



## IT & EDI/B2B Risk Assessments Rationale/Benefits

Risk Management is a systematic methodology for identifying, analyzing, controlling, reporting, and reviewing risk factors—within a system, within a network, and throughout an organization.

The objectives of Risk Management are:

- Eliminate and/or reduce weaknesses.
- Improve security controls and processes.
- Determine and preserve a successful balance between risk probability vs. productivity and profitability.
- Reduce operational disruptions and losses.

Risk Management has become increasingly important because of Sarbanes Oxley compliance requirements which address **the security and integrity of IT systems and controls** as well as the accuracy of financial reporting.

A successful Risk Management program should:

- Provide information on historical events, today's issues, and planned responses to possible future events.
- Increase efficiency by reviewing and streamlining processes.
- Predict and eliminate future risks and provide a plan to deal with contingencies.
- Satisfy internal and external auditing requirements.
- Design performance improvements, reduce unnecessary expenses, and control the cost of compliance.
- Improve the confidence of trading partners, internal business partners, shareholders, and regulators.

Risk Management of EDI and B2B systems and processes presents special challenges because of the interrelationship of the trading partners—vendors, suppliers, distributors—and the many points of connectivity between the entities and systems throughout the supply chain.

Risk Management should enhance and support your EDI and B2B systems and processes by:

- Securing the integrity of critical information.
- Protecting key logical and physical infrastructure components.

Risk Management phases:

- Risk Assessment
- Risk Reduction Plan
- Risk Reduction Implementation and Follow-up

Risk Management should be an iterative process, with the three phases repeated periodically to ensure that the processes in place continue to be effective and that new risks are identified and controlled.

Advantages of third-party EDI/B2B Risk Assessment:

- Allows your decision-makers and staff to continue their priority tasks.
- Brings a proven Risk Assessment methodology and framework to your project.
- Provides technical Risk Assessment expertise—in-depth knowledge of EDI, B2B, and Internet security.
- Provides business Risk Assessment expertise—process improvement, process documentation, project leadership, and culture analysis and management.
- Brings objectivity to the analysis of your EDI/B2B systems, processes, and culture.
- Reduces the project timeline through dedicated project objectives.

Our Risk Assessment process provides the framework and the deliverables to enable your EDI/B2B management and staff to manage the Implementation and Follow-up phase. Or, we can provide the project management and support to direct the implementation.



## EDI/ B2B Risk Assessment Process

Risk Assessment of an EDI/B2B infrastructure (system, network, people, partners) presents complexity and unique challenges to the evaluation process. These challenges include:

- EDI connectivity to multiple VANs.
- B2B web portals for a portion of the trading partners and/or trading-partner-specific portals.
- Internal partners as well as external trading partners.
- Third-party processors—service bureaus—that become part of the supply chain.
- Changing custody of the data at various points along the supply chain.
- Multiple front-end and back-end applications feeding to and from the EDI/B2B network.

For assessing an EDI/B2B department and system, we examine the following key factors:

1. **Physical security**
2. **Personnel security**
3. **Contractual security**
4. **Data/Transaction security**
5. **System security**
6. **Network security**
7. **Business Resumption/Disaster Recovery**

Each key factor is evaluated according to:

- Existing security controls (physical/logical)
- Current weaknesses
- External risk sources/internal risk sources
- Past events
- Potential events
- Cost vs. consequence
- Compliance (e.g., Sarbanes-Oxley, ISO/IEC, GS1)

We lead a collaborative assessment project, where your IT management designates staff to work with our consultant. We facilitate this process with an organized framework, including scheduled interviews and questionnaires, which eliminates wasted time and time away from core tasks.

### 1. **Physical security factors**

- Premises: building, external suite, computer/server room, offices
- During business hours, after hours
- Card-key access management
- Key-secured computer cabinetry
- Key-secured desks
- Guards, monitoring, CCTV, cameras
- Visitor escort/sign-in logs

### 2. **Personnel security factors**

- Background checks
- Network, system, application log-ins
- User IDs/passwords
- Trace of individual accounts and time stamping
- Logs—network, system, application
- Audited actions—success/failure audits
- Add/delete/change, download/print directives
- Disclosure/confidentiality
- Security awareness/training—risk response readiness

### **3. Contractual security factors**

- Customer contracts/requirements
- Trading partner agreements
- Confidentiality agreements
- Employee contracts and code of conduct
- Contractor contracts and code of conduct
- Service level agreements with internal partners
- Offsite storage facility contract
- Third party—service bureau—contracts

### **4. Data/Transaction security factors**

- Encryption
- Digital certificates
- Transport protocols
- Sensitivity: high, medium, low
- Integrity
- Confidentiality
- Authentication
- Reliability
- Non-repudiation
- Audit logs/reporting
- Archival and recoverability
- Document classification/retention

### **5. System security factors**

- Log-in management: users, administrators, management, software vendors
- Passwords/PINs
- Use of personal computers and PDAs
- Administrative levels of access
- Modification restrictions/protection of software code
- Anti-virus software parameters

### **6. Network security factors**

- Firewall, VPN, Tunnel
- VAN connectivity
- Web connectivity
- Security protocols
- ACLs—Access Control Lists
- Domain level authority, access, control
- Intrusion-detection technology
- Partitioning of internal networks

### **7. Business Resumption/Disaster Recovery factors**

- Online archival and retention
- Backup copies of: operating system software, system data and security files/tables, production libraries/directories and databases (including program source), development tables, libraries/directories, and databases
- Backup rotation/transport schedule
- Retention of tape/disks
- Security of offsite storage facility
- Escalation levels for problem resolution and recovery



## Our EDI/B2B Risk Assessment Expertise

- Technical Risk Assessment expertise—including in-depth knowledge of EDI, B2B, and Internet security.
- Business Risk Assessment expertise—process improvement, process documentation, project leadership, and culture analysis and management.

Proficiency in industry accepted standards and in using related procedures and documents in the assessment process:

- ANSI ASC X12
- GS1/GDSN
- IETF EDIINT
- SEC (Securities and Exchange Commission)
- ISO/IEC 17799:2005, the international standard Code of Practice for Information Security Management
- Committee on Sponsoring Organizations of the Treadway Commission (COSO)
- Control Objectives for Information and related Technology (COBIT)
- National Institute of Standards and Technology (NIST)

Direct participation in EDI/B2B standards development:

- Chair of the eTG (eCom Technology Group) Committee of GS1 which defines technical requirements on B2B message transport and routing, message architecture, security, and more.
- Chaired work group at ANSI ASC X12 that developed a cross-industry guideline for Internet EDI/XML transport.
- Chaired the Texas Data Transport Working Group, tasked with the development of the EDI and XML transport standards for the State of Texas Energy Deregulation.
- Provided EC/EDI/Internet security training and development for the Data Interchange Standards Association (DISA), the administrative entity that supports ANSI ASC X12.

Over 15 years EDI/EC leadership, business development, and technical expertise; and 25 years IT management and technical experience.

Successful implementation of secure traditional EDI and internet EDI, EC, and XML systems for clients in the retail, energy, electronics, and semi-conductor industries, and for governments and associations.

Hands-on experience with technical EDI/Internet security and transport components:

- EDIINT AS1, AS2, AS3
- ebXML Message Services
- FTP—File Transfer Protocol
- Secure FTP—Secure File Transfer Protocol
- FTP/SSL—File Transfer Protocol/Secure Socket Layer
- HTTP—HyperText Transfer Protocol
- HTTPS/SSL—Secure Hypertext Transfer Protocol/Secure Socket Layer
- IMAP—Interactive Mail Access Protocol
- IPsec—Internet Protocol Secure
- L2TP—Layer 2 Tunneling Protocol
- PGP—Pretty Good Privacy
- OpenPGP/GnuPG
- POP3—Post Office Protocol Version 3
- PPTP—Point-to-Point Tunneling Protocol
- S/MIME—Secure Multipurpose Internet Mail Extensions
- SMTP—Simple Mail Transport Protocol
- TCP/IP—Transmission Control Protocol/Internet Protocol
- TELNET—Network Virtual Terminal Internet Protocol
- Tunnels/VPN—Virtual Private Networks
- XML Encryption and digital signature