# Risk management at LINX

**Daniel Smith**
Cybersecurity Governance and Risk Manager

Wednesday, 29 May 2024

LINX122

# What is a risk?

- A risk is an uncertain event which may occur in the future
- A risk may prevent or delay the achievement of an organisation's objectives or goals
- A risk is not certain – its likelihood can only be estimated
- Not all risk is bad, some level of risk must be taken in order to progress / prevent stagnation

# What is risk management?

- Risk management is the process of identifying, assessing, prioritising, and mitigating potential risks
- It involves understanding the risks an organisation faces, making informed decisions about how to handle them, and implementing strategies to reduce their potential harm
- It is not about eliminating all risks
- Instead, it is about gaining a better understanding of the nature, scale and potential effects and then taking appropriate action

# Why is it important?

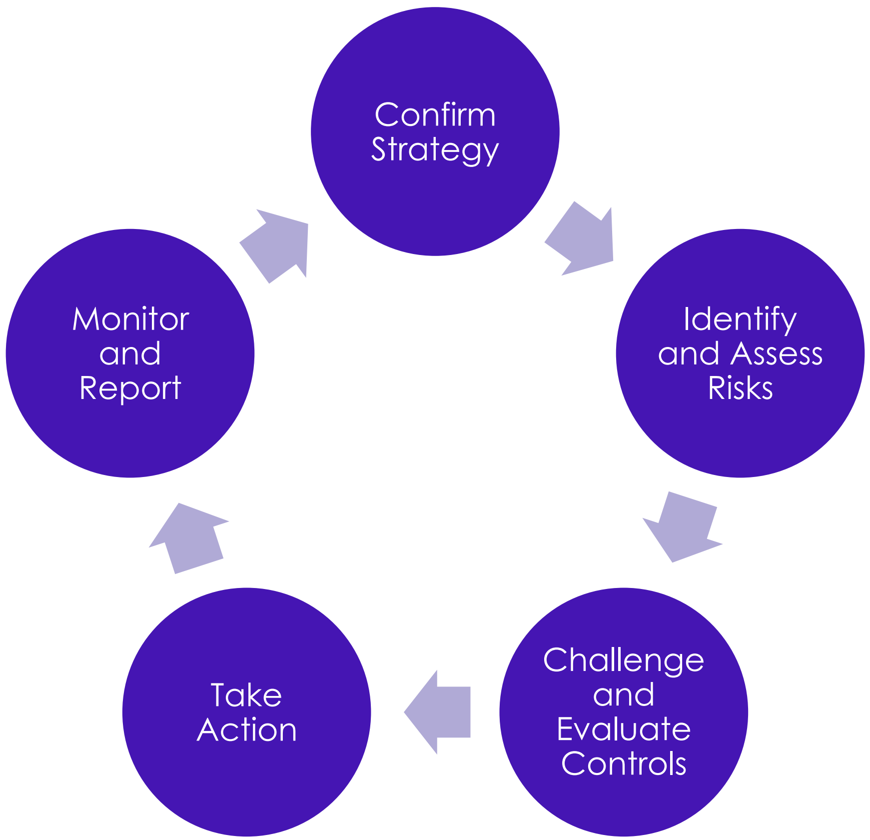
- Protection of assets and resources
- Business continuity
- Strategic decision-making
- Enhanced stakeholder confidence
- Compliance and legal requirements
- Improve resource allocation

*The only alternative to risk management is crisis management --- and crisis management is much more expensive, time consuming and embarrassing.*

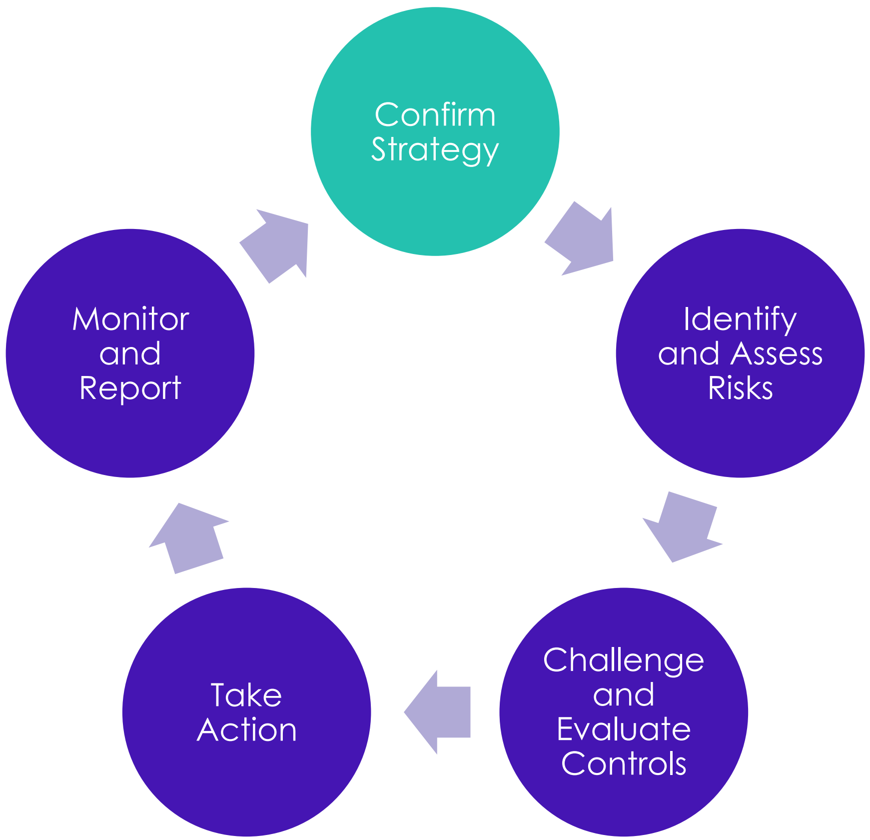
**James Lam**

**Enterprise Risk Management, Wiley Finance © 2003**

# Risk management cycle



# Risk management cycle – step 1



# Risk management responsibilities

- Cybersecurity Governance and Risk Manager
- Senior Management Team
- Board
- Asset owners
- Risk owners
- All staff

# Risk register

- We use a risk register to capture risk data in a standard format
- A risk register provides the means of describing, scoring and ranking risks
- It identifies ownership, controls in place, the need for further reduction and the recording of additional controls that are to be put in place
- The overall aim of the risk register is not to document all the risks faced by an organisation, but the more significant ones and to record the action plans to mitigate those risks to acceptable levels

# Asset identification

- We use an asset-based assessment for the risk register
  - An asset is anything we want to protect
- First, we identified a series of top-level assets which the business relies on to function
  - Essentially, these are the core things that we want to protect
- Then for each top-level asset, we identify the critical assets that underpin them
  - We also identify the function of that asset and any critical dependencies

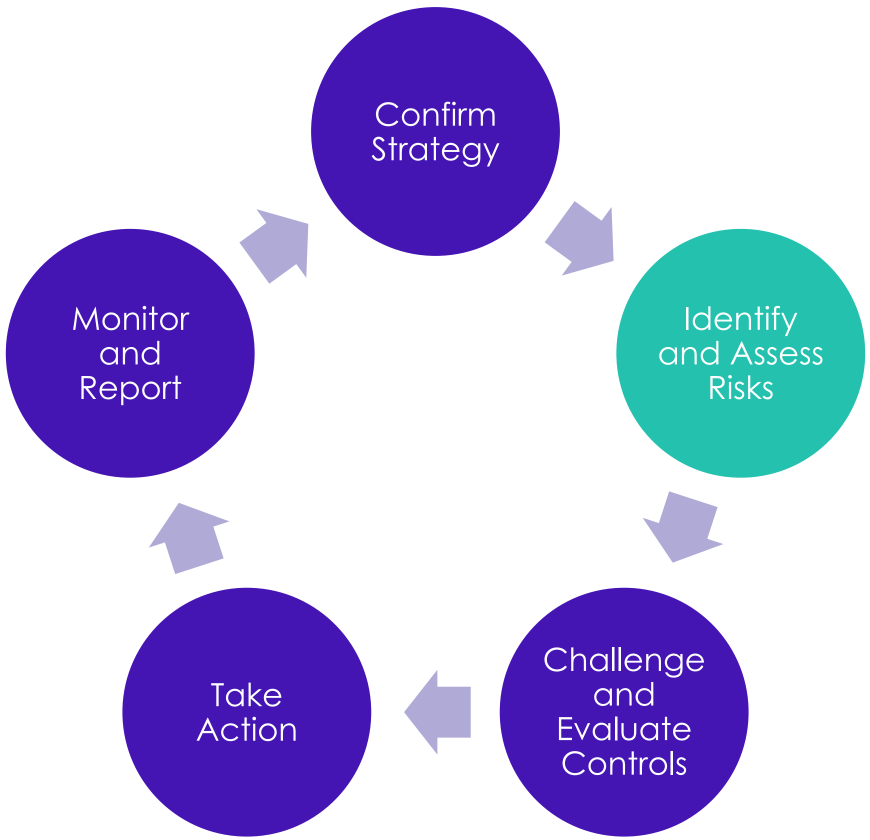
# Top-level assets

1. Exchange platform
2. Economic viability
3. Financial controls
4. Legal and regulatory
5. Reputation
6. Welfare
7. Skills
8. Business support operations
9. Public Affairs
10. Governance
11. Mutuality

# Asset resilience analysis

- We subsequently undertake a resilience analysis for each of our critical assets
- This is designed to assess how resilient these assets are against unidentified risks
- For each asset, we ask five questions in relation to it
    1. Do we know what we want?
    2. Do we know how to deliver it?
    3. Can we deliver it?
    4. Can we protect it?
    5. Can we recover it?
- This shows the asset's overall resilience with identified risks being permitted exceptions

# Risk management cycle – step 2



# Threats and vulnerabilities

- For each critical asset, we identify the threats facing it and the associated vulnerabilities
- A vulnerability is a flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by a threat
- A threat is a potential for a threat agent to exploit a vulnerability
- A risk is the potential for loss when the threat happens

linx

# Mitigating assets

- We also identify any assets that mitigate the impact or likelihood of the threat materialising
- However, for an asset to be considered mitigating it has to be subject to the asset resilience analysis so we can identify if we have any critical dependencies that are particularly vulnerable

# Risk scoring

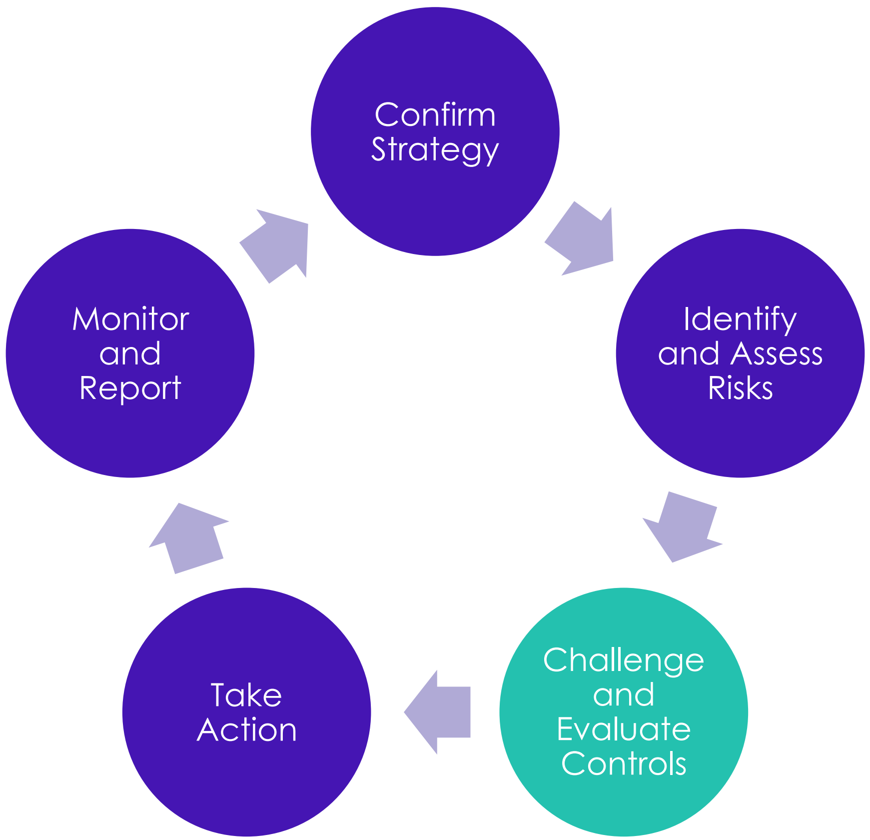
- Each critical asset was given a score from 1 to 5 to determine the maximum impact of a failure of that asset
- Each threat was then given a score from 1 to 5 to determine the likelihood of it occurring
- Risk owners were asked to provide an inherent score for both impact and likelihood and a residual score
    - Guidance was provided to help owners judge a suitable impact and likelihood score
- An inherent and residual score for each risk was then calculated using a weighted risk scoring matrix

linx

# Weighted risk scoring matrix

| Likelihood | Impact | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 5 | 5 | 10 | 15 | 20 | 25 |
| 4 | 4 | 8 | 12 | 18 | 20 |
| 3 | 3 | 7 | 10 | 12 | 19 |
| 2 | 2 | 6 | 8 | 10 | 17 |
| 1 | 1 | 2 | 4 | 8 | 15 |

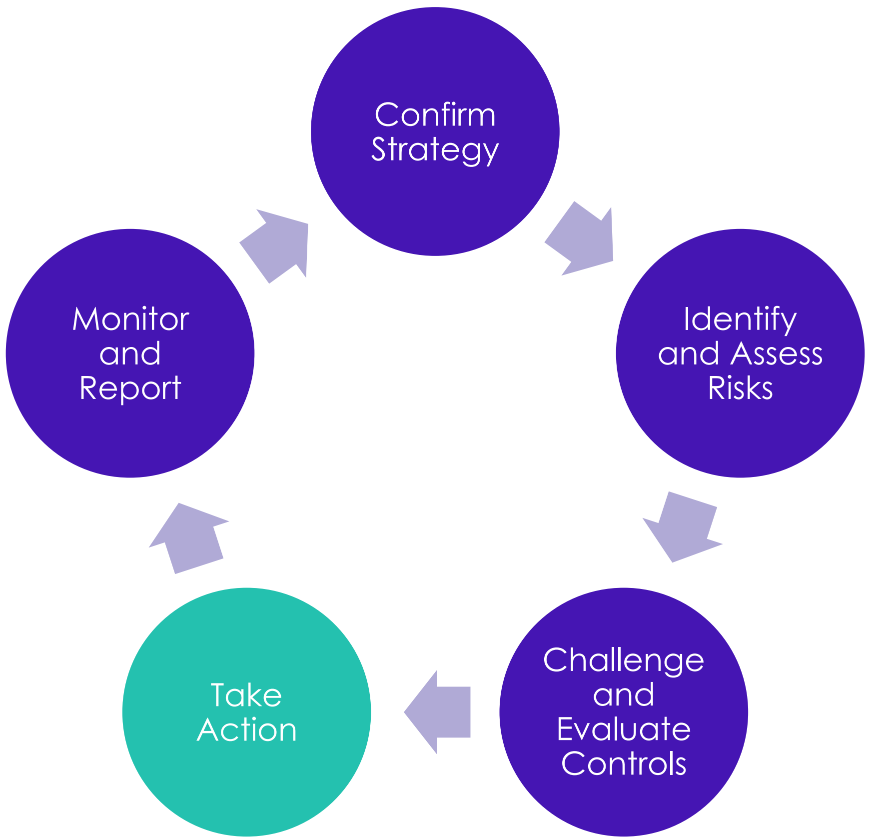
# Risk management cycle – step 3



# Risk status

- Each risk is given a status i.e. whether it is controlled, accepted or needs mitigation.
  - Controlled means we have controls in place that we consider broadly adequate/fit for purpose
  - Accepted means we believe that it is outside our control or not susceptible to further controls that we consider practical and within our reasonable capabilities
  - Needs mitigation means we believe further steps could and should be taken by us to further mitigate the risk
- When considering whether a risk is controlled, we only take account of mitigations that are identified in the asset list and have been subject to the asset resilience analysis
- If no mitigating assets could be identified, the risk must be described as accepted or needing mitigation

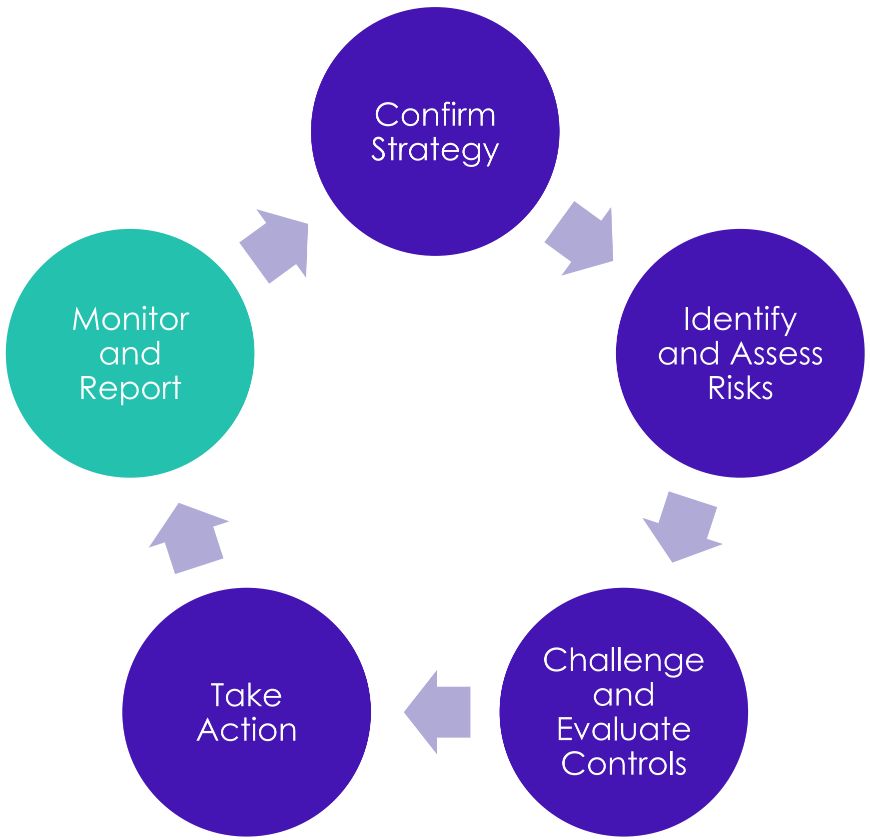
# Risk management cycle – step 4



# Implementing risk treatment strategies

- Risks scored below 8
  - It is not necessary to treat risks with a score below 8
  - These risks are monitored by the relevant risk owner and reassessed annually
- Risks scored 8 and above
  - Members of the Senior Management Team review all these risks and assess whether the controls identified are sufficient to control the risk
  - If new controls are required, the SMT member will be responsible for coordinating action to ensure new controls are put in place for the relevant risk
- Risks scored 12 and above
  - All risks scored 12 and above are reviewed and discussed at Board level
  - Strategies for treating these risks must be approved by the Board

# Risk management cycle – step 5



# Risk monitoring and reporting

- Risk owners update and review the risks allocated to them annually
- The Senior Management Team then review existing risks and identify any additional risks to ensure consistency of reporting and scoring
- The outcome of this process is presented to the Board
- Risks may also be fast-tracked on to the risk register by members of staff if an urgent issue were to arise
    - This could result from a serious incident, complaint or claim, risk assessment, internal/external assessment or other ad hoc report/review

# Risk landscape

- Geopolitical risks
- Threats to the global supply chain
- Energy supply
- New laws and regulations
- Overseas expansion

# Thank you

daniel@linx.net

linkedin.com/company/linx/

facebook.com/LondonInternetExchange/

twitter.com/linx_network

youtube.com/user/LINXnetwork