

Security Operations

Threat Prevention

- Network/Application Firewall
- Vulnerability Management
- Application Security
- Information Security Policy
- DLP
- Anti Malware, Anti-spam
- Proxy/Content Filtering
- Patching
- DDoS Protection
- Hardening Guidelines
- Desktop Security
- Transport Layer Security
- Public Key Infrastructure

Incident Management

- Incident Response
- Media Relations
- Incident Readiness
- Forensic Investigation
- Data Breach Preparation

Threat Detection

- Log Analysis/correlation/ SIEM
- Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
- NetFlow Analysis
- DLP
- Threat hunting
- MSSP Integrations
- SOC Operations

Selling InfoSec (Internal)

- Aligning with Corporate Objectives
- Continuous Management Updates
- Innovation and Value Creation

Project Delivery Lifecycle

- Security Testing
- Requirements
- Design
- Certification and Accreditation

Budget

- Security Projects
- Business Case Development
- Alignment with IT Project
- FTE and Contractors
- Balancing Budget for People, Trainings, Tools/Technology

Security Architecture

- Network Segmentation
- Application Protection
- Defense-in-depth
- Remote Access
- Encryption Technologies
- Backup/Replication/Multiple Sites
- Cloud/Hybrid/Multiple Cloud Vendors

Legal & Human Resources

- Data Discovery
- Vendor Contracts
- Investigations/Forensics

Compliance and Audits

- GDPR
- PCI DSS
- ISO 27001
- HIPAA
- SOC 2
- Other Compliance Needs

Business Enablement

Mobile Technology

- Policy
- Technology
- Lost/Stolen Devices
- BYOD
- Mobile Apps Inventory

Cloud Computing

- Cloud Architecture
- Strategy and Guidelines
- Cloud Risk Evaluation
- Compliance
- Ownership/Liability/Incidents
- SaaS Strategy
- Log Integration

Merger/ Acquisition

- Acquisition Risk Management
- Integration Cost
- Identity Management

Governance

- Strategy and Business Alignment
- Risk Management Framework
- Resource Management
- Roles and Responsibilities
- Metrics and Reporting

Identity Management

- Credentialing
- Account Creation/Deletions
- Single Sign On
- Repository (LDAP/Active Directory)
- 2-Factor Authentication
- Role-Based Access Control
- Ecommerce and Mobile Apps
- Password resets
- HR Progress Integration
- Integration Cloud Based Identities

Risk Management

- Physical Security
- Vulnerability Management
- Ongoing Risk Assessments
- Integration to Project Delivery
- Code Reviews
- Risk Assessment Methodology
- Policies and Procedures
- Associate Awareness
- IoT Technologies
- Operational Technologies

