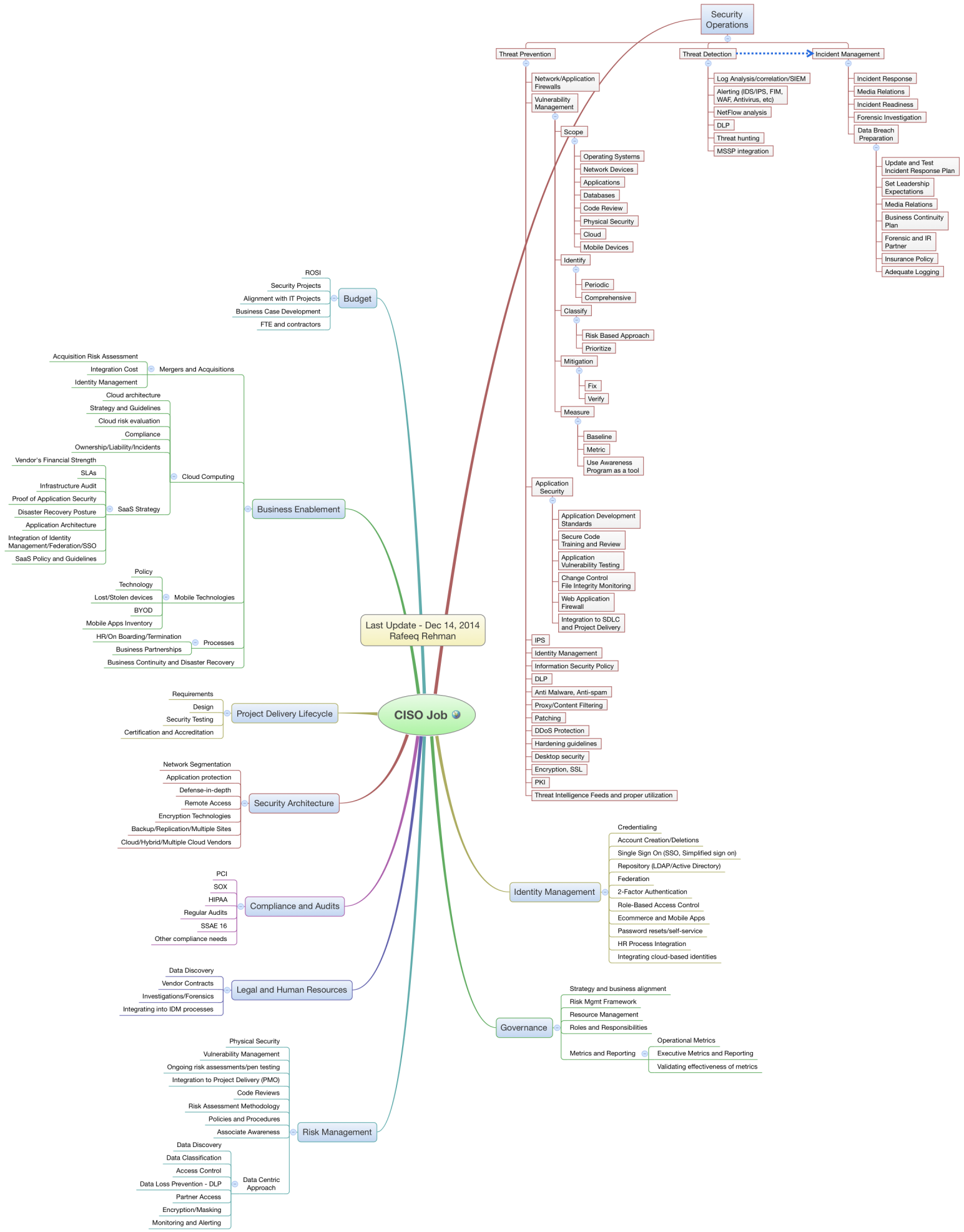
Last Update - Dec 14, 2014
Rafeeq Rehman
CISO Job
Security Operations
Threat Prevention
Threat Detection
Incident Management
Network/Application Firewalls
Vulnerability Management
Scope
Operating Systems
Network Devices
Applications
Databases
Code Review
Physical Security
Cloud
Mobile Devices
Identify
Periodic
Comprehensive
Classify
Risk Based Approach
Prioritize
Mitigation
Fix
Verify
Measure
Baseline
Metric
Use Awareness Program as a tool
Application Security
Application Development Standards
Secure Code Training and Review
Application Vulnerability Testing
Change Control File Integrity Monitoring
Web Application Firewall
Integration to SDLC and Project Delivery
IPS
Identity Management
Information Security Policy
DLP
Anti Malware, Anti-spam
Proxy/Content Filtering
Patching
DDoS Protection
Hardening guidelines
Desktop security
Encryption, SSL
PKI
Threat Intelligence Feeds and proper utilization
Log Analysis/correlation/SIEM
Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
NetFlow analysis
DLP
Threat hunting
MSSP integration
Incident Response
Media Relations
Incident Readiness
Forensic Investigation
Data Breach Preparation
Update and Test Incident Response Plan
Set Leadership Expectations
Media Relations
Business Continuity Plan
Forensic and IR Partner
Insurance Policy
Adequate Logging
Budget
ROSI
Security Projects
Alignment with IT Projects
Business Case Development
FTE and contractors
Business Enablement
Mergers and Acquisitions
Acquisition Risk Assessment
Integration Cost
Identity Management
Cloud Computing
Cloud architecture
Strategy and Guidelines
Cloud risk evaluation
Compliance
Ownership/Liability/Incidents
SaaS Strategy
Vendor's Financial Strength
SLAs
Infrastructure Audit
Proof of Application Security
Disaster Recovery Posture
Application Architecture
Integration of Identity Management/Federation/SSO
SaaS Policy and Guidelines
Mobile Technologies
Policy
Technology
Lost/Stolen devices
BYOD
Mobile Apps Inventory
Processes
HR/On Boarding/Termination
Business Partnerships
Business Continuity and Disaster Recovery
Project Delivery Lifecycle
Requirements
Design
Security Testing
Certification and Accreditation
Security Architecture
Network Segmentation
Application protection
Defense-in-depth
Remote Access
Encryption Technologies
Backup/Replication/Multiple Sites
Cloud/Hybrid/Multiple Cloud Vendors
Compliance and Audits
PCI
SOX
HIPAA
Regular Audits
SSAE 16
Other compliance needs
Legal and Human Resources
Data Discovery
Vendor Contracts
Investigations/Forensics
Integrating into IDM processes
Risk Management
Physical Security
Vulnerability Management
Ongoing risk assessments/pen testing
Integration to Project Delivery (PMO)
Code Reviews
Risk Assessment Methodology
Policies and Procedures
Associate Awareness
Data Centric Approach
Data Discovery
Data Classification
Access Control
Data Loss Prevention - DLP
Partner Access
Encryption/Masking
Monitoring and Alerting
Governance
Strategy and business alignment
Risk Mgmt Framework
Resource Management
Roles and Responsibilities
Metrics and Reporting
Operational Metrics
Executive Metrics and Reporting
Validating effectiveness of metrics
Identity Management
Credentialing
Account Creation/Deletions
Single Sign On (SSO, Simplified sign on)
Repository (LDAP/Active Directory)
Federation
2-Factor Authentication
Role-Based Access Control
Ecommerce and Mobile Apps
Password resets/self-service
HR Process Integration
Integrating cloud-based identities