

Business Operation Support Services (BOSS)

| Compliance | |
|----------------------------------|---------------------------------|
| Audit Planning | Contract Authority Maintenance |
| Independent Audits | Third-Party Audits |
| Internal Audits | Info. System Regulatory Mapping |
| Intellectual Property Protection | |

| Operational Risk Management | |
|-----------------------------|----------------------|
| Operational Risk Committee | Crisis Management |
| Business Impact Analysis | Key Risk Indicator |
| Business Continuity | |
| Planning | Testing |
| Risk Management Framework | |
| Business Assessment | Technical Assessment |
| Independent Risk Management | |

| Human Resources Security | |
|----------------------------|-----------------------|
| Employee Termination | Employment Agreements |
| Background Screening | Job Description |
| Roles and Responsibilities | Employee Awareness |
| Employee Code of Conduct | |

| Data Governance | |
|----------------------------|---|
| Data Owner/ Stewardship | Data Classification |
| Handling/Labeling/Security | Secure Disposal of Data |
| Clear Desk Policy | Rules for Information Leakage Preventions |
| Rules for Data Retention | |

| Security Monitoring Services | |
|---------------------------------------|------------------------------------|
| SIEM Platform | Event Mining |
| Database Monitoring | Application Monitoring |
| Honey Pot | End Point Monitoring |
| Event Correlation | Cloud Monitoring |
| E-mailing Journaling | Market Threat Intelligence |
| Counter Threat Management | SOC Portal |
| Managed Security Services | Knowledge Base |
| Branding Protection | Anti-Phishing |
| Real-time internetwork defense (SCAP) | User Behavior and Profile Patterns |

| Legal Services | |
|-------------------------------------|-------------|
| Contracts | E-Discovery |
| Incident Response Legal Preparation | |

| Internal Investigation | |
|------------------------|-------------------|
| Forensic Analysis | E-mail Journaling |

Information Technology Operations & Support (ITOS)

| IT Operation | | |
|---------------------------|----------------------|--------------------|
| Disaster Recovery Plan | | |
| Plan Management | Test Management | |
| IT Governance | | |
| Architecture & Governance | Standards & Guidance | |
| Resource Management | | |
| Segregation of Duties | Contractors | |
| PMO | | |
| Program Management | Project Management | Remediation |
| Portfolio Management | | |
| Maturity Model | Roadmap | Strategy Alignment |

| Service Delivery | | |
|------------------------------------|-----------------------|-------------------|
| Service Level Management | | |
| Objectives | Internal SLAs | OLAs |
| External SLAs | Vector Management | Service Dashboard |
| Information Technology Resiliency | | |
| Availability Management | Resiliency Analysis | Capacity Planning |
| Application Performance Monitoring | | |
| Asset Management | | |
| Service Costing | Operational Budgeting | |
| Charge Back | Investment Budgeting | |

| Service Support | | |
|---------------------------|--------------------------|---------------------|
| Configuration Management | | |
| Capacity Building | Software Management | Physical Inventory |
| Automated Asset Discovery | Configuration Management | |
| Knowledge Management | | |
| Best Practices | Trend Analysis | Benchmarking |
| Security Job Aids | Security FAQ | |
| Change Management | | |
| Service Provisioning | Approval Workflow | Change Review Board |
| Planned Changes | | |
| Project Changes | Operational Changes | |
| Emergency Changes | | |

| Incident Management | | |
|----------------------------|--|----------------|
| Security Incident Response | Automated Ticketing | Self-Service |
| Ticketing | Cross Cloud Security Incident Response | |
| Problem Management | | |
| Event Classification | Root Cause Analysis | Trend Analysis |
| Problem Resolution | Orphan Incident Management | |
| Release Management | | |
| Scheduling | Testing | Build |
| Version Control | Source Code Management | |

Technology Solution Services (TSS)

| Presentation Services | | | | |
|-----------------------------|------------------|------------------|----------------|--------|
| Presentation Modality | | | | |
| Consumer Service Platform | | | | |
| Social Media | Collaboration | Search | E-Readers | E-mail |
| Enterprise Service Platform | | | | |
| B2E | B2M | B2B | B2C | P2P |
| Speech Recognition (IVR) | | | | |
| Presentation Platform | | | | |
| End-Points | | | | |
| Mobile Devices | Portable Devices | Fixed Devices | | |
| Mobile Device Management | Medical Devices | | | |
| Desk Top | | Smart Appliances | | |
| Company Owned | Third-Party | Public Kiosk | Secure Sandbox | |
| Handwriting (ICR) | | | | |

| Application Services | | | | |
|----------------------------|------------------------------------|--------------------------------|--------------|-----------------|
| Programming Interfaces | | | | |
| Input Validation | Security Design Pattern | Security Application Framework | Code Samples | Attack Patterns |
| Intergration Middleware | | | | |
| Connectivity & Delivery | | | | |
| Abstraction | | | | |
| Development Process | | | | |
| Self-Service | | | | |
| Security Code Review | Application Vulnerability Scanning | Stress and Volume Testing | | |
| Software Quality Assurance | | | | |

| Information Services | | | | |
|----------------------|---------------------|------------------------------|------------------|----------------|
| Service Delivery | | | | |
| Service Catalog | SLAs | OLAs | Contracts | Recovery Plans |
| Reporting Services | | | | |
| Dashboards | Data Mining | Business Intelligence | Reporting Tools | |
| Data Governance | | | | |
| Risk Assessments | Non-production Data | Information Leakage Metadata | Data Segregation | |

| BOSS | | |
|------------------|-----------------------------------|---------------------------------------|
| Risk Assessments | Data Classification | Process Ownership |
| Audit Findings | HR Data (Employees & Contractors) | Business Strategy |
| Risk Management | | |
| GRC | RA | BIA |
| DR & BC Plans | VRA | TVM (Threat Vulnerability Management) |

| Service Support | | | | |
|--------------------------------|-------------------|-----------------------------------|-------------------------|--------------------|
| Configuration Rules (Metadata) | Service Events | Configuration Management Database | | |
| Knowledge Repository | | Change Logs | | |
| User Directory Service | | | | |
| Active Directory Services | Registry Services | LDAP Repositories | Location Services | X.500 Repositories |
| Federated Services | DBMS Repositories | Virtual Directory Services | Meta Directory Services | |

| Security Monitoring | | | | | | | |
|---------------------|----------------------|-----------------------|--------------------|----------------|-----------------|------------------------|-------------------------|
| Session Events | Authorization Events | Authentication Events | Application Events | Network Events | Computer Events | Privilege Usage Events | eDiscovery Events |
| DLP Events | NIPS Events | Compliance Monitoring | CRLs | ACLs | Database Events | HIDS-HIPS | Transformation Services |

Infrastructure Services

| Internal Infrastructure | | | |
|---------------------------------|------------------------------|--------------------------|-------------------------|
| Facility Security | | | |
| Controlled Physical Access | | | |
| Barriers | Electronic Surveillance | Security Patrols | Physical Authentication |
| Asset Handling | | | |
| Data | Storage | Hardware | |
| Environmental Risk Management | | | |
| Physical Security | Equipment Location | Power Redundancy | |
| Availability Services | | | |
| Patch Management | Servers | | |
| Compliance Monitoring | Service Discovery | Secure Build | Image Management |
| Equipment Maintenance | | | |
| Network Services | | | |
| Network Segmentation | Authoritative Time Source | | |
| Storage Services | | | |
| Virtual Infrastructure | | | |
| Desktop "Client" Virtualization | | | |
| Local | | | |
| Remote | | | |
| Session-based | VM-Based (VDI) | | |
| Application Virtualization | | | |
| Client Application Streaming | Server Application Streaming | | |
| Virtual Workspaces | | | |
| Vertical Isolation | | | |
| Server Virtualization | | | |
| Virtual Machines (Host Based) | | | |
| Full | Paravirtualization | Hardware-assisted | |
| OS Virtualization | TPM Virtualization | Virtual Memory | |
| Storage Virtualization | | | |
| Block-Based Virtualization | | | |
| Host-Based | | | |
| LDM | LVM | LUN | |
| Storage-Device Based | | | |
| Network-Based | | | |
| Appliance | Switched | | |
| File-Based Virtualization | | | |
| Network Virtualization | | | |
| Network Address Space | | | |
| IPv4 | IPv6 | | |
| External (VLAN) | Internal (VNIC) | | |
| Database Virtualization | Mobile Device Virtualization | Smartcard Virtualization | |

Lead Authors: Jon-Michael C. Brook, Michael Roza
Contributors: Shawn Harris, Sunil Shanthi, Michael Theriault, Rolando Marcelo Vallejos, Ashish Vashishtha, Suri Venkat, Henry Werchan
CSA Team: Sean Heide, Jim Reavis, AnnMarie Ulskey (Design), John Yeoh

Security and Risk Management

| Governance Risk & Compliance | | | |
|------------------------------|--------------------|--------------------------------|-----------------|
| Compliance Management | | Policy Management | |
| Vendor Management | | Exceptions | Self-Assessment |
| Audit Management | IT Risk Management | Technical Awareness & Training | |

| InfoSec Management | | | |
|--------------------|----------------|---------------------------|----------------|
| Capability Mapping | Maturity Model | Risk Portfolio Management | Risk Dashboard |
| | | Residual Risk Management | |

| Privilege Management Infrastructure | | | |
|-------------------------------------|---------------------------|-------------------------------------|------------------------|
| Identity Management | | | |
| Domain Unique Identifier | Federated IDM | Identity Provisioning | Attribute Provisioning |
| Authentication Services | | | |
| SAML Token | Risk Based Authentication | Multi Factor Authentication | OTP |
| Smart Card | Biometrics | Network Authentication | Single Sign On |
| Password Management | WS-Security | Middleware Authentication | Identity Verification |
| | | Out of the Box (OTB) Authentication | |

| Authorization Services | | | |
|-----------------------------|--------------------------|--------------------------------------|---------------------|
| Entitlement Review | Policy Enforcement | Policy Definition | Policy Management |
| Principal Data Management | Resource Data Management | XACML | Obligation |
| | | Out of the Box (OTB) Authorization | |
| Privilege Usage Management | | | |
| Keystroke / Session Logging | Password Vaulting | Privilege Usage Gateway | Resource Protection |
| | | Hypervisor Compliance and Governance | |

| Threat & Vulnerability Management | | |
|-----------------------------------|----------------|----------------------|
| Compliance Testing | | |
| Databases (DBs) | Servers | Networks |
| Vulnerability Management | | |
| Application | Infrastructure | DB |
| Penetration Testing | | Threat Management |
| Internal | External | Source Code Scanning |
| | | Risk Taxonomy |

| Infrastructure Protection Services | | | |
|-------------------------------------|---------------------|-----------------------------|-------------------------|
| Server | | | |
| Behavioral Malware Prevention | White Listing | Sensitive File Protection | |
| HIPS / HIDS | Anti-Virus | Host Firewall | |
| Endpoint | | | |
| Anti-Virus, Anti-Spam, Anti-Malware | HIPS / HIDS | Host Firewall | Media Lockdown |
| Behavioral Malware Prevention | Inventory Control | Content Filtering | Forensic Tools |
| | | White Listing | |
| Network | | | |
| Behavioral Malware Prevention | Firewall | Content Filtering | DPI |
| NIPS / NIDS | Wireless Protection | Link Layer Network Security | Black Listing Filtering |
| Application | | | |
| XML Appliance | Secure Messaging | Application Firewall | Secure Collaboration |
| | | Real Time Filtering | |

| Data Protection | | | |
|----------------------------|--------------------------------|------------------------|-----------------------|
| Data Life Cycle Management | | | |
| Meta Data Control | eSignature (Unstructured Data) | Data De-identification | Life Cycle Management |
| Data Masking | Data Obscuring | Data Tagging | Data Seeding |

| Data Loss Prevention | | | |
|----------------------|---------------------------|------------------------|-----------------------|
| Data Discovery | Network (Data in Transit) | Endpoint (Data in Use) | Server (Data at Rest) |

| Intellectual Property Protection | |
|----------------------------------|---------------------------|
| Intellectual Property | Digital Rights Management |

| Cryptographic Services | | |
|---------------------------------|--|--|
| Key Management | | PKI |
| Symmetric Keys | Asymmetric Keys | Signature Services |
| Data-in-Use Encryption (Memory) | Data-in-Transit Encryption (Transitory, Fixed) | Data-at-Rest Encryption (DB, File, SAN, Desktop, Mobile) |

| Policies & Standards | | | |
|--------------------------------|-----------------------------|---|-------------------------------|
| Operational Security Baselines | Job Aid Guidelines | Role Based Awareness | Information Security Policies |
| Technical Security Standards | Data / Asset Classification | Best Practices & Regulatory Correlation | |

