Asset Universe Sample:

- ✓ Customer Bill Payment (Consumer or Business)
- ✓ Customer Electronic Statements (Consumer or Business)
- ✓ Customer/Business Online Banking (? Name of Provider ?)
- ✓ Customer/Consumer Online Banking (? Name of provider ?)

Risk Universe Sample:

- ✓ Customer Error (Business or Consumer)
- ✓ Denial of Service Attack (DOS)
- ✓ Dormant User Accounts
- ✓ Employee Error Failure to properly identify customers
- ✓ Fraud - External Fraud
- ✓ Fraud - Internal Fraud
- ✓ Identity Theft
- ✓ Incomplete Data for Reporting/Decision Making
- ✓ Integrity of Information
- ✓ Malicious Activities External (not Fraud)
- ✓ Malicious Activity Internal (not Fraud)
- ✓ nonCompliance to Regulations (e.g. GLBA, BSA/AML etc..)
- ✓ Outside party lawsuit
- ✓ Phishing / Pharming / Vishing
- ✓ Remote Access
- ✓ Social Engineering Attacks
- ✓ System Reliability / Availability - Downtime
- ✓ Third Party Connectivity Lost (i.e. Service Provider)
- ✓ Turnover of Key Personnel (IT or others)
- ✓ Unauthorized Logical Access to Systems/Data
- ✓ Vendor Failure Web Site Defacement

Risk Universe Sample:

- ✓ Access Control - Access Enforcement
- ✓ Access Control – Account Management User Access
- ✓ Access Control - Account Management: Terminated
- ✓ Employee Process
- ✓ Access Control - Application Security Specifications
- ✓ Access Control - Authorized and Secure Remote Connection Controls (e.g. VPN, modem procedures)
- ✓ Access Control - Screen Saver / Automatic Logout
- ✓ Access Control - System Administration Level Restrictions Access Control
  - Use of encryption
- ✓ Access Control - User Access Rights Review (Network/Application) Application
- ✓ System Balancing
- ✓ Assess Risk - Human Firewall testing : Social Engineering
- ✓ Assess Risk - Periodically Scan for Rogue Wireless
- ✓ Assess Risk - Risk Assessment is Proactive and Effective

- ✓ Assess Risk - Technical Vulnerability Scanning (Internal/External)
- ✓ Assess Risk - Web Application Vulnerability Scanning
- ✓ Audit - Application User Activity Monitoring
- ✓ Audit - Intrusion Detection or Prevention System (IDS/IPS)
- ✓ Audit - IT controls testing, independent reviews
- ✓ Audit - Network User Activity (Log/Event Monitoring)
- ✓ Audit- Monitoring- Privileged Accounts System Administration
- ✓ Authentication - Account Login Restrictions, Password Content Authentication - Multi-factor (e.g. tokens, biometrics or similar for customers)
- ✓ Bonded or Similar Contracted Cleaning Service (e.g. employees)
- ✓ Business Continuity - Storage of Backup Media & Documentation Offsite Business Continuity and/or IT Disaster Recovery Plan Documentation Business Continuity and/or IT Disaster Recovery Plan Testing
- ✓ Change and Problem Management
- ✓ Compliance Department review
- ✓ Customer Awareness and Education
- ✓ Data Loss Prevention Solutions - DLP (monitoring, blocking)
- ✓ Data/Record Retention Policy - eDiscovery
- ✓ E-Mail Filter (incoming and outgoing)
- ✓ Employee Handbook Employee
- ✓ Personal Bank Account / Loan Review
- ✓ Employee Security Awareness Training Program
- ✓ Employee Training (i.e. procedures, software use, functionality and features)
- ✓ Employment Standards - Background / Credit Checks
- ✓ Firewall - Internet Perimeter
- ✓ Firewall - Personal Laptop/Desktop
- ✓ Incident Management: Preparedness and Response to Incidents
- ✓ Information Security Program Policy, Standards & Procedures
- ✓ IT Insurance Coverage
- ✓ IT Strategic Planning includes Security
- ✓ Strategy Malicious Code Protection - antivirus (? name solution ?) Management Oversight (i.e. Board of Directors, IT Committee)
- ✓ Media Handling - Shredding / Sanitation of Sensitive Information (Hard
- ✓ Copy & Electronic)
- ✓ Network Diagram
- ✓ Outsourcing to Third Party Patch Management
- ✓ Physical - Alternate Power Supply (UPS / Emergency Generator)
- ✓ Physical Security Environmental - Fire Suppression / Cooling / Water Sensors
- ✓ Physical Security General - Cameras / Locks / Zones of Access
- ✓ Physical Security Technical - Restricted and/or Monitored access to USB/Firewire/CD-DVDRW
- ✓ Purchase Approval Process
- ✓ Red Flags - Identity Theft - CIP
- ✓ Segregation of duties
- ✓ Spare Equipment
- ✓ Suspicious Activity Report (SAR)
- ✓ Reporting Systems Tracking of absenteeism by HR Vacation
- ✓ Policies Vendor Management Program - (Oversight and Due Diligence)
- ✓ Vendor Source Code in Escrow
- ✓ Web Site Content Controls & Monitoring