GDSN Security Audit

Requirements

Delivery Date: 10/16/07
Version Number 1.1
Disposition: **Final**

Document Summary

Version Number	1.1
File Name	GDSN_SecurityAudit_v1 1_Final_from2007_Oct16
Delivery Date	10/16/07
Owner	GDSN Inc.
Description	GDSN Security Doc

Document Revision History

Version Number	Date of Change	Changed By	Revision Description
0.01	01/20/2007	Sean Lockhead	Creation of Document
0.02	01/24/2007	Sean Lockhead	Feedback from Architecture Committee Meeting
0.03	01/31/2007	Sean Lockhead	Incorporate comments
0.04	05/01/2007	Sean Lockhead	Clean up for Legal Review
0.05	05/07/2007	Sean Lockhead	Finalize for Review
1.00	05/23/2007	Sean Lockhead	Final Review Complete on Architecture Call
1.1	10/16/2007	Sean Lockhead	Finalization of Document for posting

Table of Contents

1 Executive Summary

1.1 Introduction

With strong commitment to the vision and principles of Global Data Synchronisation, it is recognized that in order for this vision to be achieved, standard, compliant product information must be able to flow uninterrupted between trading partners in a secure fashion. Data to support the exchange of supply chain information includes in some cases price which is the most sensitive of all data. Not only does it carry the greatest risk when not handled securely, but it also carries the greatest rewards when handled securely.

One of the key considerations for ensuring the usability and wide adoption of the GDSN Network is the security needs and concerns involved in implementing and interacting with such a network. Responding to concerns expressed both from the community and the industry at large, GDSN has collaborated on this proposed strategy for developing a set of security guidelines that address all aspects of security (physical, logical, business processes and contractual).

This document describes the GDSN requirements for addressing a security audit within the GDSN network as well as beyond the network to include recommendations for the relationship between source / recipient data pools and data source / data recipients.

It is the position of GDSN that Trading Partner agreements ultimately govern and drive the Supplier and Retailer relationship and their associated relationships with their Data Pools. As such, Trading Partners must have legally enforceable agreements in place where data ownership and security are concerned.

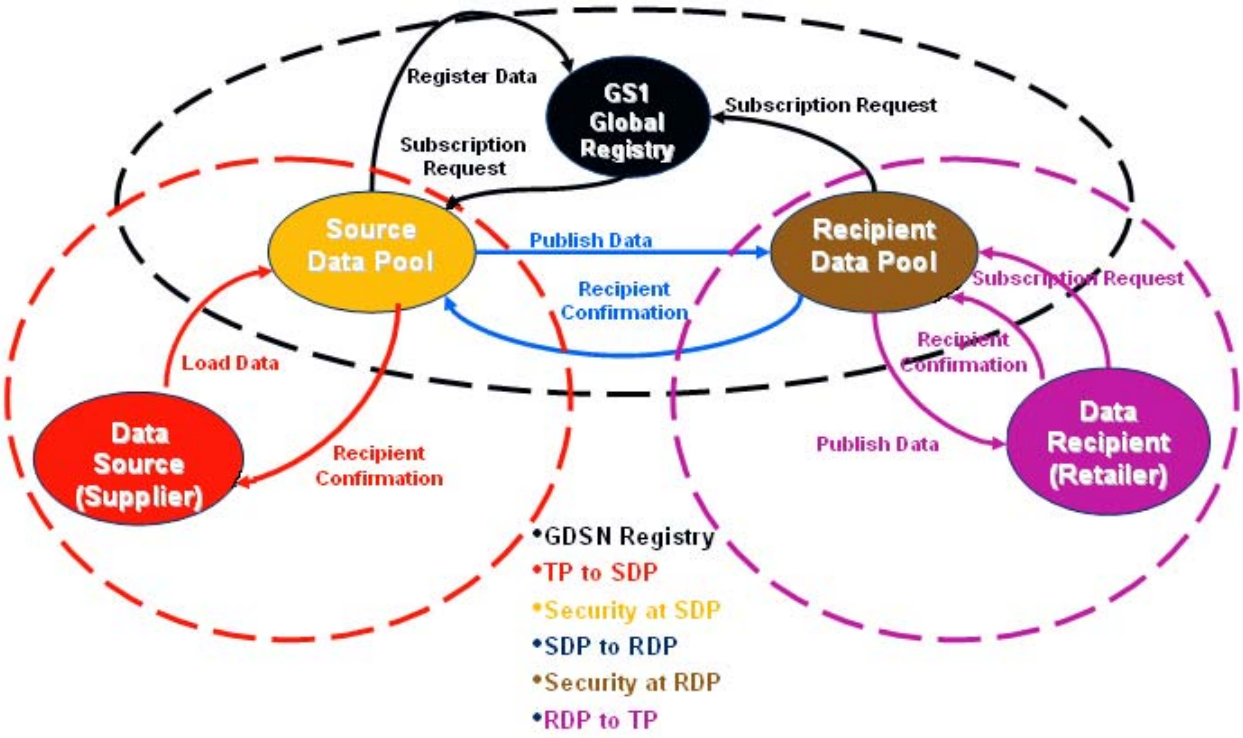
This security audit requirements document is intended to examine the breadth and depth of the aspects of a security audit, the various components and either requirements or recommendations depending on whether in, or out of the network.

A Security Audit is addressed in all related aspects with the goal of ensuring confidence in the data source / data recipient that the storage and handling of their GDSN data is secure at all times through the process both in / out of GDSN network. Actual enforcement by GDSN Inc. would be restricted to the GDSN processes. As such, security audits must be addressed at several levels within and throughout the process which includes participants beyond the GS1 Global Registry, beginning with the Data Source, to the Source Data Pool, to the Recipient Data Pool, and finally the Data recipient. Depending on the point in the process, different solutions, measures and / or controls will be required to ensure security of the data.

The information contained in this document represents the current view of GDSN, Inc. and may be changed over time as technology; security best practices and supply chain automation evolve.

1.2 Choreography

GDSN CHOREOGRAPHY



RELATIONSHIP SCENARIOS:

Information Technology Platform Ownership

Companies have an almost limitless variety of options on how to manage their Information Technology (IT) infrastructure. In the simplest scenario a Company owns all IT assets, runs them in a facility they own, manages the infrastructure themselves and they manage and administer the applications.

While this is not a comprehensive list, some of the common used options to manage IT infrastructure are:

- Leased IT assets (processors, hard drives, network equipment, communication lines, etc) from a financing company
- Leased IT assets and have them running in a shared data center
- Own IT assets and have them running in a third party data center
- Leased network services between facilities owned by the company
- Outsource to a third party the operation of data center and all IT assets

- Outsource the running of a business application to a third party
- Outsource all IT infrastructure operations
- Use a hosted application run by a third party
- Use part of a shared service run by a third party

Additionally, with the advent of telecommuting, Wi-Fi hotspots, Virtual Private Networks (VPN), use of personally owned computers, etc, many of the above scenarios get even more complex

Frequently the ownership of IT assets is difficult to discern even to members of the IT department. Due to the constant reallocation of scarce resources many large companies are a combination of all of the above models with numerous variations.

2 Common Elements

2.1 GDSN Data

GDSN Data can be viewed as Party, Catalogue Item, Price, or any other information that is communicated in the Global Data Synchronisation Network (GDSN). The processes for the dissemination of this information are related but not truly interchangeable. An effort is made to try and address both the similarities as well as the differences.

2.2 Transport Protocols

In the GDSN, the only transport protocol is the use of electronic data over the public Internet, Applicability Statement 2 (EDIINT AS2). This is a mandatory requirement for Data Pools and the Global Registry in the GDSN.
For additional information, please refer to EDIINT AS2 document and Operations Manual.

2.2.1 Encryption

Encryption is critical part of secure data handling. Within GDSN there is AS2 encryption. Beyond GDSN there can be other types. There are different levels of encryption:

- Transport Protocol Message encryption (AS2)
- Data (Payload) Encryption
    - Full – Encryption of entire payload – Requires additional content. What are the benefits and constraints (Same question applies to Partial as well)
    - Partial – Encryption of certain individual attributes value(s) within the payload. Note: Encrypting attribute values is above and beyond the current scope of GDSN and would only be recommended if the function is needed.

Data messages communicated between all parties in the GDSN network will by encrypted by the use of EDIINT AS2 protocol.

There are no standards governing the storage of data in neither the Data Pools nor the communication between the data pools and their trading partners. Internal storage and encryption of the data is based on the business relationship between the Data Pool and its trading partners... For example, Price security obligations may be managed by the mutual agreement of the data pool and its members.

2.2.2 Digital Certificates

Certified Data Pools must use a self-signed certificate or a signed digital certificate from a recognized third party organization that is responsible for the issuance of these types of certificates. All Data Pools and the Global Registry must implement the use of digital certificates and maintain an up-to-date listing of all the other Data Pools and Global Registry digital certificates

Any use of a digital certificate between a data pool and their trading partners would be handled within their relationship agreement. Refer to the operations manual in regards to any additional digital certificate information or AS2 information.

2.3 GDSN Data Ownership

To properly address security issues and concerns as they relate to the Data Pools, the major issue that must be addressed and resolved is to establish the chain of custody and ownership of the data as it moves through the supply chain. The “ownership” of the data dictates what operations may be performed and by whom at each point in the chain. Based on the previous statement it may be assumed and temperate / based on the trading partner relationship that the retailer owns the rights to distribute the data they received from the supplier and is typically governed by the terms of a trading partner agreement. It is also assumed they can store it in any form they prefer if it is satisfactory to mutual agreements with suppliers, as long as no trading partner agreements that are in addition to GDSN agreements in place are violated.

One of the most interesting questions for security of data is who is responsible for the data as it passes through transactional messaging systems that span several business entities and boundaries. When a source gives permission to a source data pool to send GDSN Data information to a recipient the information is sent to the recipient for their use. Does that data belong to the recipient? This issue is typically mediated by a trading partner agreement between the supplier and the retailer. This agreement will outline the responsibility of each party and the terms of use and confidentiality governing the data. If trading partners through this document agree on the use and security and confidentiality surrounding the information to be shared then the trading partner agreements that exist with each of the service providers involved between the trading partners must include a provision that each provider will be held to the same or more stringent security measures and confidentiality. A sample Trading Partner agreement is shown in Appendix A.

The following assumptions are made:

- The trading partner agreements between the Data Source and their Source Data Pool and their trading partners govern the data ownership, confidentiality and responsibilities of the GDSN Data information.
- When the Data Source initiates publication of their data to a trading partner, the data to be communicated is going to be sent to the correct Data Recipient.
- At the time the data is published to the trading partner, the data is exposed to the Data Recipient.
- The Data Recipient is responsible for controlling what actions may be taken with this data and protecting the confidentiality of the data.

<u>Potential Issues:</u>

- What are the ramifications of the retailer receiving data from supplier in the sense of what can be done with the data in the context of data ownership?
- What agreements must be in place allowing entities to use or host it on their secured site (web portal) for the use of their user community (individual stores, users)?
- If they can host it and they place the GDSN data on their own web portal, can the web portal be hosted by third party?
- Can the hosted solution with GDSN Data information be outsourced? There may be additional agreements that need to be in place to protect the confidentiality of the data?
- Are there any mutual agreements between supplier and retailer that govern what kind of third party is allowed to host the retailer’s solution?

It appears that once the retailer receives the data they can communicate or make it available to their own users in any format they prefer.

3 GDSN Registry

3.1 Summary – GS1 Global Registry

The Global Registry (GS1 Global Registry) is responsible for ensuring that trading partners registered at the Global Registry (members of GDSN), and have passed the GDSN-mandated validations. Through the use of the Basic Party Synchronisation process, the Global Registry communicates all validated Trading Partners (GLN's) to all Data Pools for use in the GDSN Business Message Standard use cases.

The Global Registry is responsible for ensuring that registry transactions (Item, Party, Subscriptions etc.) processed at the Global Registry have passed the GS1 Global Registry-specific GDSN-mandated validations and have been submitted by registered, validated Parties (GLN). Through the use of the Catalogue Item Synchronisation process, the Global Registry enables the Data Pools to communicate the Standards-based Business Message standard messages for all the use cases.

The Global Registry Item / Subscription matching process functionally provides the Data Pools and Trading Partners the information necessary to perform the GDSN use cases. The Global Registry distributes subscriptions to the one or more Data Pools having registered items that can fulfill the subscription criteria. Through the use of the Catalogue Item Synchronisation process, the Global Registry enables the Data pools to communicate the Standards-based Business Message standard messages for all the use cases.

3.2 Physical

3.2.1 Database

Access to the Global Registry is restricted to authorized personnel of the GS1 US Technology Services Group (TSG) as the technology service provider of the Global Registry for GDSN Inc.

The GDSN Customer Support also should have access to the information contained in the Global Registry as well as messaging to and from the Global Registry.

Data access types for Global Registry personnel are as follows:

- Add – who / what can add, how is managed / restricted
- Change – who / what can add, how is managed / restricted
- Delete – who / what can add, how is managed / restricted

3.2.2 Messaging

The GDSN makes use of the electronic data over the public Internet and the Applicability Statement 2 protocol (EDI INT AS2).

The AS2 protocol uses the Hyper Text Transmission Protocol (HTTP). The AS2 specification solely describes the secure transmittal of data over the Internet using HTTP. It is a specification

on securing and transporting data, not on validating or processing the data. The transported data is then dispatched to the appropriate processor based upon its content-type.

As part of the EDI INT messaging, the use of digital certificates is mandated in the Global Data Synchronisation Network. The exchange of the digital certificates is facilitated by the GDSN Customer Support Group.

3.3 Compliance

The GS1 Global Registry must successfully complete all certification events and remain certified for participation in the GDSN.

3.4 Legal

The GS1 Global Registry is required to meet or exceed the Service Levels set forth in the GDSN Inc. / GS1 US Technology Services Group. (Refer to SLA definitions).

3.4.1 Service Level Agreements (SLA)

- It is the responsibility of the Global Registry to maintain a reference list of Certified Data pools that can effectively communicate with the Global Registry. Each Data pool has a set of information associated with it that is stored in the Global Registry.
- The function of setting up the Data pools in the Global Registry falls to the GDSN Customer Support Staff, operating under the direction of GDSN Inc. representatives and in unison with the GS1 Global Registry provider.
- The Global Registry is required to process valid messages sent to it. It is agreed that scheduled outages which have been communicated by the Global Registry to all affected Data Pools in the manner specified in this document can affect the timeliness of the processing (e.g. processing can take place after the scheduled outage period).

3.5 Communication within the GDSN

The trading relationship between the Global Registry and the Data pools covers how the data is communicated between the network entities.

Please refer to GRALA (Global Registry Access and License Agreement) for additional information.

3.5.1 Data Communication

All GDSN data is communicated using GDSN standards-based XML message(s).

3.6 Trading Partner Security Requirements

Requirements raised by the GDSN Trading Partners about information registered in the Global Registry:

- Trading Partners must be satisfied that any information registered in the Global Registry (parties, items, subscriptions) is only accessible by the authorized entities

- Data pools and Trading Partners want to ensure that information communicated to and from the Global Registry to each entity is secured from an access-control as well as an authorization perspective.
- As new functionality is added to the Global Registry, additional requirements may surface.

3.7 Global Registry Security Requirements

The Security Audit process should ensure that the Global Registry, at a minimum, demonstrates the following:

- Successful completion of a third party administered security audit (when defined)
- Adequate access controls are in place to ensure data is exposed and distributed only to the appropriate Data pools.

4 Trading Partner to Source Data Pool

4.1 Summary

Source Data Pools have the ultimate responsibility for the communication of GDSN Data into the Global Data Synchronization Network (GDSN). They are responsible for gathering the GDSN Data from their supply side trading partners, performing validations upon the data, registering the items in the Global Registry, managing that the data is sent to the correct trading partner or their GDSN-certified RDP and for ensuring the data is compliant when distributed into the network. The following explains the role of the Source Data Pool in the Security Audit Process, highlighting the issues and concerns related to the Source Data Pools and their relationships with their trading partners.

4.2 Communication of Synchronization Data

The trading relationship between the Source Data Pools and their trading partners governs the requirements Source Data Pools have for how they receive data from their members, as well as additional value-added services they perform for those members. The requirements cover how the data is received from the trading partner and what transport protocol is utilized. These services could include additional data validations, transformation of the data from different formats, use of the data within other applications offered by the Source Data Pool and any other value-added services offered or performed by the Source Data Pool. A Security Audit should embrace these service areas for requirements gathering.

4.2.1 Data Pool Value-Added Services

Restrictions placed upon Source Data Pools that limit how they can handle GDSN Data information sent from trading partners could severely hamper the Source Data Pool's ability to perform or provide these services for their members. It may also limit the Source Data Pool's ability to comply with all of the GDSN Data synchronization process requirements relating to validations, synchronization list processing and maintenance and potentially disrupt their ability to support the existing business process of their trading partners.

- GDSN Data applications
- Robust user interface allowing the Data Source to enter information directly into the Source Data Pool
- Workflow processing
- Supplier and/or Retailer specific validations
- Message and file level track and trace for audit or problem resolution
- Reporting
- Retransmission capabilities
- Other

A Security Audit should embrace these service areas for requirements gathering.

4.3 Trading Partner Security Audit Requirements

Several requirements have been raised by the different parties involved in the communication of GDSN Data information through the GDSN:

- Suppliers are concerned that they only have trading agreements with their own Source Data Pools and their Data Recipients, but not the intervening Recipient Data Pools.
    - This should be addressed by the audit processes and procedures definition.
- Both the retailers and suppliers want assurance that the data pools provide access controls that restrict access to the GDSN Data to only the trading partner for whom the data is intended.
    - This should be addressed by the audit processes and procedures definition.
- There are current proprietary data pool implementations of additional value-added services that the data pool community will not want GDSN Data synchronization security to constrain.
    - This should be addressed by the audit processes and procedures definition.
- Some trading partners believe some level of encryption may be required. Encryption could include the entire message down to individual tags contained within the message payload. While providing an additional level of security, encryption can also create barriers to how GDSN Data is communicated within the network as well as impediments to the processing that may be required of the data pools.
    - This should be addressed by the audit processes and procedures definition.
- The GDSN Security Audit requirement shall ensure that data pools demonstrate the successful completion of a third party administered security audit.
    - The definition and process and procedures definition enable this requirement to be met for the GDSN community.
- Adequate access controls are in place to ensure data is exposed only to the appropriate data recipients.

5 Security at Source Data Pool

5.1 Summary

This document describes the proposed strategy for addressing security audits of GDSN Source Data Pools (SDP) within the GDSN network. A data source is normally synonymous with a manufacturer, however may include other roles, e.g. distributor, broker, wholesaler, etc. There are different aspects of security audits that need to be addressed.

5.2 Data Stored vs. Data Passed

Another issue often raised is a requirement of some suppliers that data doesn't reside on the data pool but only is passed to recipient. Even the GDSN data that is not intended to be available to the community of the data pool (for viewing or download) and only "to be passed" is still stored there for the very short time until is passed.

There are potential ways to provide for a pass-through mechanism. For example, one possible solution is to encrypt the part of the message (for example, Item Price Type Segment) so that the data pool can perform validation and distribution of GDSN Data, and still only the intended recipient can read price values and retrieve the information that is intended solely for them.

A GDSN Security Audit Process can potentially analyze the data storage and passage capabilities for the Source Data Pool.

5.3 SDP Security Concerns

The suppliers do not have agreements with solution providers of the retailers. In the case of GDSN these solution providers are Recipient Data Pools as well as other solution providers used by the data recipient. But the supplier can have a mutual agreement with the retailer regarding their data. If they are not comfortable with the solution and processes of that retailer they can opt to use either peer to peer solutions, or continue to use current processes and not use GDSN for that relationship.

The basic role and behavior of the data pool in the GDS network is clearly defined, but each data pool provides value-added services to its members which are not.

A GDSN Security Audit may be necessary to perform the checks for these types of relationships.

A decision will need to be made if this level of detail within a GDSN Security Audit is necessary.

5.4 Conclusion

To establish a high confidence level for exchange of GDSN data in the GDSN we could recommend security audit guidelines for all participants. Some data (such as price-based data) may have additional security audit requirements.

A security audit segment can be added into the legal GDSN data pool agreement stating that the data pool agrees to make the data available only to the designated party. If the data recipient is a

member of another data pool then only that data pool would get the data (i.e. a SDP can only guarantee that the data has been delivered to a RDP).

6 Security from SDP to RDP

6.1 Summary

As part of the GDSN, one of the most important stages of the synchronisation choreography is when information (item, party, price, etc.) is sent from the source side through the network to the recipient side. It is at this point when information is exchanged in a way that is governed by the standards process and all of the certified data pools are working in a standards-based, validated fashion between Source Data pool and Recipient Data pool.

6.2 GDSN Certification

All Data pools operating in the Production GDSN environment where all the live synchronisation processes occur must have passed the GDSN certification process as defined by GDSN Inc. and GS1. There are limited certification criteria that impact the overall security of the GDSN, as most of the certification concentrates on the functionality.

6.3 SDP to RDP Security Concerns

6.3.1 Priority / Applicability of Multiple Agreements

1. DP – DP in GDSN
2. DP – DP non-GDSN
3. TP – DP
4. TP – TP

The GDSN security audit needs to ensure that there are no conflicts between multiple agreements in place and that any security audit process account for these multiple agreements.

The GDSN security audit needs to establish a clear line of precedence (and priority) for agreements such that there are no conflicts between multiple agreements in place and that any security audit process account for these multiple agreements.

7 Security at Recipient Data Pool

7.1 Recipient Data Pool Role

The role of the Recipient Data Pool (RDP) in the Global Data Synchronization Network (GDSN) is to provide an interface between the GDSN and the data recipient. A data recipient is normally synonymous with a retailer, however may include other roles, e.g. distributor, broker, wholesaler, etc. To perform this role the RDP receives GDSN standard messages from source data pools and the Global Registry and routes them to and only to the recipient designated in the messages which could include third parties outside the network.

7.2 Recipient Data Pool Security Audit Requirements

7.2.1 Established Relationships

The RDP may act as a data repository on behalf of the data recipient. In this scenario the RDP (and SDP) will hold the data for the recipient. This scenario has the data recipient responsible for security of supplier data based on its relationship with the recipient data pool. This type of solution is very common among data pools and solution providers. It allows for a staging arena for the Data Recipient's data and for reloads of the data should a failure happen in the recipient's internal data repository. This should be based on a mutually-agreeable timeframe and to not exceed the agreements between the Data Source and the Data Recipient and the Trading Partner and its Data Pool. In this scenario the security audit of the data and processes needs to ensure that the requirements are met through several relationships.

The first relationship is a Trading Partner relationship. This is an agreement between the Trading Partners and will govern the use of and confidentiality of the data in the relationship. A Trading Partner Agreement can be executed that describes the use of data, by whom, for what and the penalties for breaches in the contracted use of data. A security audit must be strategically defined for this relationship.

The second relationship is between the recipient Trading Partner and its data services provider. In this relationship the Recipient needs to hold its data providers to an equal or higher level of security than is mandated by the Trading Partner agreement. There can be multiple service providers between the source and recipient which are all responsible for upholding / maintaining integrity and security of the data. This will include but may not be limited to GDSN recipient data pool(s) applications and application architecture, data bases and database architecture, service oriented architecture, data centers, long and short haul disaster recovery, on and off-site backup and recovery, third party solution partners, data transport mechanisms and protocols. There should be limited specific requirements in terms of technology platform considerations.

The ability to perform a security audit for this type of relationship becomes a little unclear as to how detailed and how far a GDSN-based security audit should go in establishing the audit criteria.

8 Security from Recipient Data Pool to Data Recipient

8.1 Summary

Message Information at Recipient Data Pool involves a unique situation since the GDSN data at this stage of the choreography represents information received from elsewhere in the network.

8.2 Communication of Synchronization Data

The trading relationship between the Recipient Data Pools and their trading partners governs the requirements Recipient Data Pools have for how they receive and transmit data for their members, as well as additional value-added services they perform for those members. The requirements cover how the data is received from the trading partners and what transport protocol is utilized. These services could include additional data validations, transformation of the data from different formats, use of the data within other applications offered by the Recipient Data Pool and any other value-added services offered or performed by the Recipient Data Pool. A Security Audit should embrace these service areas for requirements gathering.

8.2.1 Data Pool Value-Added Services

Restrictions placed upon Recipient Data Pools that limit how they can handle GDSN Data information sent to and from trading partners would severely hamper the Recipient Data Pool's ability to perform or provide these services for their members. It may also limit the Recipient Data Pool's ability to comply with all of the GDSN Data synchronization process requirements relating to validations, synchronization list processing and maintenance and potentially disrupt their ability to support the existing business process of their trading partners.

- GDSN Data applications
- Robust user interface allowing the Data Recipient to enter information directly into the Data Pool
- Workflow processing
- Supplier and/or Retailer specific validations
- Message and file level track and trace for audit or problem resolution
- Reporting
- Retransmission capabilities
- Other

The GDSN Security Audit Process would need to be strategically defined to address this type of relationship as to not constrain nor force a particular implementation methodology in this setting.

8.3 Authorisation

Authorisation is the ability to ensure that the entity that is attempting to perform a task is really the entity it says it is. The ability to authorise an entity or a trading partner is instrumental in establishing confidence in the data pool as well as the GDSN itself.

A GDSN Security Audit needs to ensure the ability to perform the authorisation function.

8.4 Access Control

This is the method by which only the entities that have rights and privileges to access and receive the data are the only ones to have access to it. This ability to properly ensure that an entity or a trading partner is allowed to receive or view the messages is also instrumental in establishing confidence in the data pool as well as the GDSN itself.

A GDSN Security Audit needs to ensure the ability to perform the access control function.

9 General GDSN Security Audit Requirements

9.1.1 Audit Discussion Guide

Requirements for a GDSN Security Audit should take into consideration:

- Is the GDSN Security Audit a Certification Requirement?
- What is the Frequency of a GDSN Security Audit?
- What is currently executed today in the GDSN?

9.1.1.1 Functional / Technical

Requirements for a GDSN Security Audit should take into consideration:

- How code is developed (processes)
- Open access to source code
- Personnel involved in any of the areas of the GDSN (DS, SDP. GR, RDP, DR)
- Functional – to be defined as functional developed
- Frequency – Consistency with currently implemented industry guidelines

9.1.1.2 Global Registry Impact

Today the Global Registry does not undergo any GDSN Security audits. The checks and balances are through the issues that arise through existing Global Registry deployments and operations.

Requirements for a GDSN Security Audit should take into consideration:

- An audit would be held once one was defined
- Frequency would have to consider cost against any recommendation.

9.1.1.3 Data Pool

- There is a requirements decision needed for what is the best for the GDSN community and the GDSN management. Is the GDSN audit:
  - A single audit that everyone undergoes, or does GDSN Inc.
  - Build a GDSN audit and contract someone to administer, or specific criteria that must be audited for with a basic requirement that whatever audit is used, ID list of what audits are acceptable.
- Data Pool to Trading Partner agreement must cover 3rd parties. Data Pools and 3rd party agreement, 3rd party to other retailer (TP agreement….).
- The number of relationships that can exist between Trading Partners which must be covered contractually. Each individual trading relationship must be analyzed to determine how / if they determine to do business and determine the viability of a GDSN Security Audit solution.

9.1.2 Security

- How is physical access to facility controlled? examples: Badges, Guards, CCTV cameras, Perimeter access controls, Internal area controls, Badge logs, Visitor escort policy, Sign-in logs
- How is access to related systems, applications, and networks controlled? Network login, User/ID password, Strong authentication
- Can system, application, and network actions be traced to an individual account and action time? Network logs, system logs, application logs, audited actions, non-audited actions, success audits, failure audits
- How information is (electronic & paper) protected from unauthorized disclosure and modification? What is the Document Retention Policy
    - Electronic: account authorization, account privileges, encryption.
    - Paper: locked offices, locked filing cabinets, locked desk drawers, document classification markings, shredding policies
- Protection of the software code to prevent things like “backdoors” left in the code, etc.
- Global Registry and Data Pool personnel with access to the data, and address Add, Change, Delete actions, download capabilities, printing, disclosure of information, confidentiality, etc. Do organizations have background checking policies and procedures?

9.1.3 Anti Virus

- Does the organization have anti-virus software installed on all related systems? Servers, user desktops, user laptops, user PDA's, email system
- How frequently are the anti-virus software and signature files updated? daily, monthly, quarterly, immediately or "n" days/week after release from vendor
- How frequently is the anti-virus software used to scan for viruses? Hourly, daily, weekly, or on email receipt?
- What level of control for work stations? Can individual users disable any of these key features? Disable or bypass the anti-virus software? Download software, install software? Perform admin level functions?
- What are personnel to do if they detect a virus? Stop using system, contact admin, and remove virus, document date/time and virus type, remove system from network?

9.1.4 Password & PIN Security

- Is there a password policy? password sharing, protection, password length, complexity and age requirements
- What password length and complexity technical controls are in place? password length enforcement, special numeric enforcement, password age enforcement, password reuse enforcement, invalid attempt thresholds
- Do users use shared accounts? multiple people using one account
- Are default passwords required to be changed?

- What is the process for resetting a password when user cannot remember it? Call helpdesk, visit admin, submit form signed by supervisor etc.

9.1.5 Network & Computing Resources

- How is access to related systems controlled? Username password, 2-factor authentication, one time password, etc.
- Are any related systems configured for remote access? Remote admin, remote users, modem, VPN, secureID or PKI
- Are related systems connected to any other networks? dual homes systems, internet connectivity, shared networks
- Are employees allowed to use their non-business personal computers to access related systems, or connect to related networks?

9.1.6 Backups & Disaster Recovery

Questions:

- Are there formal documented backup procedures and schedules that exist in creating 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
- What is the backup rotation schedule?
- Is the internal control environment over process clearly defined?
- Is documentation reviewed and updated annually?
- Have internal controls been systematically tested?
- Is testing of the internal controls retained in accordance with record retention?
- Is system and security configuration stored in a secure location on-site?
- Are backup files stored in a secure location onsite?
- Where is the onsite backup storage facility located?
- How long are backup tapes/disks kept onsite?
- Does company have an off-site storage facility?
- Does company have a written contract with off-site storage facility?
- How long does it take to retrieve a backup from an off-site storage facility?
- Backups and disaster recovery
- How often are backups moved to the off-site location?
- Are file and library backups kept at the off-site storage facility? Security files? Operating system? Documentation? Policies and procedures?
- Is a copy of the disaster recovery procedures at the off-site facility?

- Are the backups stored in secured containers while transport to and from the off-site facility?
- Does the company have a current disaster recovery plan?
- Does the plan include a sequence for restoring the systems that takes into consideration the criticality of the system?
- Has the disaster recovery ever been tested? And when?
- Have the test results been documented and followed up for problems?
- Have Information Management (System Support) and user responsibilities related to implementing and testing been defined?
- Have critical business and information assets been defined?
- Has a risk assessment been conducted to identify risks and evaluate the impact to business?

10 Known Audit Systems

10.1 SAS 70

Much of the information in this section is based on the American Institute of Certified Public Accountants (AICPA) audit guide entitled "Service Organizations, Applying SAS No. 70, As Amended".

10.1.1 SAS 70 Overview

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on effective internal controls at service organizations.

SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.

SAS 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report (see below). SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

SAS No. 70 is generally applicable when an auditor ("user auditor") is auditing the financial statements of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centers, Internet data centers, or other data processing service bureaus.

In an audit of a user organization's financial statements, the user auditor obtains an understanding of the entity's internal control sufficient to plan the audit as required in SAS No. 55, Consideration of Internal Control in a Financial Statement Audit. Identifying and evaluating relevant controls is generally an important step in the user auditor's overall approach. If a service organization provides transaction processing or other data processing services to the user organization, the user auditor may be required to gain an understanding of the controls at the service organization.

10.1.2 Service Auditor's Reports

One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2003). A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period (e.g. January 1, 2003 to June 30, 2003). The contents of each type of report are described in the following table:

Report Contents	Type I Report	Type II Report
1. Independent service auditor's report (i.e. opinion).	Included	Included
2. Service organization's description of controls.	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other information provided by the service organization (e.g. glossary of terms).	Optional	Optional

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.

In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

10.1.3 Benefits to the Service Organization

Service organizations receive significant value from having a SAS 70 engagement performed. A Service Auditor's Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of

effectively designed control objectives and control activities. A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).

Without a current Service Auditor's Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources. A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user auditor's requirements.

SAS 70 engagements are generally performed by control oriented professionals who have experience in accounting, auditing, and information security. A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

10.1.4 Benefits to the User Organization

User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls. The user organization receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

User organizations should provide a Service Auditor's Report to their auditors. This will greatly assist the user auditor in planning the audit of the user organization's financial statements. Without a Service Auditor's Report, the user organization would likely have to incur additional costs in sending their auditors to the service organization to perform their procedures.

10.2ISO 17799

10.2.1 Overview

ISO17799 is actually "a comprehensive set of controls comprising best practices in information security". It is essentially, in part (extended), an internationally recognized generic information security standard.

Its predecessor, titled BS7799-1, has existed in various forms for a number of years, although the standard only really gained widespread recognition following publication by ISO (the International Standards Organization) in December of 2000. Formal certification and accreditation were also introduced around the same time.

10.2.1.1 The Contents of the Standard

The ISO 17799 standard comprises ten prime sections:

1. Business Continuity Planning

   The objectives of this section are: To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

2. System Access Control

   The objectives of this section are: 1) To control access to information 2) To prevent unauthorised access to information systems 3) To ensure the protection of networked services 4) To prevent unauthorized computer access 5) To detect

unauthorised activities. 6) To ensure information security when using mobile computing and telenetworking facilities

3. System Development and Maintenance

   The objectives of this section are: 1) To ensure security is built into operational systems; 2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information; 4) To ensure IT projects and support activities are conducted in a secure manner; 5) To maintain the security of application system software and data.

4. Physical and Environmental Security

   The objectives of this section are: To prevent unauthorised access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.

5. Compliance

   The objectives of this section are: 1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements 2) To ensure compliance of systems with organizational security policies and standards 3) To maximize the effectiveness of and to minimize interference to/from the system audit process.

6. Personnel Security

   The objectives of this section are: To reduce risks of human error, theft, fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; to minimise the damage from security incidents and malfunctions and learn from such incidents.

7. Security Organisation

   The objectives of this section are: 1) To manage information security within the Company; 2) To maintain the security of organizational information processing facilities and information assets accessed by third parties. 3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer & Operations Management

   The objectives of this section are: 1) To ensure the correct and secure operation of information processing facilities; 2) To minimise the risk of systems failures; 3) To protect the integrity of software and information; 4) To maintain the integrity and availability of information processing and communication; 5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) To prevent damage to assets and interruptions to business activities; 7) To prevent loss, modification or misuse of information exchanged between organizations.

9. Asset Classification and Control

   The objectives of this section are: To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

10. Security Policy

The objectives of this section are: To provide management direction and support for information security.

Within these sections are the detailed statements and clauses that comprise the standard itself. In addition, the standard includes a Forward (setting the scene), a Scope, and a section defining various terms.

10.2.1.2 Certification and Compliance

The first step towards ISO 17799 certification is of course to comply with the standard itself. This is good security practice in its own right, but it is also the longer term status adopted by a number of organizations, who require the assurance of an external measure, yet do not wish to proceed with an external or formal process immediately.

In either case, the method and rigor enforced by the standard can be put to good use in terms of better management of risk. It is also being used in some sectors as a market differentiator, as organizations begin to quote their ISO 17799 status within their individual markets and to potential customers.

There is no doubt that ISO17799 in not going to disappear - far from it. Whatever your intention, however, it is hoped that this Directory will assist. You can directly acquire not only the standard itself or the accompanying introductory toolkit, but software to help with compliance, ISO 17799 aligned security policies, a risk analysis product (risk assessment is actually a basic requirement of the standard) and a number of other essential resources.

A. TRADING PARTNER AGREEMENT

An Example of s Trading Partner Agreement is shown below. This is relevant mostly in the confidentiality areas as well as relationship establishment.

****

Trading Partner Agreement

KANSAS ELECTRONIC DATA INTERCHANGE (EDI) PROJECT AGREEMENT

This is an agreement between the parties named below to use Electronic Data Interchange (EDI) technologies and techniques for the purpose(s) and objective(s) set out below or as amended from time to time in writing by mutual agreement and such further purposes and objectives as the parties may agree in writing from time to time with reference to this Agreement.

1. Parties. The parties to this agreement are: Kansas Division of Workers Compensation (hereafter KDWC); and _____ _ (Partner Company) and all other companies within the (Partner Company) authorized to write WC insurance or provide insurance related services (hereafter Reporter).

2. Purpose. Reporter is either required to file or may be allowed by law or regulation to file for itself or on behalf of customers or clients a First Report of Injury and Subsequent Report of Injury to the KDWC. The Objective is to initiate, implement and maintain First Report of Injury and Subsequent Report of Injury through electronic filing.

3. Both agree that the Objective is lawful and performance hereunder shall be deemed complete performance of the parties' obligations under any law or regulation governing the Objective. This document shall be deemed to fulfill any requirement on the part of the Reporter to apply to KDWC or any related governmental entity for permission to file information electronically.

4. Exhibit A, annexed and incorporated in this Agreement, sets forth the following mutually agreed elements of the arrangement between the parties.

a. The schedule form, including data element definitions, and format of the data transmissions from the Reporter, including original submissions and corrections or re submissions as needed (data transmissions).

b. The test and implementation plan and schedule under which the parties will prepare to send and receive data from each other.

c. The schedule, form, including data element definitions, and format of data transmissions from the KDWC, including acknowledgments, notices of error or notices of acceptance as applicable (data transmissions).

d. The Value Added Network (VAN) or other data transport method or carrier that will be used to transmit and receive data transmissions.

e. The allocation of data transmission costs between the parties.

5. Each party shall retain the content of data transmissions in confidence to the extent required by law.

Agreed this ____ day of _____ 20__, for the parties by their duly authorized or lawfully empowered representatives.

(signature) (signature)

(name) (name)

(title) (title)

Kansas Division of Workers Compensation

KANSAS Division of Workers Compensation [Exhibit A]

A.1. The Reporter and KDWC agree to use the national EDI standards for First and Subsequent Reports of Injury, Release I, established by the International Association of Industrial Accident Boards and Commissions, in any available format (i.e. flat file or ANSI X12).

B.1. The Project will commence with the transmission of the version of the First Report Injury defined per paragraph C3 below on _____. During the testing phase, the Reporter will be required to file paper forms in addition to the electronic transmission of records. Once the testing requirements are met, the Reporter will no longer be required to file paper forms with the KDWC. If the Reporter's customers are required to file a paper copy of the First Report, the KDWC agrees to waive the requirement for all reports made to the KDWC by the Reporter on behalf of its customers.

B.2. The parties will perform a test of the reporting system. The test will determine whether the transmission mechanism is acceptable. Acceptance will occur when the parties agree that 85% of all electronic first reports (a) meet or pass all technical requirements for the test period, which shall be no longer than four (4) consecutive weeks. The term of the test will not exceed 90 days unless an extension is agreed to between the parties.

C.1. The format of data elements and definitions will conform to the International Association of Industrial Accident Boards and Commissions (I.A.I.A.B.C.) data dictionary as it is today and as amended from time to time and approved by the I.A.I.A.B.C. or as otherwise agreed between the parties in writing.

C.2. The transmission of data will occur on of each week from the Reporter or as otherwise agreed and will be received by the KDWC within the following business week.

C.3. The data elements for the First and Subsequent Reports and their priority are found on the attached trading partner table. (Attachment 1) Additional tables for other reports and forms can become part of this agreement by mutual agreement between the parties.

C.4. Any error in transmission will be timely identified by the KDWC, but not greater than five (5) business days.

D.1. Transmission will be accomplished via the Value Added Network (VAN) or web as agreed between the parties from time to time.

E.1. The Reporter shall pay transmission cost for all reports being sent to the KDWC. KDWC shall not bear the costs of any transmissions to the Reporter; Reporter shall pay transmission costs for all reports sent by KDWC to the Reporter.

Kansas Trading Partner Profile Application and Confirmation Form

Form Data Entry Requirements: (M) Mandatory (C) Conditional (O) Optional

Purpose: [ ] Submit [ ] Change [ ] Delete Trading Partner

A. (M) Trading Partner Name:

B. (M) Trading Partner Type: [ ] Insurer [ ] Third Party Administrator

[ ] Self Insured Self Administrated

C. (M) In Production Status with other IAIABC State(s): [ ] No [ ] Yes

D. (M) Plan to use Kansas Web Claim Data Entry Option [ ] No [ ] Yes

(C) If yes ,anticipated annual claim volume: (C) Qualifying Reason:

E. Trading Partner (Sender) ID 1. (M) FEIN:

2. (O) TP 3 digit ID (If allowed by State):

3. (M) Postal Code:

F. Trading Partner Physical Address 1. (M) Street Address:

2. (M) City:

3. (M) State:

4. (M) Postal Code:

G. Trading Partner Mailing Address (If Different) 1. (O) Street Address:

2. (O) City:

3. (O) State:

4. (O) Postal Code:

H. EDI Business Contact Info. 1. (M) Name:

2. (M) Title:

3. (M) Phone:

4. (M) E-mail Address (preferred):

or Fax) Fax:

Complete Section I if using a Vendor's Data Entry Service or Web data entry EDI solution and skip J & K.

I. Vendor Information 1. (M) Vendor Name:

2. (M) Vendor Contact Name:

3. (M) Vendor Contact Phone Number:

4. (O) Vendor Contact E-mail Address:

Complete Section J if your Information Technology Staff operates your EDI system, or Imports or Exports Transactions to Client State.

J. EDI Trading Partner's Information Technology Contact Information 1. (M) Name:

2. (M) Title:

3. (M) Phone:

4. (M) E-mail (preferred):

or Fax:

Complete Section J if your organization controls the File Type or Network used.

K. EDI Communication Information 1. (M) EDI File Type: IAIABC Flat File R1 [ ] R2 [ ] R3 [ ]

ANSI 148/824 Version (3041) [ ] TBD [ ]

2. (M) Network: [ ] AT&T

[ ] Transmitter

[ ] Advantis Mailbox ID:

Account ID

Message Class:

Reporter's Trading Partner Transmittal Form

TO: State of Kansas

Department of Labor

Division of Workers Compensation

FROM: (Reporter Name)

(Reporter Attention Line)

(Reporter Address Street)

(Reporter Address City, State, Postal Code

Reporter Telephone Number

*Master FEIN: *Postal Code: Form ____ of ____

- See Instructions.

#	LEGAL NAME	FEIN
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		