Security Management Model

Cyber Security

- 24x7 Security Operations Center (SOC) – SIEM, XDR, SOAR
  - Detection & Analysis
  - Incident Response & Recovery
  - Major Incident Management (MIM)
- Cyber Threat Intelligence (CTI)
  - Open Source Intelligence (OSINT)
  - CTI Vendors
  - Internal Source
  - Indicators of Compromise (IoC)
  - Tactics Techniques and Procedures (TTP)
  - Advanced Persistent Threats (APT)
- Offensive Cyber Defense
  - Red Teaming/Purple Teaming/Pentest/ Ethical Hacking
  - Honeypots
  - Attack Vectors and Counter Measures
- Vulnerability Management
  - Vulnerability Scanning
  - Vulnerability Assessment (CVE)
  - Risk based Prioritisation
  - Remediation Plan
  - Risk based Patching, Hotfix, Periodic system reboot
  - Rescan to validate, Ongoing Monitoring
- Identity and Access Management (IAM)
  - Previlige Access Management
  - Password Policy and Enforcement
  - Quarterly Access Revalidation
- BAU Security Operations
  - RCA/Problem Management
  - Change Management
  - Capacity Management
  - Release Management
  - EOS/EOL Management
- Security Design, Build, Transition, Retire
  - Security Design & Building
  - Project Implementation
  - Security Service Onboarding
  - Secure Decommission & Disposal
- Application Security
  - DevSecOps
  - Application Security Testing (Static, Dynamic, Automated, Manual)
  - API Security
  - DDoS Protection
  - Web Application Firewall (WAF)
  - Application Whitelisting
- Network Security
  - Firewall
    - Intrusion Prevention System (IPS), Intrusion Detection System (IDS)
    - Physical & Virtual Firewall
  - Routers, Switches, Loadbalancer Security
  - Wireless Security
    - Wifi Intrusion Prevention System
    - Bluetooth
  - Data Loss Prevention (DLP)
  - Zero Trust Network Access (ZTNA)
  - Micro-Segmentation
- Cloud & Infrastructure Security
  - DMZ Architecture
  - Backup & Restoration
  - Cloud Security Controls
  - Cloud Access Security Broker (CASB)
  - Next-Generation Secure Web Gateway (NG SWG)
- End Point Security
  - Email Security
  - Browser Isolation
  - Anti-virus
  - Remote Access, Virtual Private Network (VPN)
  - Device Management
    - Bring Your Own Device (BYOD)
    - Mobile Device Security
    - Device Encryption
- Security Log Management

Governance Risk Compliance (GRC), Audit

- Strategic Plaanning
  - Strategic Priorities
  - Security Policy
- Stakeholder Management
  - Stakeholder Heatmap
  - RACI
  - Escalation Matrix
- SLA and KPI Management
- Risk Management
  - Business Risk
  - Operational Risk
- Compliance Management
  - Hardening Standards
  - Secure Software Development Framework (SSDF)
  - Compliance Gap assessment and Remediation
  - Compliance Reporting
- Reporting and Communication
  - Communication Plan
  - Daily, Weekly, Monthly, Quarterly meeting
  - Periodic Reports
  - Ad hoc Reports & Meeting
- Audit Management
  - Internal Review & Audit
  - External, Regulatory, Compliance Audit
  - Audit Gap and Remediation
- Issue Management
  - Service Improvement Plan (SIP)
  - Back to Green Plan
- Resiliency, Business Continuity Plan (BCP)
  - Annual DR Drill
  - Table Top Drill
- Vendor Management

Physical Security

- 24x7 Physical Security Monitoring
- Physical Media Management
- Physical Device Security
- Perimeter Security
- Access Control
- Natural Disaster
- Manmade Disaster
- IOT, OT Security

Third Party Security

- Third Party Security Assessment (TPSA)
- Gap Analysis and Remediation

Human Resource Security

- Screening & Onboarding
- Security Awareness & Training
- Offboarding
- Defense against Social Engineering

People Process Technology

- People Management
  - Onboarding and Offboarding
  - Skill Gap assessment, Training, and Career Planning
  - Attrition and Knowledge Management
  - Work Shift Management, Team Building, Team Motivation
  - Agile Squad, Social Contract, Daily Standup
- Process and Documentation
  - Standard Operating Procedures (SOP)
  - Architecture and Technical documents
  - Process Owner, Document Owner
  - Periodic Review and Sign Off
  - Artifacts/Documents Secure Storage & Management
- Asset & Inventory Management
  - Hardware Assets
  - Software Assets
  - Third Party Vendor Products
- Automation and Continous Improvement

Finance Management

- Budget Management
  - Budget Forecast & Planning
  - Return on Investment (RoI) & Business Justification
- Cost Management
  - Labor Cost
  - Hardware Cost
  - Software Cost
  - 3rd Party Vendor Cost
  - Rated Services Cost
  - Capex Spending
  - SLA Penalty
- Manage Plan Vs Actual