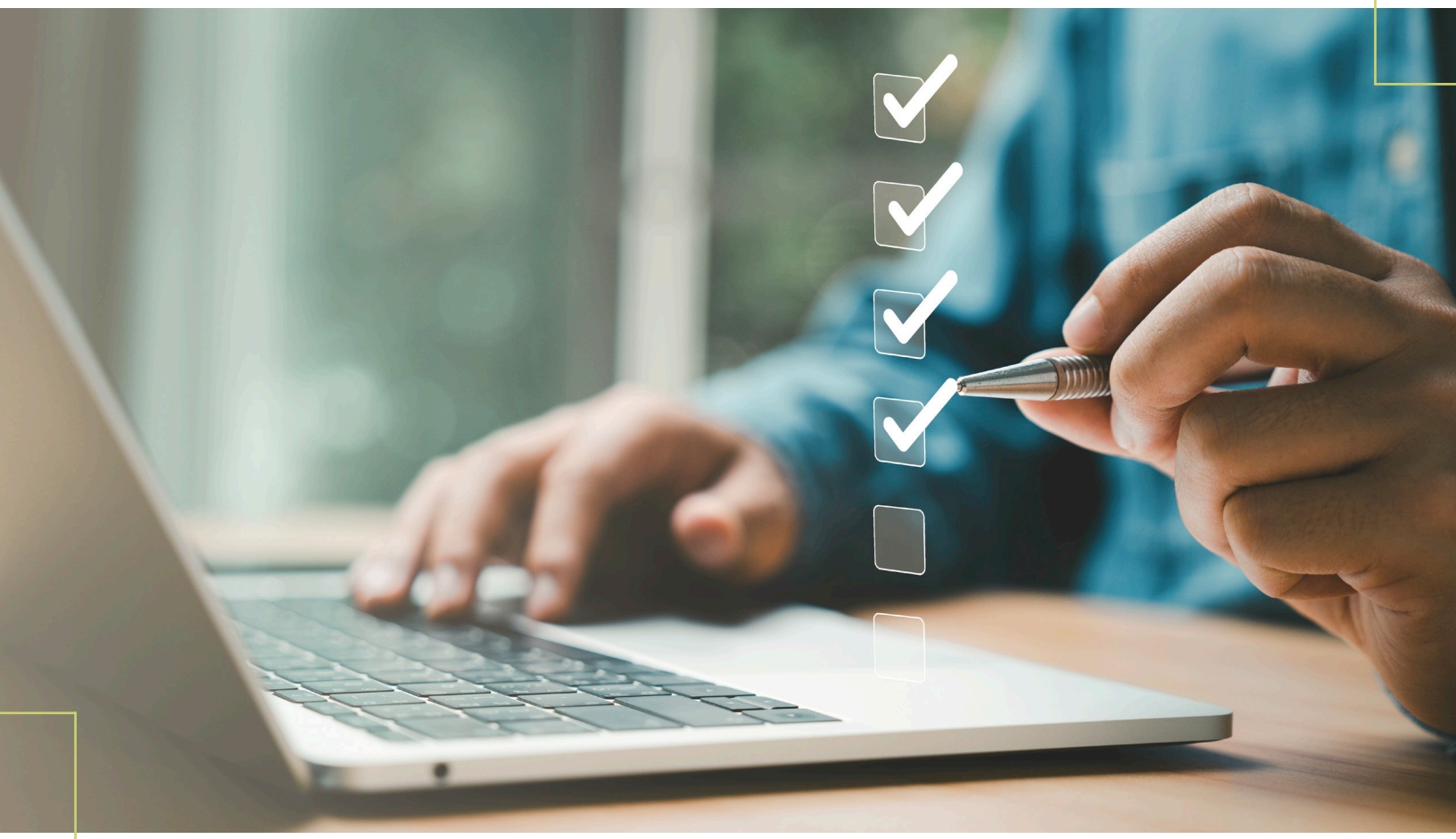
FDIC InTREx:

What Documentation Are You Expected to Have?



Written by: Jon Waldman, President, Partner, Co-Founder
SBS CyberSecurity, LLC

FDIC InTREx:

What Documentation Are You Expected to Have?

The FDIC rolled-out the Information Technology Risk Examination procedures (InTREx) in 2016 and updated the procedures in September 2023. These procedures are used by the FDIC, Federal Reserve, and State Examiners and make expectations regarding required documentation from financial institutions a bit clearer. The following is a list of documentation pulled from the InTREx procedures. We hope this helps you as you update your Information Security Program documentation and as you prepare for your next IT examination.

General Required Documentation:

Listed multiple times in InTREx

InTREx highlights a great deal of documentation in its four core modules, and even more in a few supplemental sections. The following is a list of documents that are mentioned multiple times throughout the examination procedures that all financial institutions should include in their Information Security Program documentation:

- **Most recent IT examination report(s) and work-papers**
- **Pre-examination memoranda and file correspondence**
- **Formal Information Security Program documentation, including:**
  - Information security controls, including cybersecurity
  - Network security controls, including intrusion detection
  - Acceptable use
  - User access rights management
  - Electronic funds transfer
  - Vendor management and third-party risk
  - Remote access
  - Bring your own device (BYOD)
  - Institution-issued mobile devices
  - Anti-virus/anti-malware
  - System configuration standards
  - Change/patch management
  - Physical and environmental security
  - Encryption
  - Unauthorized/unlicensed software
  - Information security training program, including both the staff and the board of directors
- **Incident response plan, including:**
  - Identifying and reporting incidents
  - Assessing the nature and scope of an incident
  - Incident escalation procedures
  - Identifying what customer information and information systems have been accessed or misused
  - Notifying primary federal regulator(s), law enforcement, and customers considering the Computer-Security Incident Notification Rule
  - Filing of a SAR
  - Incident response and recovery
  - Testing program, including results-tracking

- **Business continuity and disaster recovery plan(s), including:**
  - Enterprise-wide business continuity plan
  - Business impact analysis
  - Risk/threat assessment, including cyber risks/threats
  - Appropriate recovery operations
  - Pandemic preparedness
  - Testing program, including results-tracking
- **Vendor management program**
  - Vendor risk assessment
  - Acquisition of key vendors
  - Ongoing management of vendors (both foreign and domestic)
- **Most recent IT risk assessment**
  - IT asset inventory, including cloud-based and virtualized systems
  - Criticality of IT assets
  - Threats (including likelihood and impact)
  - Inherent risk level
  - Controls to reduce risk
  - Control testing
  - Residual risk level
  - Frequency of IT risk assessment
  - Acceptable levels of risk
  - Remediation of unacceptable risks
- **Most recent cybersecurity risk assessment**
- **Most recent internal and external IT audit reports**
- **Board and committee minutes related to the review of:**
  - IT-related committee meetings and decisions
  - Approval of Information Security Program and IT-related policies
  - IT and cybersecurity risk assessments
  - IT audits
  - Vendor management
  - Change/patch management, including major IT projects
  - Network security, including security or cyber incidents
- **Organizational charts that reflect:**
  - Business and IT structure
  - Audit reporting structure
- **Remediation and action tracking to demonstrate management responses to IT audit and examination recommendations and deficiencies**

Additional InTREx Required Documentation:

By Section

In addition to the documents listed multiple times throughout InTREx, the following are documents to be reviewed under each identified section:

Audit

- **IT audit policy and charter**
- **IT audit plan/schedule, including:**
  - Information security, including compliance with the Interagency Guidelines Establishing Information Security Standards
  - Cybersecurity
  - Network architecture, including firewalls and intrusion detection/prevention systems (IDS/IPS)
  - Incident response planning
  - Business continuity and disaster recovery planning
  - Security monitoring, including logging practices
  - Change and patch management
  - Third-party outsourcing
  - Social engineering
  - Electronic funds transfer
  - Electronic banking (all products, services, and channels), including mobile banking
- **Most recent IT audit risk assessment**

Management

- **IT governance**
  - Documentation regarding the committees, names, and titles of the individual(s) responsible for managing IT and information security
- **IT asset inventory**
- **IT-related committee minutes**
- **IT job descriptions, including qualifications of key IT employees**
- **Insurance policies (including cybersecurity insurance)**
- **Strategic plans (business and IT)**
- **Succession plans**
- **IT budgets**

Development and Acquisition

- **Change management policy and procedures, including:**
  - Request and approval
  - Testing
  - Implementation
  - Backup and back-out
  - Documentation
  - User notification and training
- **Project management policy and procedures**
- **System development life cycle process and procedures (if applicable)**
- **IT-related contracts and license agreements**

Support and Delivery

- **Business operations-related policies, including:**
  - Monitoring of systems for problems or capacity issues
  - Daily processing issue resolution and escalation procedures
  - Independent review of master file input and file maintenance changes
  - Independent review of global parameter changes
  - Document imaging and management systems
  - Item processing functions, including check imaging
- **Up-to-date network topology**
- **Information technology profile (InTREx)**
- **Most recent network vulnerability assessment and penetration testing reports**
- **Regulatory vendor reports (e.g., TSP reports)**

Other Requirements:

Additionally, InTREx mentions the following areas in two different "Expanded Analysis" sections – Management Expanded Analysis and Support and Delivery Expanded Analysis. Ensure these areas are appropriately addressed in your Information Security Program and IT-related documentation:

- **Cloud computing – update the following to include any cloud-based products, systems, or vendors:**
  - Information Security Program and IT-related policies
  - IT and cybersecurity risk assessments
  - Vendor management program
  - Incident response plan
  - Business continuity and disaster recovery plan
- **Managed Security Services Providers (MSSP)**
  - Type and frequency of security reports provided by MSSP
  - MSSP responsiveness to audit findings
  - Incident response capabilities
  - Service level agreements (SLA)
  - Business continuity and disaster recovery plan
  - Secure handling of sensitive data
  - In-house expertise to manage MSSP
- **Foreign-Based Technology Service Providers (FBTSP)**
  - Location of FBTSP and institution's data
  - Familiarity of FBSTP with US banking laws and regulations
  - Choice of governing law (US law is preferred)
  - Right of US regulators to audit
  - FBSTP's vendor management program
- **Wireless networks**
  - Guest wireless networks vs. corporate wireless networks
  - Security and access guidelines
  - Periodic network security testing
  - Management approval of the use of wireless networks
  - Adoption of appropriate policies and procedures governing wireless access
  - Approval of a minimum set of security requirements for wireless networks
  - Periodic security testing of wireless networks
  - Terms and conditions for guest use
- **Voice over IP (VoIP)**
  - Physical and logical security controls
  - Patch management
  - Network segmentation
  - Periodic network security testing
  - Emergency service communications

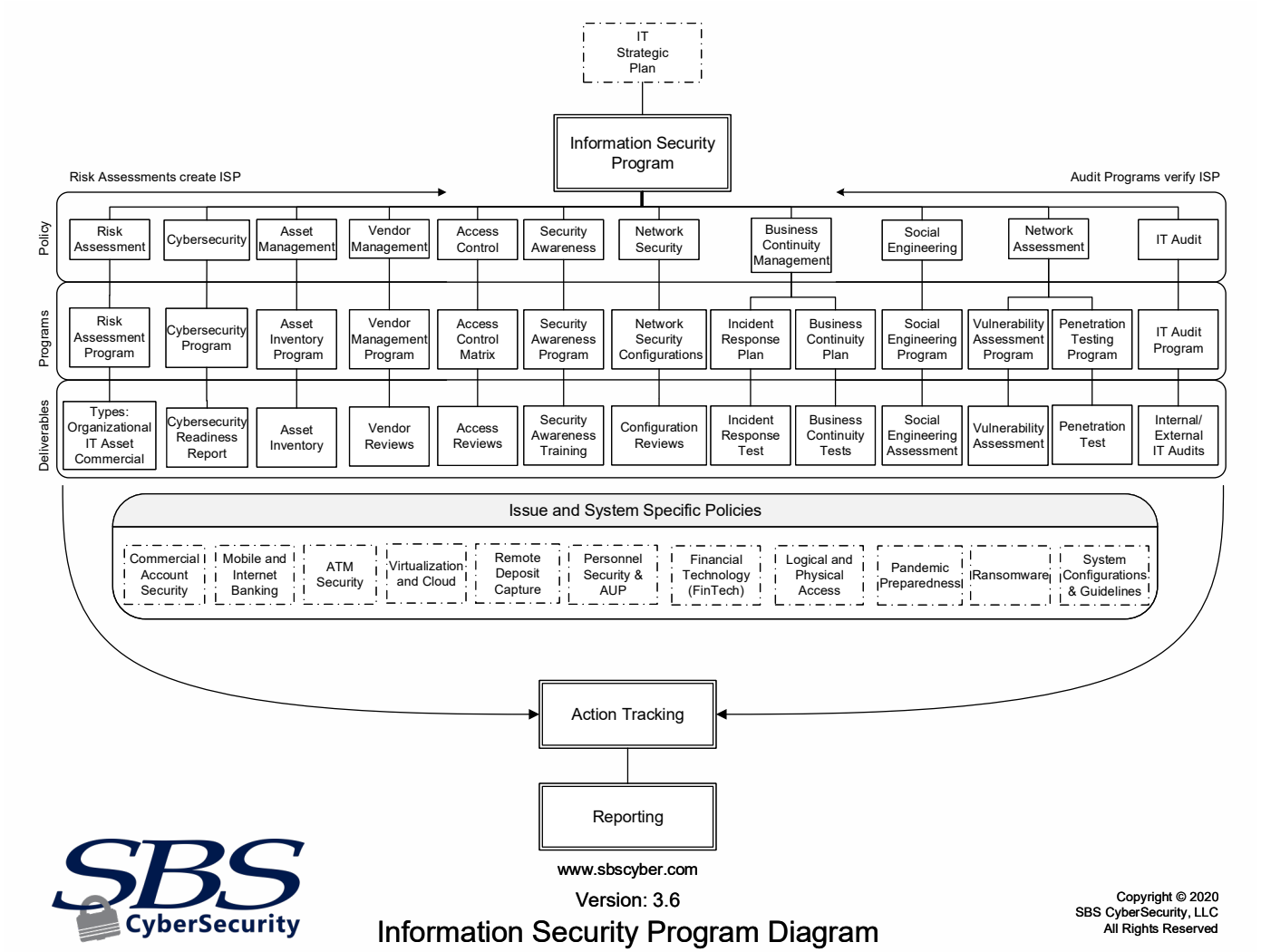
Other Requirements:

- **Virtualization**
  - Updated network topology to reflect virtualized environment
  - Access rights administration, including privileged users and remote access
  - System/image standard configurations
  - Licensing
  - Patch management
  - Incident response plan
  - Business continuity and disaster recovery plan
  - Physical security
  - Encryption
  - Monitoring, logging, and auditing
  - Network vulnerability assessment and penetration testing
- **ATM operations**
  - Physical and logical security controls
  - Patch management
  - Network segmentation
  - Dual control over cash
  - Card issuance procedures, including PIN issuances
- **Customer-facing call center operations**
  - Customer identification procedures
  - Access rights administration
  - Personnel security
  - Type and frequency of management reports
  - Scope and frequency of call center audits
- **Internal IT help desk operations**
  - Access rights administration
  - Help desk activity logging and monitoring
  - Ticketing and tracking system adequacy/prioritization
  - Type and frequency of management reports
  - Scope and frequency of help desk audits
- **Servicing provided to other entities**
  - Contract adequacy
  - Service level agreements (SLA) compliance
  - Business continuity and disaster recovery plan considerations
  - IT and cybersecurity risk assessments
  - Insurance coverages for services provided
  - Security of client data, including encryption over data-at-rest and data-in-transit
  - Type and frequency of management reports for services provided to other entities
  - Scope and frequency of help desk audits

SBS Information Security Program Blueprint

SBS has been partnering with financial institutions across the United States for more than 15 years to help build Information Security Programs that are comprehensive, manageable, and valuable. SBS' Information Security Program framework is built on regulatory guidance (primarily the FFIEC IT handbooks) with help from industry best-practice (FFIEC, ISO 27001, NIST, SANS, CIS, and COBIT). SBS has laid out the foundation of a strong Information Security Program in an Information Security Program Blueprint, as seen below.

The ISP Blueprint is designed to give bankers a visual depiction of what an Information Security Program should look like, a sense of flow from the top-down, and a path to ensure the ISP is repeatable and can handle anything you throw at it.



The focus of this whitepaper is the InTREx documentation, which aligns directly with the ISP Blueprint on the previous page. The "Policy Components" listed out in the first tier of ISP documentation in the Blueprint are the things that all financial institutions need to do, regardless of size or complexity.

If you align the ISP Blueprint Policy Components with the InTREx expected documentation, you'll find most of the major ISP Blueprint sections are listed out multiple times in InTREx, including:

- The Information Security Program
- IT Risk Assessment
- Cybersecurity Assessment
- Vendor Management
- Business Continuity/Disaster Recovery
- Incident Response
- IT Audit

There are three tiers to the top-level of the ISP Blueprint:

1. Policy Components: The high-level, long-lasting policy statements that define the purpose, scope, requirements, and responsibilities of each individual ISP component.
2. Implementation Programs: The day-to-day operating procedures for each component.
3. Plans/Deliverables/Services: The outcome from each component, whether it's the result of an assessment (report), a deliverable as a result of a service-performed, training, or testing of a BCP or IRP.

The next component of the ISP Blueprint is the Issue and System Specific Components section. These additional components of your ISP are based on your risk assessment. If your institution implements remote deposit capture, for example, you should either outline an RDC policy or include an RDC section in your ISP. The controls you have decided to implement around RDC in your risk assessment to reduce risk should then be documented in your RDC policy. If your institution does not implement RDC, you don't need to include it in your ISP. Many of these additional requirements are outlined in the "Other Requirements" section above. Those items may include cloud-computing, managed security service providers, VoIP, ATMs, virtualization, wireless, help desk, etc.

That brings us to the testing component, otherwise referred to as auditing. There are three ways to protect information: people, process, and technology. Financial institutions must also test (audit) these three areas for compliance and adequacy. Testing your processes is frequently performed through an IT audit. Testing your technology is accomplished most often through external penetration testing and internal vulnerability assessment (or other combinations of the two). Testing your people is done through social engineering assessments.

InTREx has an entire section dedicated to audit, which includes documentation around an IT audit policy, IT audit charter, IT audit plan/schedule (that includes testing for people, process, and technology), IT audit risk assessment, and making sure that findings and recommendations are tracked to remediation or acceptance.

The final component of a well-rounded ISP is Remediation and Reporting. Remediation involves closing the loop on the feedback component (audit) by ensuring improvements to the ISP are implemented (completed), tabled, or accepted. Accepted risks should be documented and reported upstream regularly. Reporting is the other final component of the ISP. Strong ISP reporting means that regular reports to senior management and the board of directors include updates and progress on all the major items discussed above – from the risk assessment, to the ISP components, to testing the institution's people, process, and technology.

When your Information Security Program is at its best, it allows your financial institution to identify risk and make decisions on how to mitigate risk (risk assessment), document those decisions in your policies and procedures (ISP), test those decisions (audit), and continuously improve security at your institution (remediation and reporting). Using a model like the ISP Blueprint can help your organization better understand how all of the components work together to build a better ISP and mature the security of your institution.

SBS CyberSecurity

Free Resources

available at: sbscyber.com

Hacker Hour Webinar

Join our free monthly interactive webinar series focused on discussing cybersecurity issues and trends.

Product Demos

Discover the power of our offerings with live demos scheduled each week highlighting individual products and services.

Security Awareness Training

Share our cybersecurity training tools with both your employees and your customers.

TRAC™ Action Tracking

Remain diligent with your remediation tracking and follow up by creating security plans associated with your risk assessment.

Join Our Email List

Follow the latest trends in cybersecurity, information technology, and upcoming educational events from SBS CyberSecurity.

Your Cybersecurity Ally

SBS CyberSecurity, LLC (SBS) is a top-rated consulting and audit firm. With over 20 years in the cybersecurity industry, SBS has provided solutions to thousands of regulated organizations across the United States and abroad. We offer dynamic solutions to help you build a proactive risk management program capable of withstanding the daily threats your organization faces. Our services are designed to assist you in making informed cybersecurity decisions to better protect your business.

For more information:

sbscyber.com | 605.923.8722