GRC

Deepdive Architectural blueprint and MDP

Robert Dirks

Security Architect - Shield vzw

Introduction

Purpose
Agenda

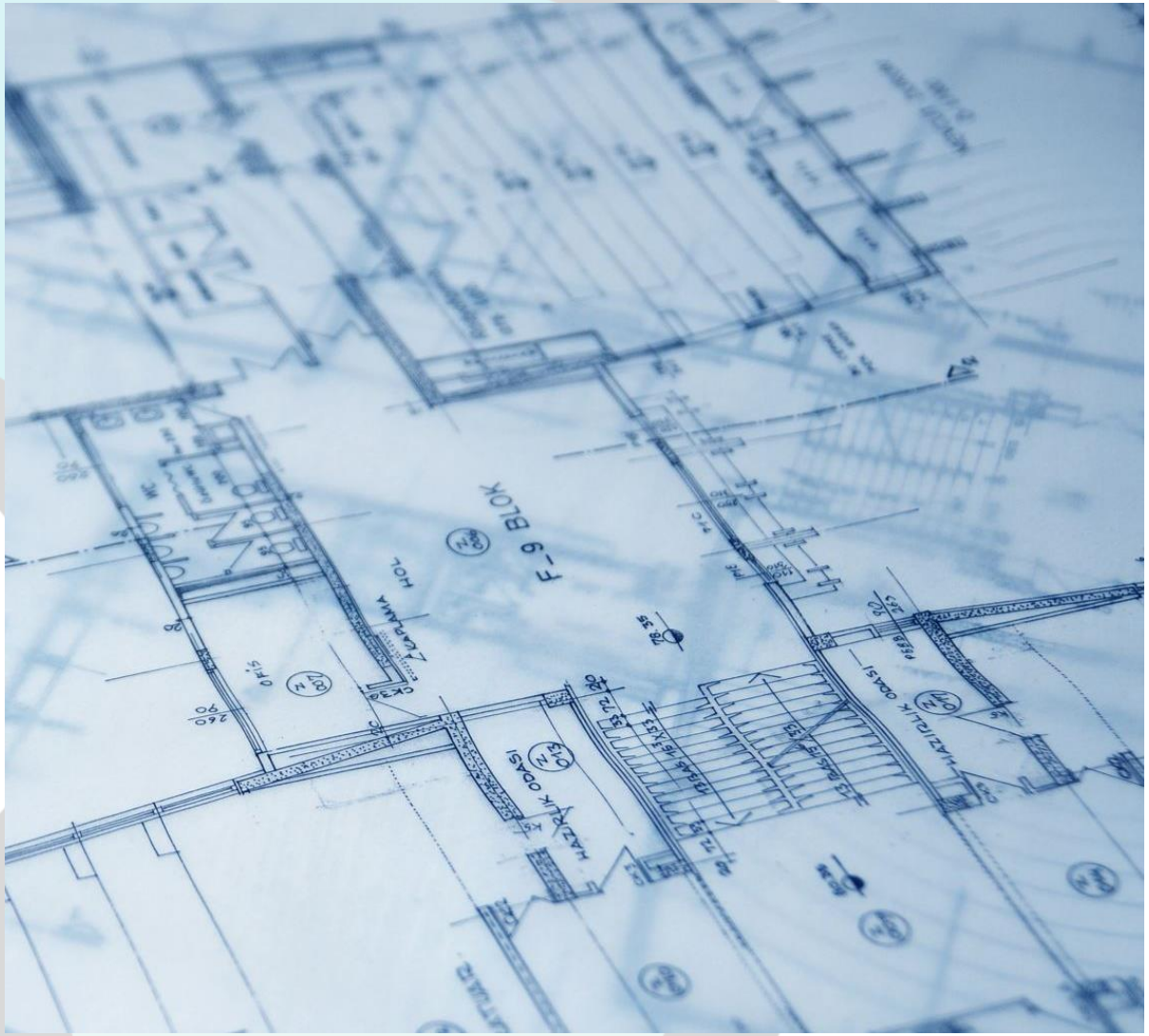
Introduction

- Purpose
  - Provide more information on
    - Architectural blueprint
    - Medical Device Policy (MDP)
- Agenda
  - Sit-rep (20 minutes)
    - The GRC Team
    - Assessments
    - Visualisation PowerBI
    - ISO27001 implementations
    - Architectural blueprint
  - Q&A (10 minutes)

Architectural blueprint

Deepdive into the blueprint and the Medical Device Policy

Why



- Industry-Specific blueprint
  - Policies, Procedures & Guidelines
- ISO 27001 & CyFun based
- Regulatory requirements
- Risk management

The mystica aspect of GRC

GRC is the integrated collection of capabilities that enable an organization to achieve objectives, address uncertainty, and act with integrity while ensuring IT governance aligns with business goals.

Source: ISACA

A framework for managing company policies, risk exposure, and compliance obligations to maintain ethical standards and regulatory requirements.

Source: Gartner

A structured approach to aligning IT with business objectives while effectively managing risk and meeting compliance requirements.

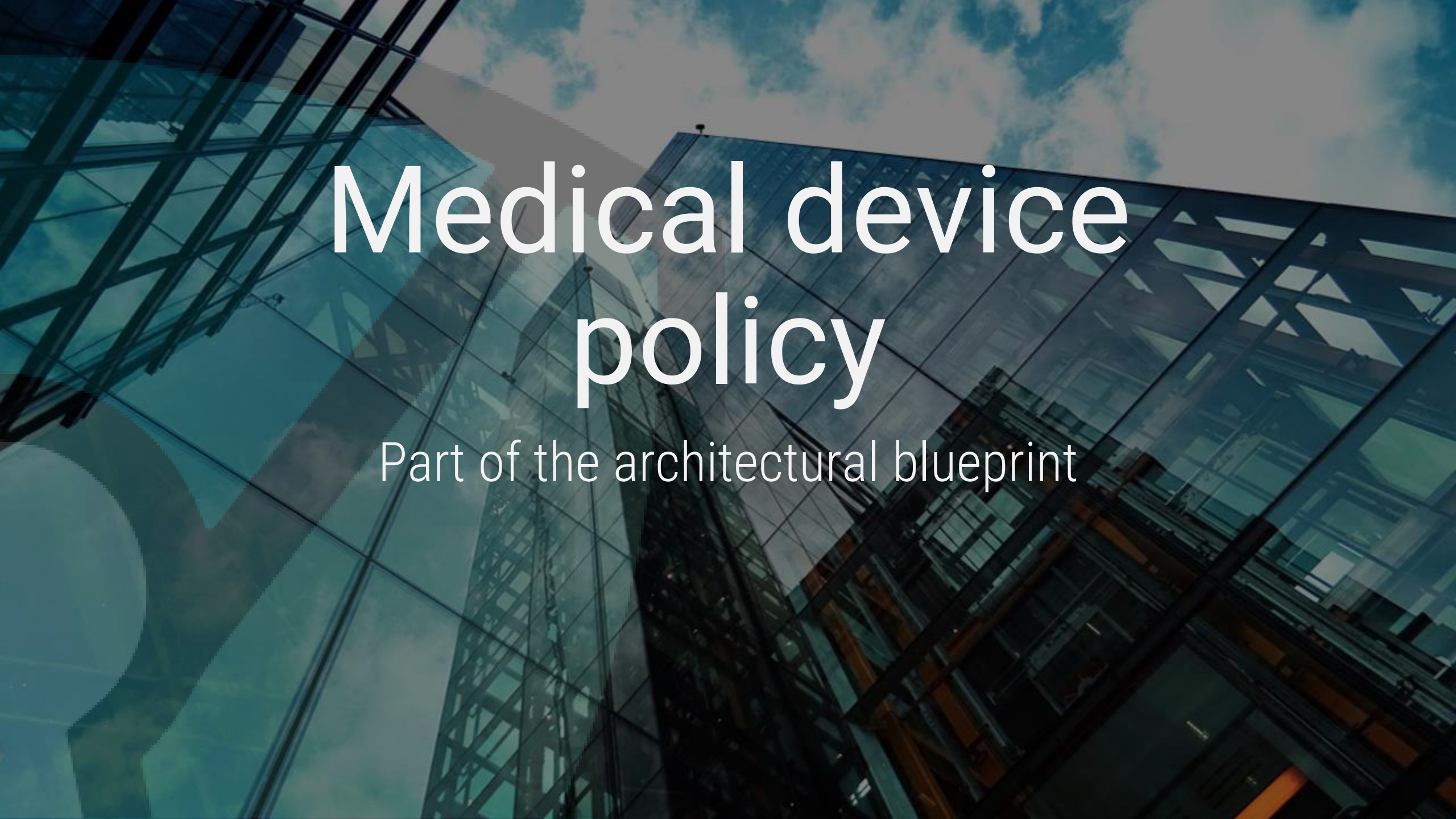
Source: NIST

Framework supporting Governance, Risk & Compliance

- Governance
  - Strategic alignment with business objectives
  - Clear roles & Responsibilities
  - Structured decision-making
  - Continuous improvement
- Risk
  - Threat & Vulnerability management
  - Risk identification, Assessment & Treatment
- Compliance
  - Regulatory & ISO 27001 Adherence
  - Audit readiness & Documentation
  - Monitoring & Evidence-based controls

Template documentation

- Providing a blueprint of
  - Policies
  - Procedures
  - Processes
- To align business with security and reduce organizational risks
- Using reference
  - Frameworks
    - ISO27001
    - CyFun



Medical device policy

Part of the architectural blueprint

Medical Device Policy (MDP)

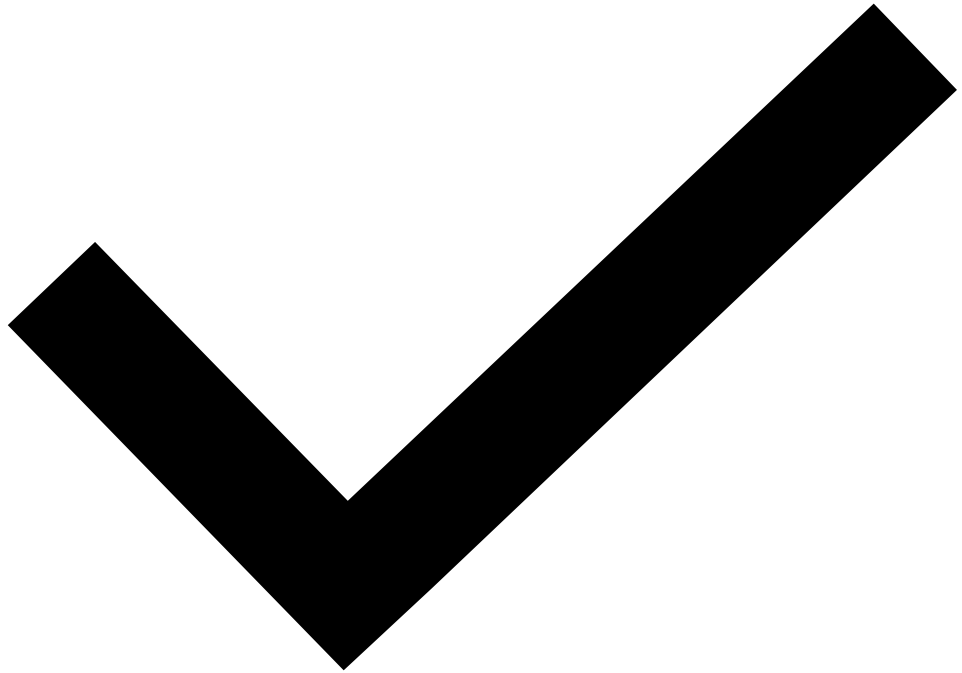
- Update
  - 1.0 version
  - Reviewed
    - Community
    - Suppliers (via Agoria)
- Deepdive
  - Definition
  - Asset management
  - Suppliers management
- In the future

Reason to define the policy

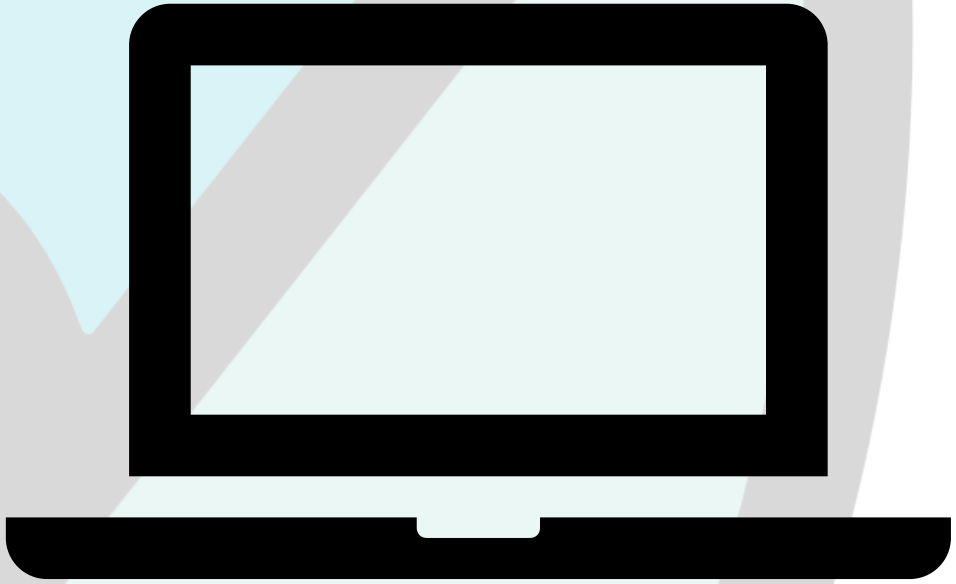
- Structure a risk based approach
  - Remove aspects based on the identified risk
- Single template to be applied
- Issue of no industry specific policy

Update

- 1.0 version finalised 25 Februari 2025
- Besides the policy
  - Leaflet
    - Providing information on the usage of the policy and the other documents
  - Mappingstable, definition and risk matrix
    - Mappingstable to other frameworks
    - Definition and basis of the definition
    - Risk matrix and scenario's
  - Lifecycle Medical Device
    - Process
    - RASCI
    - Operational checklists



Deepdive



- Asset management
  - If there is none these are the requirements
    - Register
      - Hostname
      - MAC Address
      - Hardware specifications
      - Serial numbers
      - Additional info (based on MSD2)
    - Maintain the register

Deepdive

- Supplier management
  - Comply to hospital policies
  - Comply to sector specific frameworks
  - Documented evaluation
  - Access management requirements

Deepdive

- Risk·Classification:¶

Category·of·information¤	MDR·Medical·Device·Class¤			
	Class·I¤	Class·IIa¤	Class·IIb¤	Class·III¤
Special·Personal·Data¤	5¤	5¤	5¤	5¤
Information·Decision·for·the·Care·Process¤	3¤	3¤	4¤	5¤
Ordinary·Personal·Data¤	2¤	2¤	3¤	5¤
Information·Supporting·the·Care·Process¤	1¤	2¤	3¤	5¤

·Summary·table·of·the·5·risk·class·scale·of·medical·devices°¶

- Risk scenario
  - 1-5
  - Data categories
    - Supporting care information
    - Ordinary personal data
    - Special personal data
    - Decisive care information
  - Identify risk related to information security

Future

- Excel mappingstable per category
- Mapping tenders to frameworks
- Review for broader public
- More indepth suppliers or vendor risk management / evaluation
- Translation of the document (Adoptation of the industry)

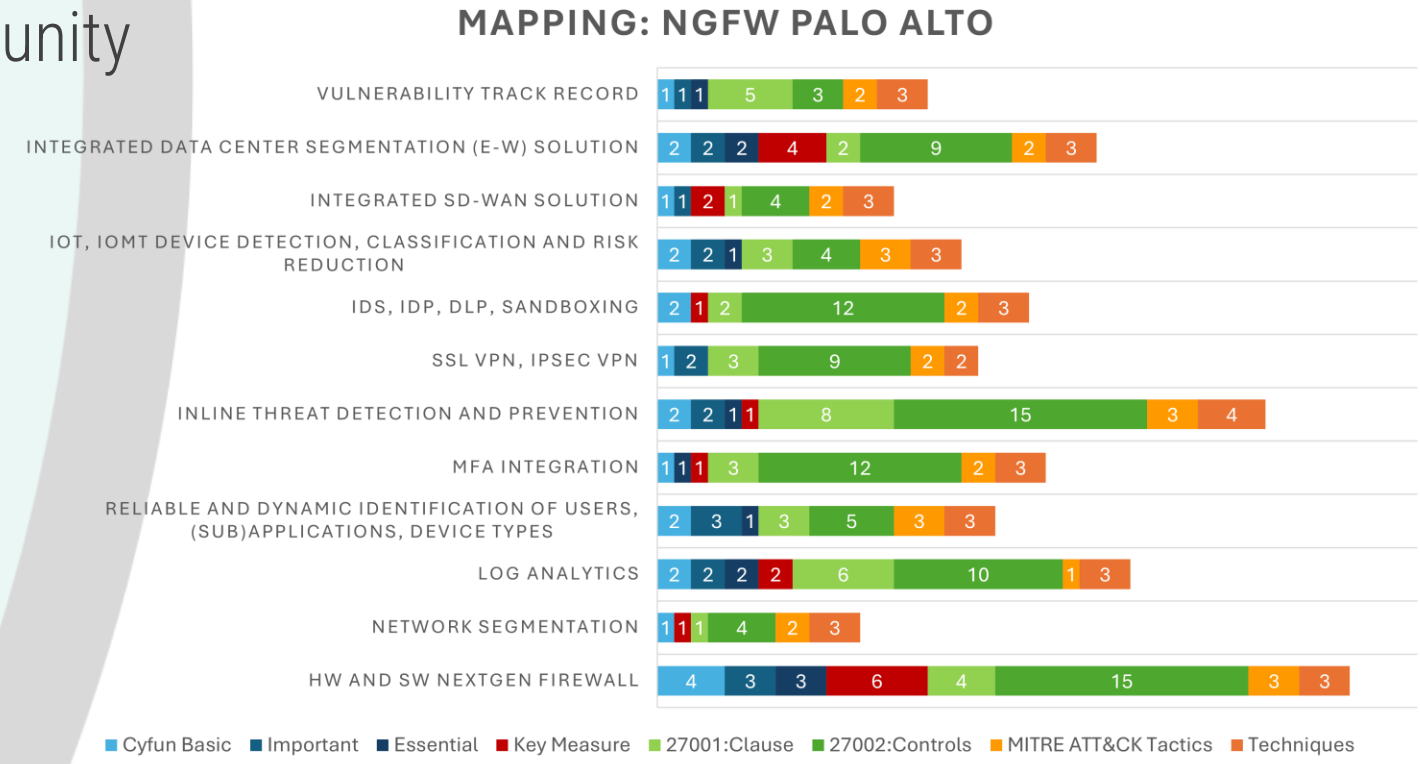
Excel mappingstable per category

- Review the categories with experts (BioTek / BioTD)
- Define weight matrix classification
- Review by GRC experts

Medical Device		Device Application		MDR	Data Categories				Environment Risk			Risk Classification		
Types	Types Notes	Sub-types	Sub-type Notes	MDR Class	Supporting Care Information	Ordinary Personal Da	Special Personnal D	Decisive care Informatio	Clinical Environement	Invasiveness	Fallback / Redundancy	Risk Sum	Risk Score	Risk Interpretation
Angiography	Imaging of blood vessels using contrast dye and X-rays.	Diagnostic Angiography	Typically lower risk, as it involves imaging without extensive intervention.	Class IIb	Yes	Yes	Yes	Yes	Ancillary / Diagnostic	Invasive / Surgical	No Redundancy	17	5	Severe (Highest) Risk
Angiography	Imaging of blood vessels using contrast dye and X-rays.	Interventional Angiography	Medium to high risk due to invasive procedures (e.g., stent placement, embolization).	Class IIb	Yes	Yes	Yes	Yes	Medium-Acuity Inpatient	Invasive / Surgical	No Redundancy	14	4	High Risk
Angiography	Imaging of blood vessels using contrast dye and X-rays.	Emergency / Trauma Angiography	Often critical risk because of urgent, life-saving interventions in unstable patients.	Class IIb	Yes	Yes	Yes	Yes	High-Acuity / Critical Care	Invasive / Surgical	No Redundancy	16	5	Severe (Highest) Risk
Central Stations	Centralized hubs aggregating patient data from multiple monitors.	ICU / High-Acuity Monitoring	Used in critical care settings (ICUs, CCUs) to aggregate and display multiple vital signs from highly acute patients (e.g. invasive blood pressure, advanced respiratory parameters).	Class IIb	Yes	Yes	Yes	Yes	High-Acuity / Critical Care	Non-Invasive	Partial Redundancy	15	4	High Risk
Central Stations	Centralized hubs aggregating patient data from multiple monitors.	Telemetry / Cardiac Monitoring	Primarily focused on continuous cardiac telemetry (ECG) for patients needing real-time rhythm surveillance.	Class IIb	Yes	Yes	Yes	Yes	Medium-Acuity Inpatient	Non-Invasive	Partial Redundancy	14	4	High Risk
Central Stations	Centralized hubs aggregating patient data from multiple monitors.	General Ward / Multi-Parameter Monitoring	Central station used in lower-acuity or general ward environments for basic vital signs (e.g., heart rate, SpO_2, blood pressure) from multiple bedside monitors.	Class IIa	Yes	Yes	Yes	Yes	Medium-Acuity Inpatient	Non-Invasive	Partial Redundancy	12	4	Moderate Risk

Mapping tenders to frameworks

- Other tenders
- Review with suppliers
- Publication towards community



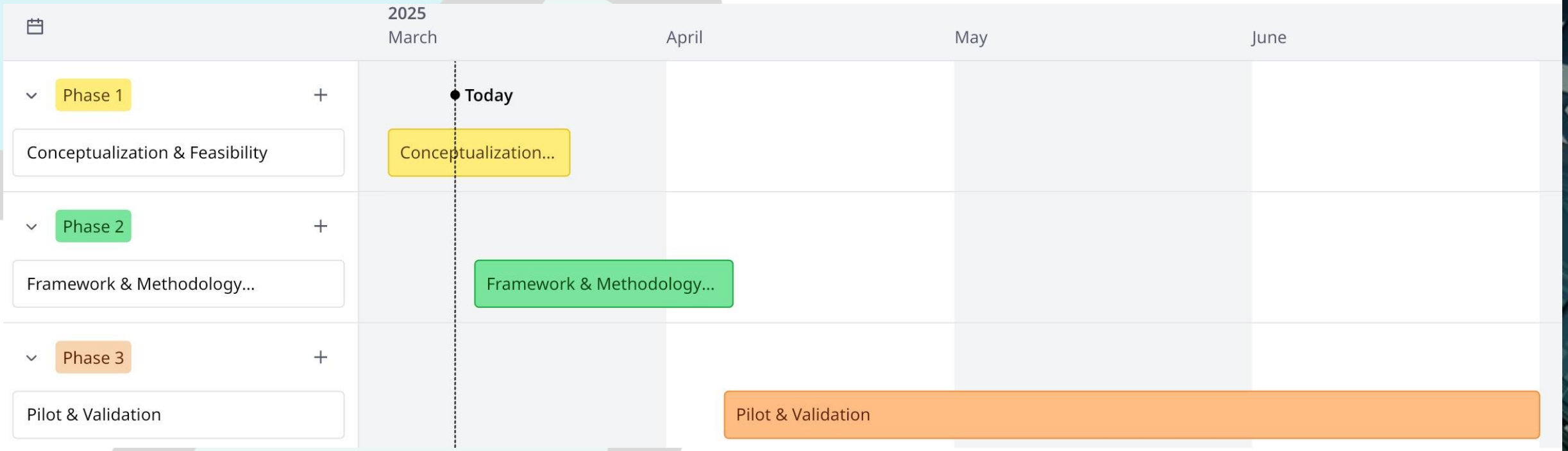
Suppliers or vendor risk management / evaluation

- Evaluation of categories
- Expand risk evaluation
- Define based categories an approach
  - For example: Critical supplier (Based on MDR category) -> Questionaire and interview
- Provide risk estimation per supplier

Suppliers or vendor risk management / evaluation

- Risk evaluation (per category)
  - Current version
    - Supporting care information
    - Ordinary personal data
    - Special personal data
    - Decisive care information
  - New version
    - Clinical environment
      - Critical care / Medium – acuity inpatient / Outpatient / Diagnostic
    - Invasiveness
      - Non-Invasive / Minimally invasive / Invasive or Surgical
    - Fallback / Redundancy
    - Concluse on risk score (calculation)
    - Risk interpretation (classes)

Suppliers or vendor risk management / evaluation



Note: timeline is still under review


Q
A

THANK YOU!

Robert Dirks
robert.dirks@shield-vzw.be
+32 491 34 79 14