Cisco
Customer Experience

Regulations inbound

Operational resilience: What does it mean for the way we conduct business?

Tim (Wadhwa-)Brown, Security Consulting Senior Engineering Technical Leader

CX CoE Security

Regulatory updates

- UK
  - Telecom Security Act
  - Data Protection and Digital Information Bill
  - Online Safety Bill
  - Updates to Network and Information Systems Regulations (NIS Regulations)?
  - Changes to operational resiliency regulations (PS21-3 etc)?
  - Reform of Computer Misuse Act?

- European
  - **NIS2 Directive**
  - European Cyber Resilience Act
  - **Digital Operational Resilience Act (DORA)**
  - Critical Entities Resilience Directive (CER)
  - Digital Services Act (DSA)
  - Digital Markets Act (DMA)
  - European Chips Act
  - European Data Act
  - European Data Governance Act (DGA)
  - EU Cyber Solidarity Act
  - Artificial Intelligence Act
  - Artificial Intelligence Liability Directive
  - European ePrivacy Regulation
  - European Digital Identity Regulation
  - ...

DORA: A quick summary

- Requirements applicable to **financial entities**
- Requirements in relation to the contractual arrangements concluded between ICT third-party service providers and fi entities
- Rules for the establishment a nduct of the **Oversight Framework for critical ICT** third-party service providers
- Rules on cooperation among **competent authorities**, and **rules on supervision and enforcement by competent authorities** in relation to the regulation

Taken from article 1: Subject matter

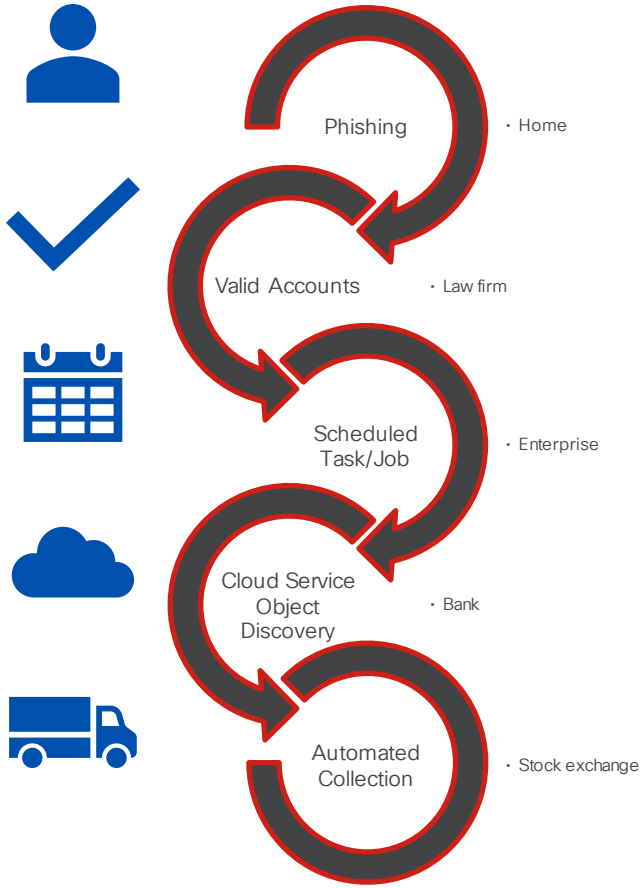
- Information and communication technology (IC sk management**
- **ng of major ICT-related incidents** notifying, on a voluntary basis, ignificant cyber threats to the competent authorities
- **Reporting of major operational or security payment-related incidents** to the competent authorities by financial entities referred to in Article 2(1), points (a) to (d)
- Digital operational **resilience testing**
- **Information and intelligence sharing** in relation to cyber threats and vulnerabilities
- Measures for the **sound management of ICT third-party risk**

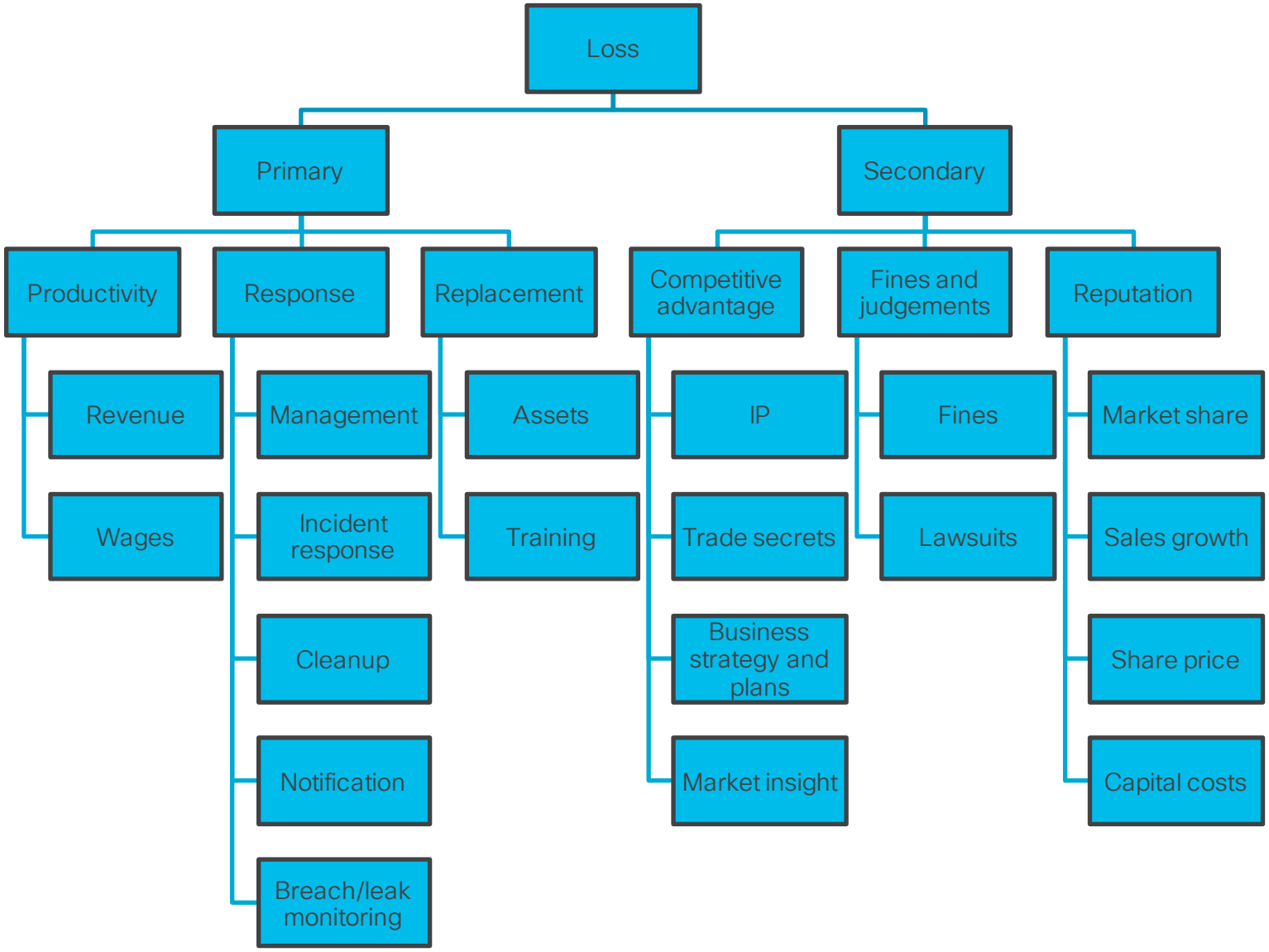
Threat landscape

Why these regulations are necessary

Worst case scenarios

- Technical failure
  - CNI networks
  - 3rd party systems
    - Payment networks
    - Telecoms networks
- Financial failure
- Societal failure
- Cyber
  - State
  - Terrorism
  - Criminal





Regulation necessary to address market gaps

DORA etc will force organisations to address externalities inherited from 3rd parties

Addressing risk

- I am not your lawyer :)
- 2 bears
  - Regulator
  - Threats
- Everyone’s a third party for someone these days
  - Hybrid working
  - SaaS
  - Digitisation of everyday life
- Risks can be inherited

- Similar to NIS2, DORA will define incident severity incidents
  - Not yet finalised
- Fines from the supervisory authority
  - Financial entities: Up to 2% of the global yearly revenue
  - Third party ICT service providers: Up to €5000000

3rd party risk by numbers

- On average, organisations share confidential information with around 583 third parties*
  - 34% of respondents admitted to maintaining comprehensive inventories
  - 63% of respondents believed they lacked resources to manage third-party relationships
  - Only 35% rated their third-party risk management programs as highly effective

* Taken from Data Risk in the Third-Party Ecosystem study by the Ponemon Institute, 2018

Considerations

- Direct will depend on the nature of the FSI but..
  - Impact of online payment services, platforms and infrastructure
  - Impact of customer/member account services, platforms and infrastructure
  - Imagine losing a system of record or similar….
- Indirect
  - Impact of cross-border arrangements
  - Impact of emergencies, societal failure etc
  - Impact of Internet access and public communications networks
  - Impact of managed service providers
  - Impact of DNS services
  - Impact of CDN providers
  - Impact of cloud services
  - Impact of data centres
  - Impact of supply chain
  - Impact of managed security service providers
  - Onwards dependencies

Even for UK businesses, expect to see regulatory changes and increased contractual pressures...

Constructing a DORA strategy

Avoiding piecemeal implementation

NIS2 vs DORA

- If NIS2 can be seen as defining capability for all critical national infrastructure
  - DORA adds the necessity for a maturity model and more detailed operational lifecycle for financial services
  - Testing is only one aspect to DORA
    - Risk management
    - Managing 3rd party risk
    - Oversight frameworks for critical 3rd party service providers
    - Incident management, classification and reporting
    - Information sharing

Questions that DORA raises

- What does an organisational approach look like?
- What should the programme of work look like?
- What does the RACI look like?
- How should it be measured?
- How can maturity be demonstrated?
- How can improvement be baked in?

Metrics that matter

- Requirements
  - An early warning within 24 hours of becoming aware of the significant incident
  - An incident notification within 72 hours of becoming aware of the significant incident
  - Upon the request of a CSIRT or, where applicable, the supervisory authority, an intermediate report on relevant status updates
  - A final report not later than one month after the submission of the incident notification
- Operational capabilities
  - Mean time to detect
  - Mean time to respond
  - Mean time to recover

What about CBEST?

- Can CBEST alone assess and measure operational resilience?
  - https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide
- PS21-3 from the FCA would imply not
  - https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience

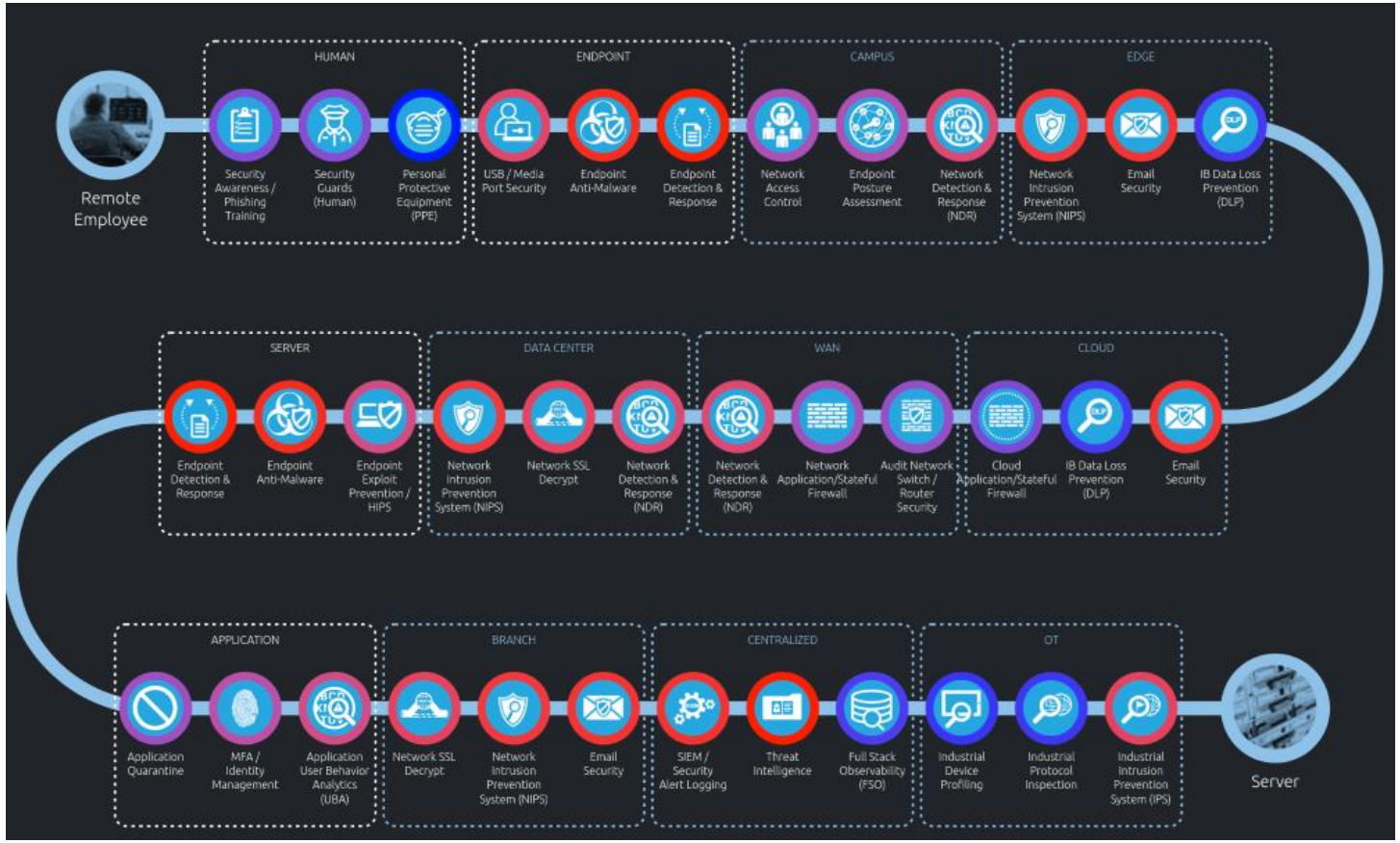
A maturity model for Threat-Informed Defense

- Risk management
  - https://www.riskmaturitymodel.org/
    - Managing 3rd party risk?
    - Oversight frameworks for critical 3rd party service providers?
- Incident management, classification and reporting
  - https://www.soc-cmm.com/
- Digital operational resilience testing
  - https://www.redteammaturity.com/
- Information sharing
  - https://www.crest-approved.org/buying-building-cyber-services/cyber-threat-intelligence-maturity-assessment-tools

Understand your threat model

- Ask yourself
  - What would happen if another pandemic hit?
  - What about ransomware?
  - Do I support any critical customers?
  - Do I know how to contact the regulator?
  - What revenue generating/service impacting systems to I have?
  - How many weeks can I operate for if we're offline?
  - Do I understand and monitor my dependencies?
  - Can I demonstrate and measure reliability?
  - What processes can I not do without?
  - Which 3rd parties do I rely on?
  - Which 3rd parties rely on me?
  - Who do I call if it all goes wrong?

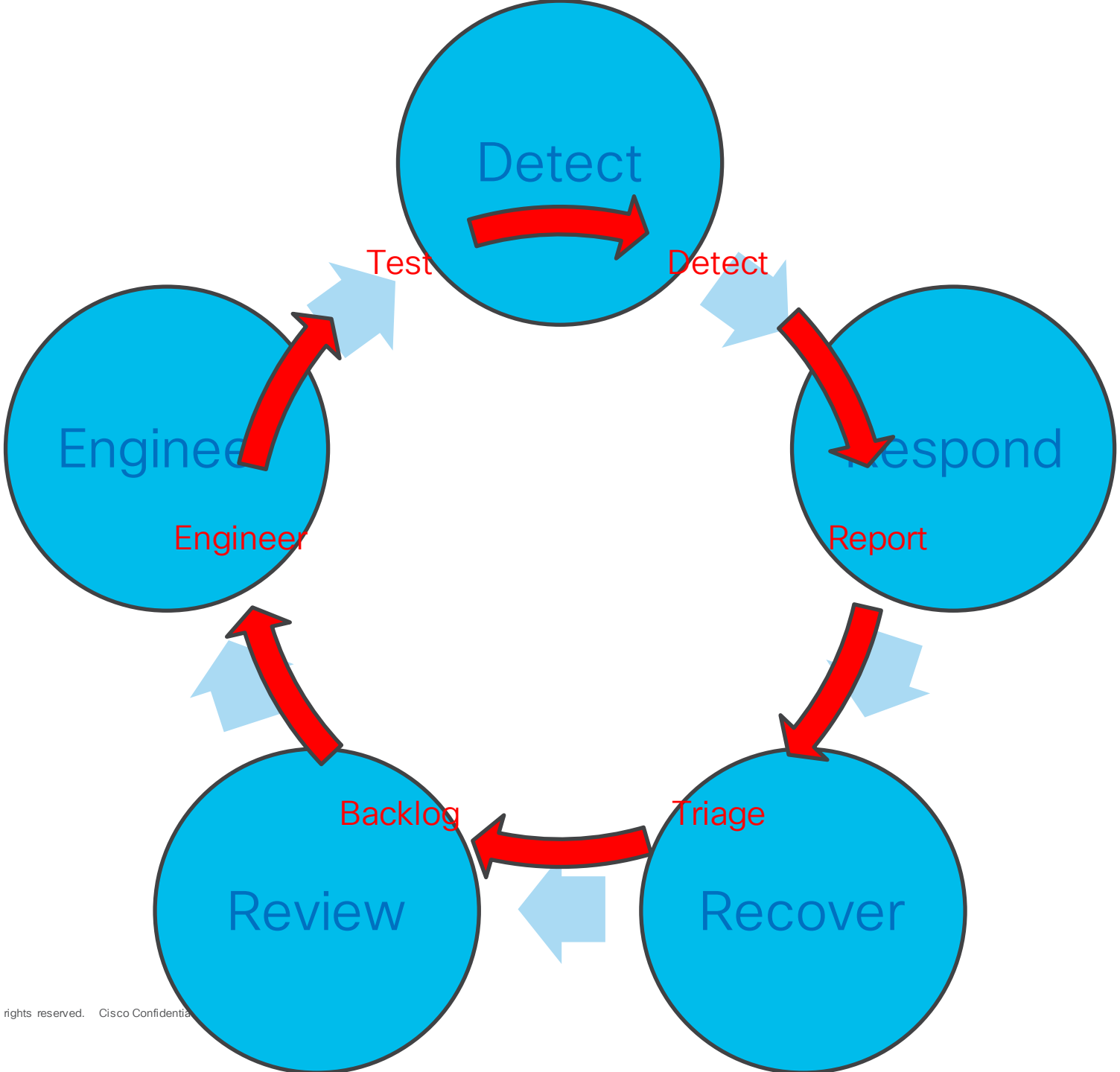
Apply a threat-informed defense

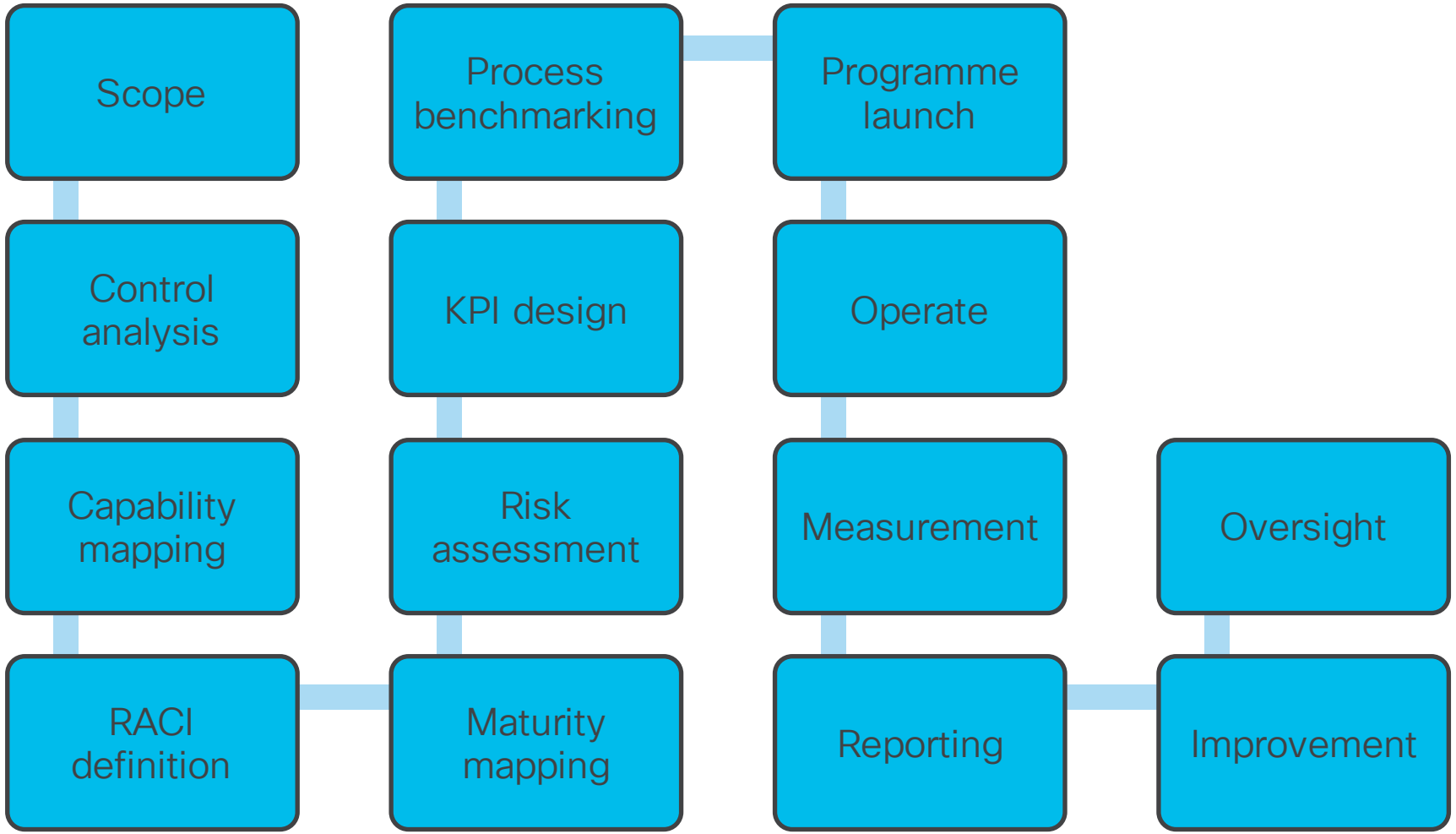


Prioritise treatment by risk:reward

- Over 70%* of breaches involve the human element e.g. stolen credentials
  - What business services do you use that don't support MFA?
  - What passwords do you need to access 3rd party systems?
- Over 80%* of breaches involve a compromised device e.g. a server, an endpoint or a mobile
  - Can employees access your business services from devices they own?
  - Do you work with 3rd parties who rely on contacting you on personal devices?

* Taken from Verizon's DBIR Report, 2023





Themes we're seeing

- What are others doing?
  - How are Cisco addressing these changes?
  - How does Cisco's product suite help us address the changes?
- What threats affect us?
  - Can you help measure our hot spots?
  - Can you help measure and improve our availability?
  - Can you kick the tires with a table top exercise?
  - Can you run our DORA programme?
- What's next...
  - Compliance as code...
  - Chaos engineering...

Sample timeline

DORA journey

Model threats relevant for the organisation

Assess visibility in the environment and identify blind spots in your logging

Compare your security posture against the requirements of the specific DORA legislation

Jan 2024 | Jun 2024 | Jan 2025

Test security controls and train the security team during a Red or Purple Team simulation exercise

Implement automation in operations through Security Engineering

Respond to changing threat landscape

Make UK & Europe a hostile place for criminals

(to paraphrase NCSC)

Next steps

- Start with NIS2 capabilities
  - https://www.cisco.com/c/m/en_emea/products/security/nis2-directive.html
    - Engage with internal stakeholders
    - Consider, based on size, investigating Cyber Essentials
    - Review your ISO27001 ISMS if you have one
    - Document your critical assets
    - Contact 3rd parties with whom you have significant business relationships
    - Carry out a table top exercise
    - Engage an Incident Response Partner
- Evaluate and set DORA/PS21-3 maturity levels?
- Build and execute programme

Questions?

twadhwab@cisco.com


Cisco
Customer Experience