieve great things for their communities. We have a long history of affordable software, hardware, educational events and group consulting. We partner with over 40 organisations to deliver high quality products and services specifically meeting the unique needs of the not for profit sector.

WWW.CONNECTINGUP.ORG

WWW.TECHSOUP.NET.NZ

Contact Us
E: events@connectingup.org P: (AU) 1300 731 844 (NZ) 09 8870 291

Advisory Boards Group
admin@advisoryboardsgroup.com

Cyber Risk

Monica Schlesinger FAICD
Advisory Boards Group

Agenda

Part 1

- *Risk Management – WHO, HOW, WHEN to identify, manage, transfer, accept or ignore.*
- *Cyber Risk in the context of Risk Management.*
- *How to identify the Cyber risks*

Risk Management - WHO?

Source:pixabay

Cyber Risk within Risk Management

Board - Managing risks that are outside of CEO Delegated (financial) authority [DA/DFA]

CEO - Managing risks from Management, up to the agreed Delegated (financial) authority [DA/DFA]

Management - Managing risks that are outside of CEO Delegated (financial) authority [DA/DFA]

Staff - Managing operational risks that are encountered in the day to day operations

Cyber Risk within Risk Management

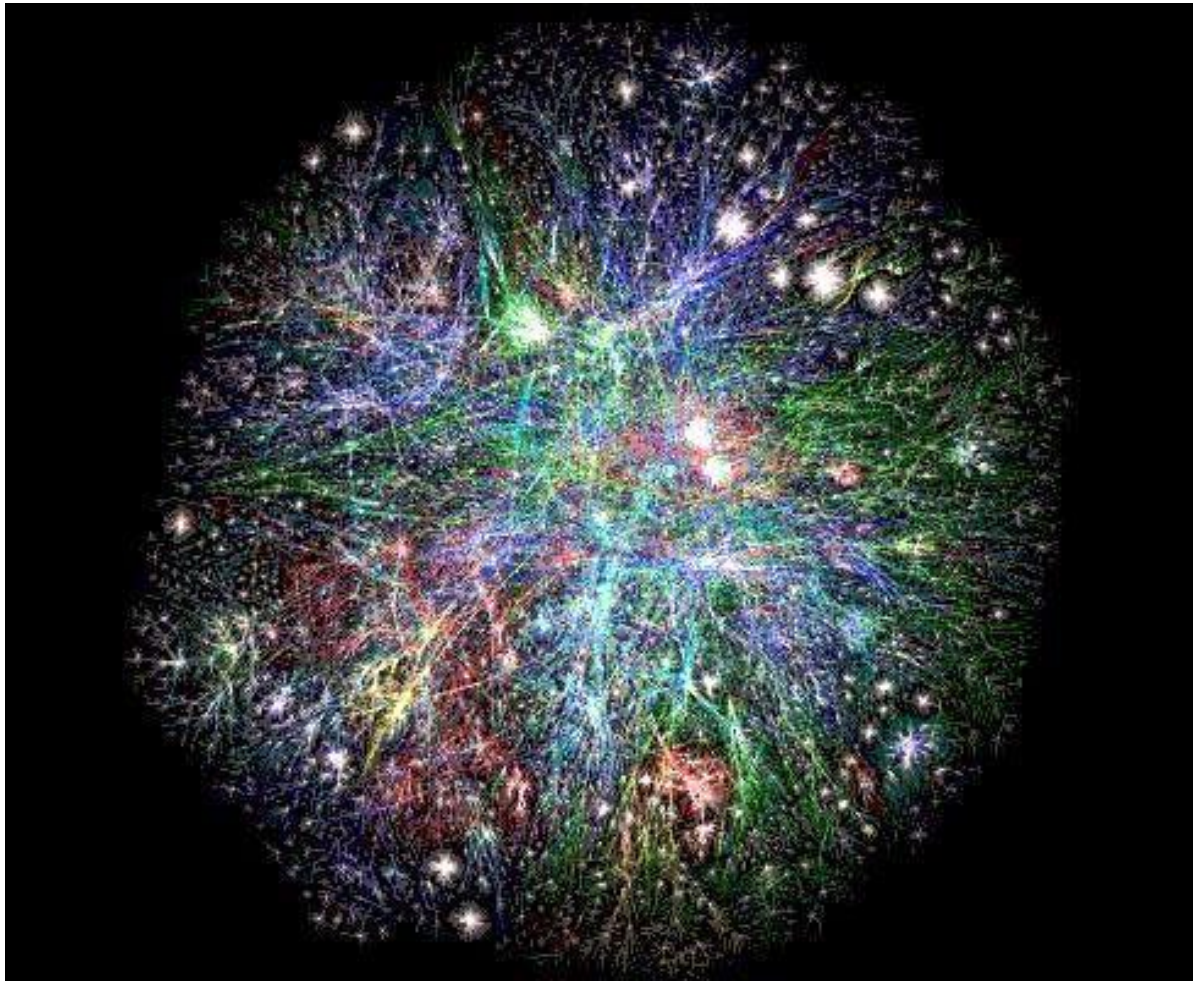
Operational aspect (CEO and organisation):

- ***Implementation*** of the Risk Management system
- ***Identifying*** the risks and opportunities
- ***Documenting*** and managing the risks
- ***Management*** of risks can be done at an agreed frequency
- ***Updating*** the Risk Register to show the changes and history of risks

Strategic aspect (Board):

- The board must create the ***Strategy*** for Risk
- The Board must define the organisation's ***Appetite*** for risk
- The board must manage the ***Extreme risks*** and the risks that are outside of the CEO's DA/DFA
- The board can appoint a Risk Management ***Committee***
- The board can vote on ***Opportunities*** that can benefit the organisation

Risk Management - HOW?



Source:pinterest 1990 - WORLD WIDE WEB by Sir Tim Berners-Lee

Risk Management – HOW?

Principles *(Duty of Care Risk Analysis Standard 5 ("DoCRA")*

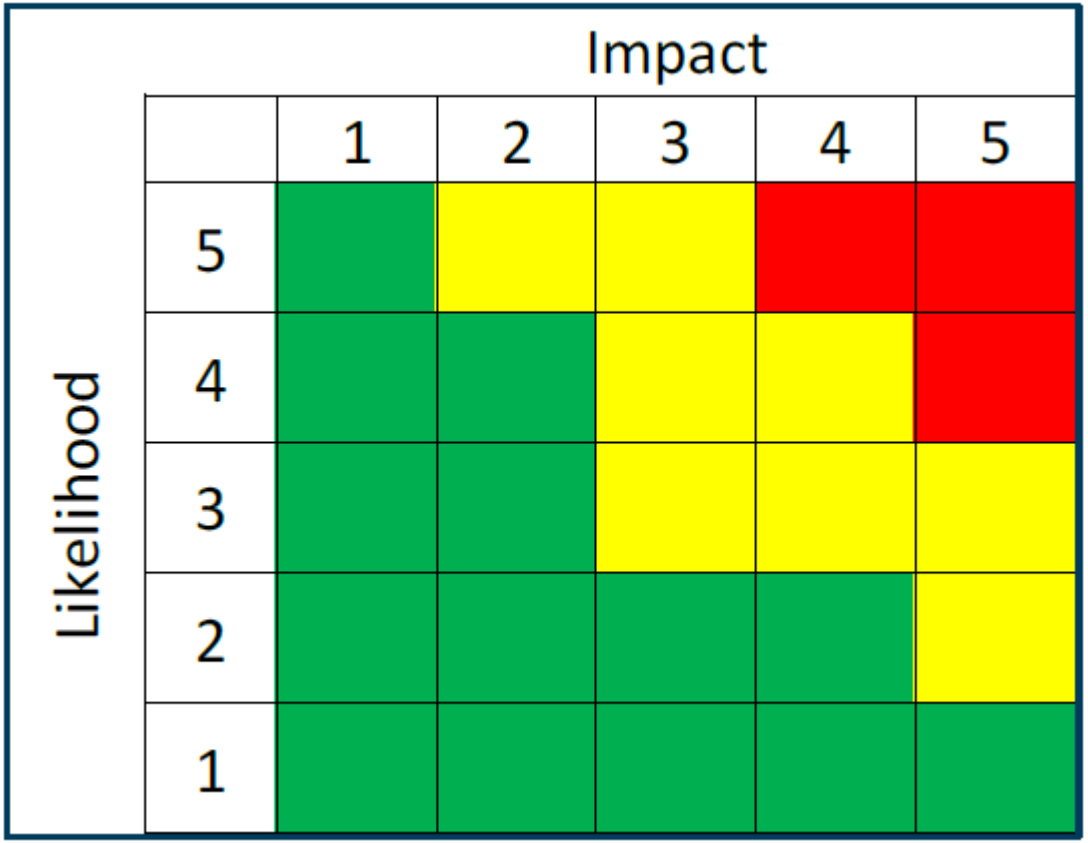
1. Risk analysis must consider the interests of all parties that may be harmed by the risk.

2. Risks must be reduced to a level that authorities and potentially affected parties would find appropriate.

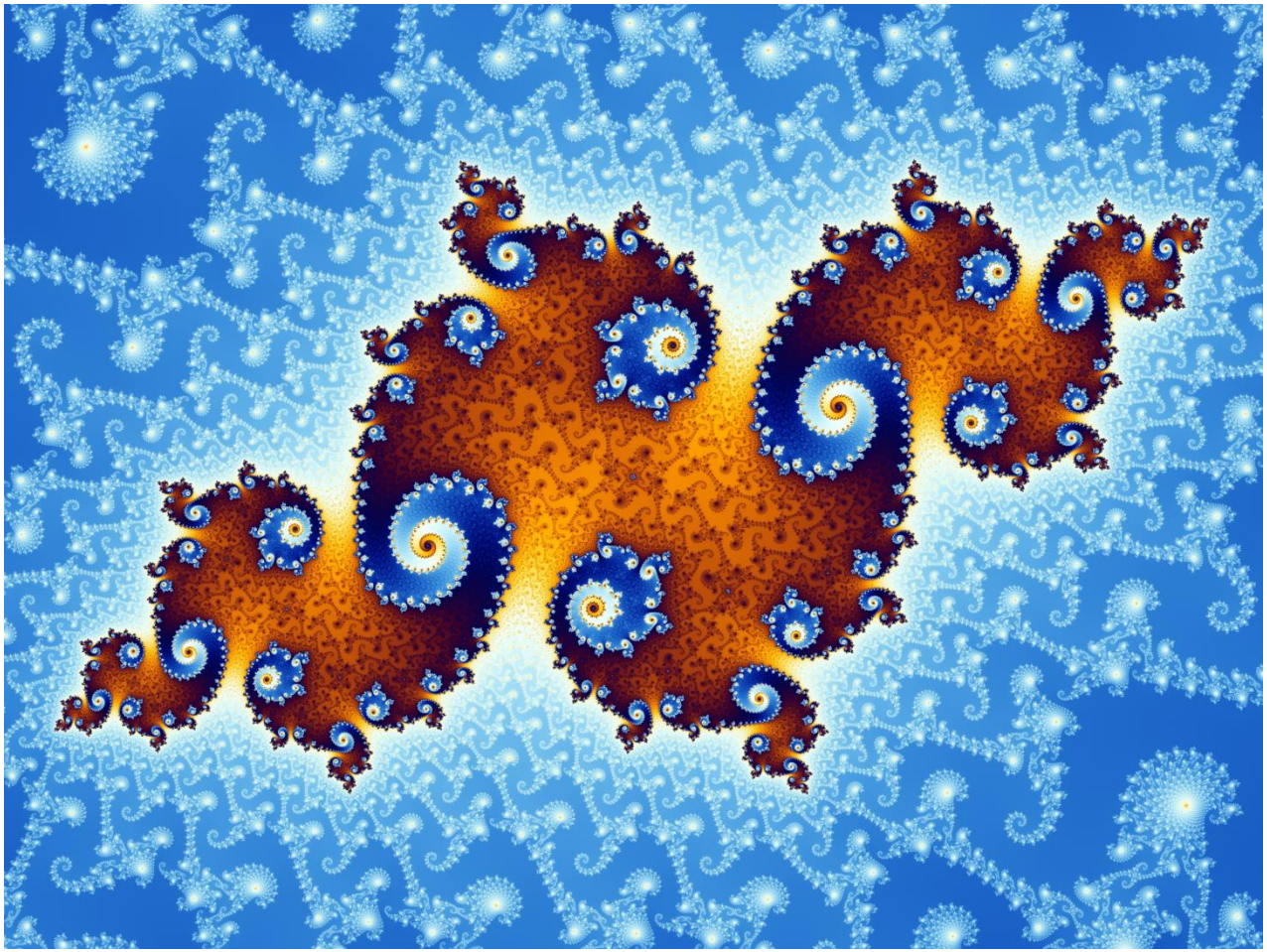
3. Safeguards must not be more burdensome than the risks they protect against.

Risk Management – HOW?

Heat map



Risk Management - WHEN?



Source:wikipedia - Mandelbrot

Risk Management – WHEN?

- Initial Risk workshops – for each department, executive team, then for the Board
- Weekly discussions in team meetings
- Risk Management Committee meetings (usually before Board meetings)
- Board meetings – Risk should be an item on the agenda

How to identify the Cyber risks

Establish a Risk Management System:

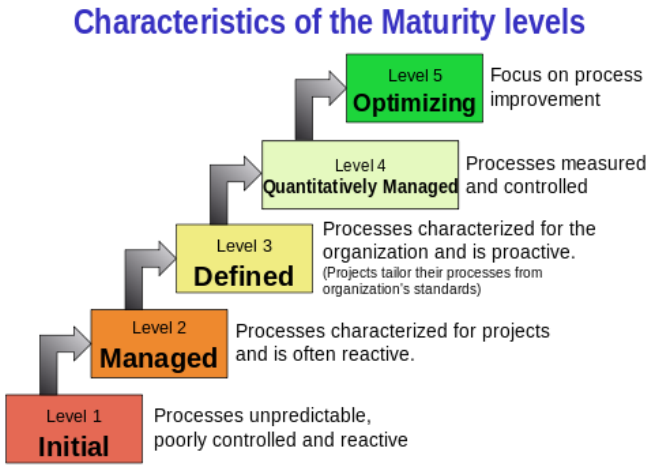
- Context (definitions, categories of risk, standards)
- Document processes, roles, responsibilities
- Frequency of discussions and meetings
- Document and agree on reporting
- Example: CIS - RAM (risk assessment method)

Train Board and Staff in Risk Management

Treat Cyber Risk as an Extreme or Very High Risk

How to identify the Cyber risks?

- Agree on the maturity level of your organisation (CMMI or NIST Tiers)



Tier	Definition
Tier 1	*Partial – Risk management process informal and ad hoc*
Tier 2	*Risk Management Process – Informed by organization risk objectives.*
Tier 3	*Repeatable - Risk Management Process – Enforced through policy, and updated with changes in the environment and threats.*
Tier 4	*Adaptive - Risk Management Process – Adaptive through lessons learned and continuous improvement.*

- CIS RAM worksheet

Thank You

- If you wish to contact us:

admin@advisoryboardsgroup.com

Or

monica@advisoryboardsgroup.com

Mob: 0419 797973

Advisory Boards Group offers Cyber Security Workshops, Directors & Officers Cyber Courses, Cyber Security Healthchecks & other services

Bibliography

- **Images:**
  - Pixabay
  - Pinterest
  - Wikipedia
- **Documents & methodologies:**
  - CIS RAM – Center for Internet Security – Risk Assessment Method
  - Advisory Boards Group - Cyber Risk Workshop
  - Advisory Boards Group – Risk Management Workshop