**📘 Summary: 03 Core Functions**

**1. Cybersecurity Operating Model**

* Two core areas:
  + **Operational**: Daily security service delivery
  + **Non-operational**: Capability development, training, risk management
* **Governance oversight**: Ensures business alignment
* HR & Facility Security often managed **separately**

**2. Cybersecurity Function: Security Architecture**

* Defines and develops security capabilities.
* **Key Components**:
  + Security principles & frameworks
  + Design patterns
  + Security maturity and blueprints
* **Processes**:
  + Assess and develop capabilities
  + Advise architecture boards
  + Create security roadmaps
  + Integrate with cloud & on-prem environments

**3. Cybersecurity Function: Security Strategy & Implementation**

* Ensures alignment of strategy and operational execution.
* **Focus Areas**:
  + Resilience
  + Maturity models
  + Risk, project, and financial management
* **Processes**:
  + Run security maturity assessments
  + Develop improvement programs
  + Update policies and run awareness training
  + Support compliance and audits

**4. Cybersecurity Function: HR, Facility & Physical Security**

* Ensures **safety of people and work environments.**
* Covers:
  + Hiring, discipline, secure areas, H&S
* **Processes**:
  + Background checks
  + On/Offboarding
  + Implement physical controls
  + Manage breaches and liaise with authorities

**5. Cybersecurity Function: Governance, Strategy & Risk Alignment**

* Aligns security efforts with business expectations.
* **Focus Areas**:
  + Operational risks, audit, capability gaps
  + Investment priorities, escalation paths
* **Processes**:
  + Run governance bodies
  + Define KPIs
  + Document outcomes
  + Approve strategy and finances

**6. Cybersecurity Challenges**

* **Evolving Threat Landscape**:
  + - * + Constant new threats
* **Technological Evolution**:
  + - * + On-prem to cloud
* **Regulatory Changes**:
  + - * + Dynamic compliance requirements
* **Organisational Change**:
  + - * + Increased agility needed
* **Emerging Security Concepts**:
  + - * + Need for continuous learning

**7. Core Security Operations Functions**

Includes both strategic and operational areas:

* **Governance & Risk**
* **Architecture**
* **Strategy & Implementation**
* **Policies & Standards**
* **Awareness & Training**
* **Network, Infrastructure & Application Security**
* **TVM**
* **Security Monitoring & Incident Response**
* **IAM**
* **Physical & Human Security**
* **Planning & Improvement**

**8. Security Operations Org Chart**

* **CISO** **leads**
  + Security Operations Lead
    - Security Engineering
    - Monitoring
    - Incident Response
    - TVM
    - IAM
    - Architecture
    - Strategy & Implementation

**9. Security Engineering – Framework Mappings**

**NIST CSF**

* Protect: Hardening, DLP, PKI, PAM
* Detect: IDS, EDR
* Respond: IR support
* Recover: Reconfiguration

**ISO 27001 Alignment**

* Covers access control, cryptography, operations, incident management, and compliance

**MITRE ATT&CK Alignment**

* Activities tied to TTPs like proxy bypass, endpoint attacks, credential access, etc.

**10. Security Engineering Function**

* Cross-functional enabler that supports all security domains.
* **Key Concerns:**
* Infrastructure, Network, Data Security, IAM
* **Key Activities and Outputs:**
* **Infrastructure**:
  + OS hardening
  + EDR deployment
  + Secure mobile configs
* **Network**:
  + Firewall/proxy rules
  + IDS/IPS configurations
* **Data**:
  + Removable media control
  + DLP & PKI setup
* **IAM**:
  + Directory & federation setup
  + Privileged Access Management (PAM)