Strategy, Leadership & Governance

Information security Governance Body
- Terms of Reference
- Ensuring relevance of content
- Member engagement

Organisation Design
- Operating model
- Roles & Responsibilities
- Org design
- Team cohesion
- Org change management
- Talent sourcing
- Talent development:
  - Cyber apprenticeships
  - Team development
  - Succession planning

Strategy & Business Alignment
- Maturity assessments & Benchmarking
- Security strategy definition & articulation
- Security programme:
  - Tactical quick wins
  - Long term roadmap

Metrics & Reporting
- Operational & Exec metrics
- Key Risk Indicators
- Validation of metric effectiveness

Stakeholder Relationships
- Alignment with corporate strategy
- Updates: leadership & staff
- Conflict management
- Innovation, value creation
- Expectations management
- Coordination with others: CSO, CRO, DPO, General Counsel

Finance
- Business case & ROI
- Alignment with wider portfolio
- Budgeting & tracking

Securing The Business

On-Boarding & termination
- Staff
- Business Partners / Clients
- Suppliers

Securing New Business Initiatives
- Identification of new initiatives
- Engagement with new initiatives

Business Continuity Planning
- Security of BC Plans
- Cyber attack scenario planning

Employee Behaviour
- Employee awareness / risk culture:
  - Awareness & training
  - Phishing simulation tests
- Investigations & forensics

Mergers & Acquisitions
- Risk management: before, during & after acquisition
- Integration of acquired targets
  - Identity integration
  - Technology integration

Security Operations

SOC Design - Outsourced / MSSP / Co-Sourced
- Knowledge transfer
- Resource commitments
- Metrics & KPIs
- Supplier management

SOC Design - In-House
- Recruitment
- Development, retention & promotion
- Knowledge retention
- Team & shift management
- Continuous training

Vulnerability Management
- Identification:
  - Scoping & Asset discovery
  - Supplier liability & operational risk of scanning
- Remediation:
  - Approach to fixing vulnerabilities
  - Verification
- Metrics & baselines

Threat Management
- Alerting from security tools
- Log analysis, correlation, SIEM Netflow analysis
- Open Source & commercial threat feeds
- Threat hunting: automated & manual
- DNS, Social Media & Dark Web

SOC Operations
- SOC Procedures & Runbooks
- Metrics & KPI reporting
- SOC / NOC / Svc Desk integration
- Partnerships with Info Sharing & Analysis Centres
- DR exercises

Security Platform Operations
- Platform lock-down, operations & monitoring
- Technology upgrades

Incident Management
- Participation of all stakeholders:
  - Exec Board
  - IT, HR, Legal, Comms / Marketing / Media Relations
  - Clients / Customers, Suppliers
- Incident process
  - Runbooks for critical incident types: ransomware & customer-facing breaches
  - Incident testing
  - Crisis plan: cyber-attack scenario
  - Security Orchestration/SOAR
  - Managed Detection & Response / MDR
- Integration with related plans
  - Crisis plan
  - Personal Data Breach plan
  - Business Continuity Plan
- Forensics & 24x7 support

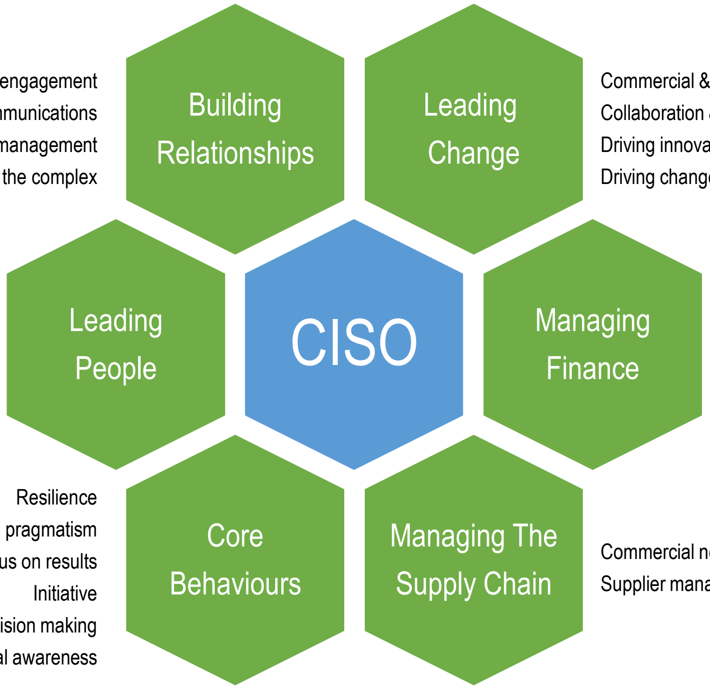
Risk & Controls

Risk management framework
- Control frameworks:
  - COSO/SOX
  - COBIT
  - ISO27000
  - NIST, FAIR, CIS
- Control assurance
  - Management risk & control reviews & reporting
  - Internal & External Audit

Cyber Risk Insurance
- Broker & underwriter engagement
- Covered scenarios
- Limits & Self-insured retentions
- Pre-Breach risk & control maturity assessments
- Post Breach engagement

Risk assessment, treatment & acceptance
- Risk assessment plan
- Risk ownership & governance
- Risk articulation & management review
- Risk acceptance processes

Continuous Improvement:
- Security health checks:
  - Testing
  - Tech risk landscape
  - Remediation roadmaps
- Incident readiness assessments
- IT Controls assessments
- Penetration tests
- Threat detection capability assessments
- Prioritised remediation planning



Stakeholder engagement
Stakeholder communications
Conflict management
Simplify the complex

Commercial & strategic focus
Collaboration & influencing
Driving innovation
Driving change

Inspiring leadership
Org design
Team management
Talent development
Driving behavioural change
Engaging comms

Budgeting
Business case

Resilience
Flexibility & pragmatism
Focus on results
Initiative
Difficult decision making
Cultural awareness

Commercial negotiations
Supplier management

Legal & Compliance

Compliance Assurance
- External assurance: ISAE3402 / SSAE18 / SOC1 / SOC2
- Internal assurance:
  - Internal Management Review
  - Internal Audit

Externally-imposed Compliance Requirements
- NIST / FISMA / HIPAA / HITECH
- China CSL
- PCI
- Sarbanes Oxley
- Data Protection Regulations
- Government Certifications:
  - Privacy Shield
  - Cyber Essentials +

E- Discovery & Legal Hold
- Preparation of data repositories for e-discovery
- Enforcement of Legal Hold

Internal Compliance Requirements
- Security policies & standards
- Project NFRs
- Publication & awareness
- Supply chain compliance

Data Retention & Destruction
- Data retention policies
- Retention schedules
- Enforcement within business functions

Securing New Initiatives

Integrating Security & Risk in SDLC / PMO
- Waterfall, Agile & DevOps

Design
- Secure coding training & review
- App development standards
- Security requirements & NFRs

Security Testing & Assurance
- Code reviews
- App vulnerability testing
- Penetration tests
- Continuous assurance
- Certification & accreditation requirements

Securing The Supply Chain

Pre-Contract Due Diligence
- Self-assessment
- Audits
- Independent assurance

Contracts
- New contracts
- Contract renewals

Reviews & Assurance
- Self-assessment
- Audits:
  - Right to Audit & remediation
- Independent assurance

Securing The Technology

Infrastructure & Server OS security
- Service Continuity & Disaster Recovery
- Hardening
- Patching
- Anti-Malware & APT protection
- Backups, replication, multiple sites
- HIPS
- Security monitoring

Application security
- Data access governance:
  - Information ownership & custodianship
  - Application access controls
  - Role-Based Access Controls
- Security monitoring
- File integrity monitoring

Identity & access
- Credential & password management:
  - Password strength / complexity
  - Password self-service resets
  - Multi-Factor Authentication
- Starters, movers, leavers:
  - Account creation & approvals
  - Account reviews
  - Account removal
  - HR process integration
- Single sign-On
- IAM SaaS solutions
- IAM Data Analytics
- Identity repository & federation
- Mobile app access control
- IOT device identities

Network security
- DDOS protection
- Firewalls, IDS, IPS
- Secure remote access
- Proxy / Content Filtering
- Secure Wireless Networks
- Network function virtualisation & SD WAN

BYOD Security
- Policy considerations:
  - Commercial opportunities
  - Personal data privacy
  - HR, financial & tax
  - Data security
- Policy enforcement

Innovation - Exploiting Emerging Tech
- AI, ML & Robotics
- Crypto currencies
- Blockchain
- 5G
- Drones
- VR & AR
- Wearables
- Autonomous vehicles

Physical security
- Landlord services
- Physical access control & monitoring
- Intrusion detection & response
- Theft prevention
- Environmental controls/ Power & HVAC
- Fire detection & suppression
- Redundancy
- BCP / Work Area Recovery sites

Cloud security
- SaaS Strategy:
  - Governance & compliance enforcement
  - Cloud specific DR & BCP
  - Supplier risks
  - SLAs & performance mgt
  - Data ownership, liability, incidents, privacy compliance
  - Security assurance
  - Mgt of Shadow IT
- Cloud security controls:
  - Cloud security architecture
  - Cloud identity / CASB
  - Virtual Machine security
  - Virtualised security appliances / Cloud-to-Cloud integration
  - Monitoring/log integration
- Access to corp data from non-corp devices

Email security
- Anti-Spam control
- Phishing & impersonation protections
- Email encryption

Endpoint Security
- Hardening
- Patching / software updates
- Anti-Malware
- HIPS / EDR
- Security monitoring / UBA
- Encryption
- PIN / password enforcement
- Apps inventory & deployment control
- Containerisation / data segregation
- Lost/stolen devices
- Cloud storage of data
- Device tracking

Data security
- Data & process mapping
- Data analytics security
- Encryption & masking:
  - PKI
  - Encryption at rest
  - Encryption in transit
- Business partner access:
  - Access approval
  - Access reviews
  - Access removal
  - Identity federation & access automation
- Data Loss Prevention:
  - DLP & Data classification policy
  - Data loss channels
  - DLP enforcement technologies

IOT / Operational Technology security
- IOT Risks:
  - Connected office devices
  - Connected medical devices
  - At home
  - Planes, trains & automobiles
  - Industrial control systems, SCADA, PLCs, HMIs
- IOT Security:
  - IOT Frameworks
  - Vulnerability mgt
  - Comms protocols
  - Device authentication & integrity
  - Network segregation
  - Device protection
  - Over The Air updates

Based on
http://rafeeqrehman.com