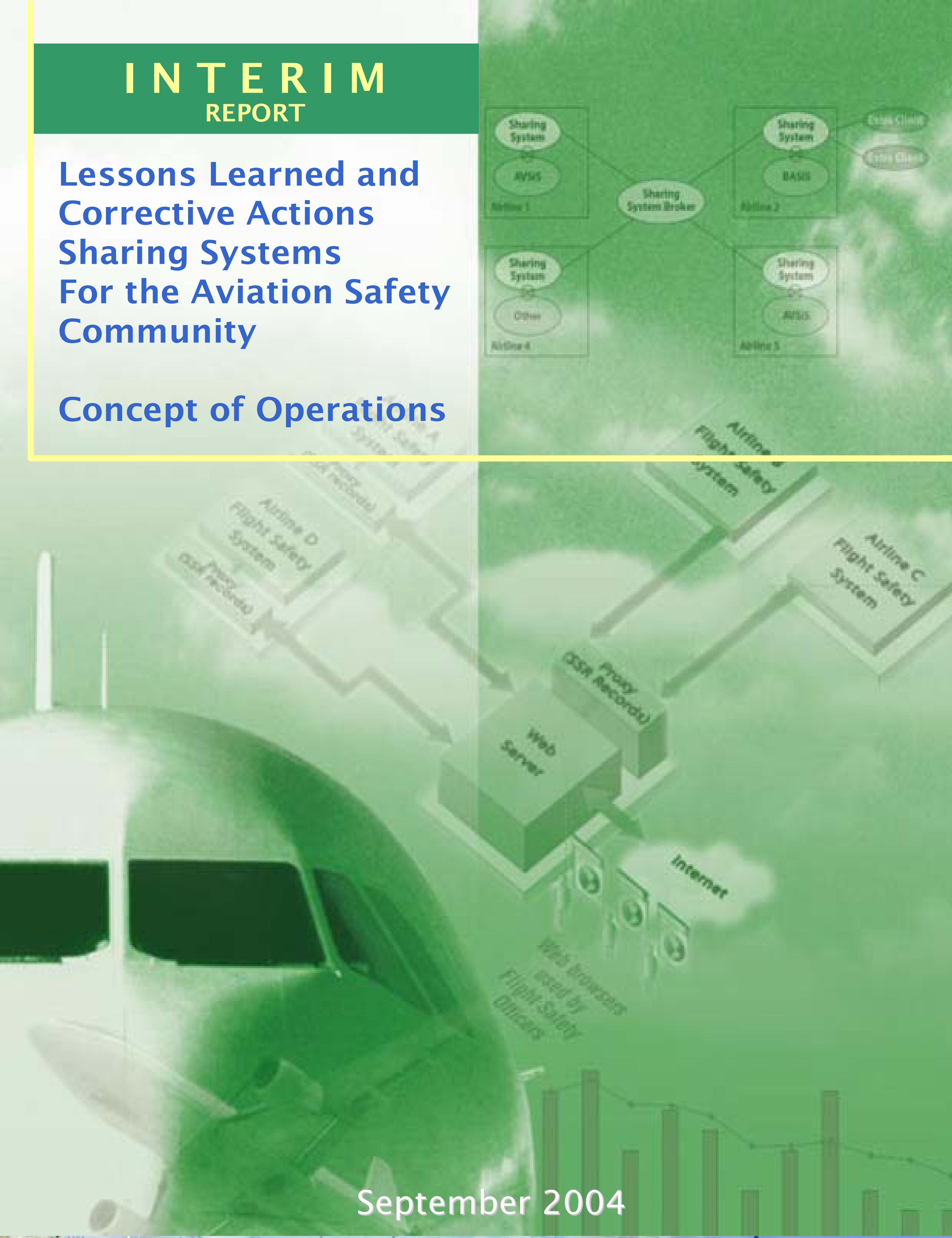
INTERIM
REPORT

Lessons Learned and Corrective Actions Sharing Systems For the Aviation Safety Community

Concept of Operations



September 2004

Global Aviation Information Network
ENHANCING AVIATION SAFETY THROUGH SHARING
GAIN

Lessons Learned and Corrective Actions Sharing Systems for the Aviation Safety Community

Concept of Operations

September 2004

Prepared by:

GAIN Working Group C

Global Information Sharing Systems

Disclaimers; Non-Endorsement

All data and information in this document are provided “as is,” without any expressed or implied warranty of any kind, including as to the accuracy, completeness, currentness, noninfringement, merchantability, or fitness for any purpose.

The views and opinions expressed in this document do not necessarily reflect those of the Global Aviation Information Network or any of its participants, except as expressly indicated.

Reference in this document to any commercial product, process, or service by trade name, trademark, servicemark, manufacturer, or otherwise, does not constitute or imply any endorsement or recommendation by the Global Aviation Information Network or any of its participants of the product, process, or service.

Notice of Right to Copy

Executive Summary

In 2002, members of the Global Aviation Information Network (GAIN) WG C identified the lack of a virtual global venue to share and exchange aviation safety lessons learned and corrective actions. The WG established Task C.3.a: Gather requirements for a system to share safety lessons learned and corrective actions [LL/CA] from a target user community. This purpose of this document is to report the requirements identified and propose a concept of operations.

The initial focus and scope for this task included flight operations and flight safety. A survey was sent to eleven airline flight safety officers to get their feedback regarding a system to share lessons learned and corrective actions. Furthermore, several informal interviews and correspondences were initiated to obtain further feedback and potential requirements. Along with the airline surveys and interviews, the WG turned to other industries and identified existing lessons learned and corrective action systems. Once the existing systems were identified, the WG documented their capabilities. With this list of capabilities, the WG identified several functional and operational requirements that would be applicable to an aviation safety LL/CA System [LL/CAS]. Lastly, to aid in the requirements gathering process, a Web-based application was developed and entitled “Requirements for a Prototype System for Sharing Safety Lessons Learned and Corrective Actions within the Aviation Community.” This proposed Concept of Operations (CONOPS) document, derived from the information gathered during these tasks, serves as a basis for a functional requirements document.

Acknowledgements

The following WG C participants were primarily responsible for the preparation of this document:

- Warren Randolph, FAA Office of System Safety
- Kevin Rodriguez, FAA Office of System Safety
- Ron Lee, Oak Ridge National Laboratory
- Simon Rose, Oak Ridge National Laboratory

WG C participants and others who contributed their ideas and comments or who assisted in the collection and documentation of requirements for an Aviation Safety Lessons Learned and Corrective Actions System are as follows:

- Dave Briles, FAA Office of System Safety
- David Fuller, Transportation Safety Board, Canada (Retired)
- Howard Posluns, Transport Canada
- Dennis Rowley, Independent Aviation Consultant
- Andy Muir, FAA Office of System Safety
- Tom Curran, Manager, Air Safety, Aer Lingus
- Geoff Gosling, Aviation System Planning Consultant
- Grant Schneeman, RS Information Systems, Inc.

Table of Contents

Acronyms

AAA	Authentication, Authorization and Accounting
ASAP	Aviation Safety Action Program
ASRS	Aviation Safety Reporting System
CA	Corrective Action
CALL	U.S. Navy Combined Automated Lessons Learned
CALL	U.S. Army Center for Army lessons Learned
CAST	Commercial Aviation Safety Team
CONOPS	Concept of Operations
IATA	International Air Transport Association
FAA	Federal Aviation Administration
FOQA	Flight Operations Quality Assurance
GAIN	Global Aviation Information Network
ICAO	International Civil Aviation Organization
IETF	International Engineering Task Force
LL	Lessons Learned
LL/CAS	Lessons Learned and Corrective Actions System
LLIS	Lessons Learned Information System
NASA	National Aeronautics and Space Administration
OPIS	Operational Performance Information System
ORNL	Oak Ridge National Laboratory
PDF	Portable Document Format
PEAT	Procedural Event Analysis Tool
SELLS	Society for Effective Lessons Learned Sharing
SME	Subject Matter Expert
STEADES	Safety Trend Evaluation and Analysis Data Exchange System
SWAP	Safety with Answers Provided

1. Introduction

1.1 GAIN Work Group C

GAIN is an industry and government initiative to promote and facilitate the voluntary collection and sharing of safety information by and among users in the international aviation community to improve safety. GAIN was first proposed by the Federal Aviation Administration (FAA) in 1996, but has now evolved into an international industry-wide endeavor that involves the participation of professionals from airlines, employee groups, manufacturers, major equipment suppliers and vendors, and other aviation organizations.

The GAIN organization consists of an industry-led Steering Committee, three work groups, a Program Office, and a Government Support Team. The GAIN Steering Committee is composed of industry stakeholders that set high-level GAIN policy, issue charters to direct the work groups, and guide the program office. The Government Support Team consists of representatives from government organizations that work together to promote and facilitate GAIN in their respective countries. The work groups are interdisciplinary industry and government teams that work GAIN tasks within the action plans established by the Steering Committee. The current GAIN work groups are: Work Group B – Analytical Methods and Tools, Work Group C – Global Information Sharing Systems, and Work Group E – Flt Ops/ATC Ops Safety Information Sharing. The Program Office provides technical and administrative support to the Steering Committee, work groups, and Government Support Team.

GAIN Work Group C (WG C) was chartered by the GAIN Steering Committee in January 1999 to “promote and facilitate the development and implementation of systems to support the global sharing of aviation safety information.” The Steering Committee has assigned three focus areas within the GAIN Action Plan to WG C to help accomplish that mission:

C.1 Facilitate the development of systems to share airline safety event information among trusted groups.

C.2 Promote aviation industry sharing systems.

C.3 Facilitate the development of a system to share safety lessons learned and corrective actions within the aviation community.

1.2 Background

The subject of this document is subtask C.3.a, “Gather requirements for a system to share safety lessons learned [LL] and corrective actions [CA] from target user community”, and is focused on flight operations safety. The primary goals are: (1) improve aviation safety, (2) reduce or eliminate repetitions of safety related problems, and (3) increase and improve information sharing amongst aviation industry organizations, individuals and other aviation entities. The intent is to develop and foster an environment to share lessons learned and corrective actions with other members within the aviation community.

The rationale for the system is that aviation accidents and incidents continue to occur, information sharing is usually anecdotal and not business-as-usual, and currently there is no single source of LL/CA information for the aviation community.

This document is a Concept of Operations (CONOPS) report, which serves as a basis for describing the functional concept of a new or revised system process. The intent of this report is to describe the services that will be provided by the new system including information describing functionality, information and/or data, environment, and constraints. his is completely independent of technology platforms, systems development methodologies, and environmental infrastructures. The next step in the development of a specific system implementation would be the completion of a formal functional requirements analysis and functional requirement specification. The functional requirements specification contains the details of data and information content, reports contents, process flows of each required function and report, access rights, and user interfaces.

1.3 Knowledge Artifacts

> *A knowledge artifact is a defined piece of recorded knowledge that exists in a format that can be retrieved to be used by others. A process drawn on a napkin at lunch can become a knowledge artifact if it can be recorded for someone else to use. Typically artifacts are something more tangible – i.e. a document, a picture or graphic, a video, an audio, a project plan, a presentation, a template … to name several.*
>
> *Artifacts are typically recorded by business units and for specific business functions. These artifacts are of certain types, and fall into different classes. These basic pieces of information…about artifacts along with the steward meta data are the beginnings of a knowledge taxonomy that can be developed and used to classify and record every piece of recognized knowledge…and enables the company to name and classify the knowledge...it becomes possible to search for and identify the knowledge that exists, and retrieve the knowledge when it is needed.*[1]

Lessons learned and corrective actions are forms of knowledge artifacts. What one user may consider a valuable lesson learned another may consider inconsequential or non-relevant information. It is critical to establish a common understanding as to what type of information (i.e., knowledge artifact) is a candidate for sharing using this system.

Through a literature search, the working group identified a paper that helps describe the varying levels of knowledge artifacts as they pertain to a lessons learned systems. In the paper, *Intelligent Lessons Learned Systems*, a table is used to describe the characteristics of each of the knowledge artifacts.[2] The WG found this table to be very useful in helping 1) identify the characteristics of lessons learned and 2) distinguishing the differences in lessons learned artifact from other knowledge artifacts that are common in the aviation safety community. A copy of the table is found below. For the purpose of this work, the table has been modified based on inputs from industry members of the WG to support the subject matter relevant to the aviation industry. Definitions for each type of knowledge artifact follow the table.

Artifact Type	**Culmination of multiple organizational experiences**	**Describes a complete process**	**Describes failures**	**Describes Successes**	**Describes a corrective action**	**Orientation**
Lessons Learned	Yes	No	Yes	Yes	Possibly	Organization
Incident Reports	No	No	Yes	Yes	No	Organization
Alerts	Possibly	No	Yes	No	Yes	Industry
Corporate memories	Possibly	Possibly	Yes	Yes	Possibly	Organization
Best Practices	Possibly	Yes	No	Yes	Possibly	Industry

Table 1-1 Knowledge Artifact Attributes

[1] Seiner, Robert S. (2001), Meta Data as a Knowledge Management Enabler. The Data Administration Newsletter (TDAN.com)

[2] Weber, R., Aha, D.W., & Becerra-Fernandez I. (2001). Intelligent lessons learned systems. International Journal of Expert Systems Research & Applications, Vol. 20, No. 1.,17-34

The following definition for a **lesson learned** is currently used by several space agencies around the world, including NASA.[3] This definition will be used for the purpose of this work:

> *"Understandings or knowledge gained by experience. The experience may be positive, as in a successful test or mission, or negative as in a mishap or failure. Successes are also considered sources of lessons learned. A lesson must be significant in that it has a real or assumed impact on operations; valid in that is factually and technically correct; and applicable in that it identifies a specific design, process or decision that reduces or eliminates the potential for failures and mishaps, or reinforces a positive result."*

An example of a lesson learned might be the proceedings from a flight data monitoring program study that was conducted by an individual operator. Lessons learned can be shared amongst parties that have a vested interest in ensuring that positive experiences are repeated and while avoiding the recurrence of negative experiences.

The Society for Effective Lessons Learned Sharing (SELLS) established guidance for establishing a process to determine if a knowledge artifact is first a lesson learned and then is suitable for sharing. Note that sharing assessments are made for every participating group based upon: their level of trust, an internal or external organization, and operational responsibilities. SELLS outlines the following steps as a beginning framework that can be suited to individual programs.[4]

1. Does the lessons learned information reference work activities similar to those performed onsite?
2. Does the site have procedures in place to control the activities described in the lessons learned information?
3. Do the procedures address the hazards identified in the lessons learned information?
4. Can the safety, efficiency, or cost-effectiveness of site activities be enhanced through the integration of the lessons learned information into the activities, work planning processes, or training?
5. Has the site experienced any adverse events as a result of these work activities?
6. Does the lessons learned information reference hazards found onsite? (e.g., industrial, environmental, or radiological)
7. Does the site have procedures in place to control the hazards described in the lessons learned information?
8. Can the site's hazard controls be enhanced through integration of the lessons learned information into procedures, work activities, or training?
9. Has the site experienced any adverse events as a result of these hazards?
10. Does the lessons learned information pertain to equipment used on site?
11. Can the safety or efficiency of site equipment be enhanced through application of the lessons learned information to the equipment design or utilization?
12. Have site personnel experienced any equipment malfunctions or accidents while using the equipment?
13. Does the lessons learned information reference a politically sensitive issue or event that does not directly pertain to site activities?
14. Could the lessons learned information impact the public's attitude toward site activities?

Table 1-2 SELLS Lesson Assessment Guidelines

WG C refers to the International Organization for Standardization definition of **Corrective Actions**:

> *"A Corrective Action is a deliberate action to eliminate the cause of a detected nonconformity or other undesirable situation."*

[3] GAO-01-1015R Survey of NASA's Lessons Learned Process
http://klabs.org/DEI/lessons_learned/GAO_Report/GAO_NASA_Lessons_Learned_d011015r.pdf

[4] Society for Effective Lessons Learned (2003), Fact Sheet: Screening Lessons Learned for Site Applicability
http://www.eh.doe.gov/ll/sells/faqs/sitescrn.pdf

Corrective actions are therefore steps that are taken to remove the causes of an existing nonconformity or to make quality improvements. A correction would be any action to eliminate a detected nonconformity. Corrective actions are a logical follow up to a lesson learned from a failure.

Incident Reports describe unsuccessful experiences. An incident report lists arguments that explain the incident without posing recommendations. Examples of an incident include Accidents and ASRS entries.

Alerts are reports of problems experienced with a particular technology or a part that is applicable to organizations in the same industry. Examples include the ASRS Alert Bulletins as well as U.S. Airworthiness Directives.

The common understanding of a **corporate memory** typically implies the set of knowledge gathered by one or more employees with respect to the activities of the company. The following excerpt provides a more robust definition from the field of knowledge management.

> *There is an increasing industrial interest in the capitalization of knowledge (i.e. both theoretical knowledge and practical know-how) of groups of people in an organization, such groups being possibly dispersed geographically. The coherent integration of this dispersed knowledge in a corporation is called "corporate memory" (Steels, 1993). The memory of an enterprise includes not only a "technical memory" obtained by capitalization of its employees' know-how but also an "organizational memory" related to the past and present organizational structures of the enterprise (human resources, project management, etc.)*[5]

Best Practices describe previously successful ideas that are applicable to organizational processes. Lessons learned include failures within the operating environment for the purpose of gaining knowledge to avoid recurrence.

This document focuses on Lessons Learned. Although each of these Knowledge Artifacts merits investigation, lessons learned were deemed to have the best potential to benefit aviation safety through sharing. Although corporate memories and best practices could also prove beneficial, these items are often not documented or considered proprietary that cannot be disseminated outside controlled groups.

1.4 Project Methodology

Development of the concepts presented in this document was accomplished through several interview and survey activities including:

- Primary research comprised of a survey of available literature was conducted to collect best practices for a Lessons Learned management program.
- Discussions with other Lessons Learned system owners to benefit from their experiences.
- WG C discussed and formulated its own set of requirements resulting from the research findings.
- Survey – In 2002 GAIN Working Group Members interviewed managers and personnel from seven airline flight operations departments by telephone and email. A summary of these interviews was prepared under the leadership of Lee Nguyen in a GAIN document in April 2002[6].

[5] Rose Dieng, Alain Giboin, Christelle Amergé, Olivier Corby, Sylvie Després, Laurence Alpay, Sofiane Labidi, Stéphane Lapalut (1996), Building of a Corporate Memory for Traffic Accident Analysis. Proceedings from the 1996 University of Calgary Knowledge Acquisition Workshop Series http://ksi.cpsc.ucalgary.ca/KAW/KAW96/dieng/dieng-kaw96.html

[6] Survey of Lessons Learned and corrective Actions Sharing System for Airline Flight Safety Management, ORNL Summary Report, April 2002.

- Interview – Airline flight safety officers were interviewed during site visits in coordination with GAIN WG B.
- A Web-based application was developed by ORNL and entitled "Requirements for a Prototype System for Sharing Safety Lessons Learned and Corrective Actions within the Aviation Community."

  The primary purpose of the Web-based application was to gather requirements. Access to the Web site was password protected and was only provided to Task C.3.a participants including airline flight safety professionals that participate in the GAIN Program. A secure port has been added to the application that may be accessed by authorized users at the URL below. Functionality includes approved reviewers being able to review LL/CA submissions and either accept or reject each pending record. A system primer with screen shot is available.

  In June 2003, the GAIN VI Conference was held in Rome, Italy. At this conference flight safety personnel from different airlines were approached regarding the GAIN LL/CA project. Flight safety personnel from five airlines indicated a willingness to share LL/CA and so in July 2003, these individuals were provided password protected access to the secure Website with 'review' and 'add' user privileges. A draft document untitled, "User Guide for Web-Based Requirements Gathering Application" was also provided. Positive feedback was given and also recommendations for minor enhancements *(list minor enhancements)* to the prototype was received and implemented. In addition sample LL/CA records were added to the prototype by the airline flight safety staff. The Web application was also reviewed by members of the Work Group C. Ongoing enhancements at the time of this report include development of additional wizard functionality to assist users with data capture and survey questionnaire regarding use of the Web application.

As discussed earlier in this report, the first phase of this task included surveys, interviews, meetings, research and discussions to identify initial requirements for this system. Upon completion of this phase, it became apparent that a functional prototype needed to be built to elicit further requirements – a straw man to aid potential users in conceptualizing the LL/CAS. The requirements identified in the first phase served as the basis for the development of the web-based prototype – Task C.3.b. With this prototype, the working group has been able to demonstrate a functional LL/CAS to several potential users, get their feedback and document further requirements. As time and resources permitted, newly identified requirements were integrated into the functional prototype.

1.5 Report Content

The CONOPS document is to describe high-level requirements, which provides a mechanism for users to describe their expectations of the system. The CONOPS is used as input to the development of a formal testable system and software requirements specifications. The objective of a CONOPS therefore is to capture the results of the conceptual analysis process. Such a document will have general characteristics that:

- Describes the envisioned system
- Identifies the various classes of users
- Identifies the different modes of operation
- Clarifies vague and conflicting needs among users
- Prioritizes the desired and optional needs of the users
- Supports the decision-making process that determines whether a system should be developed
- Serves as the basis for the Functional Requirements Document.

2. Requirements

2.1 Information

A Data Requirement (DR) is best described as an essential piece of information that is used to populate the system. The concept of operations is not intended to examine detailed requirements. At a higher level of abstraction, understanding the information that users expect to get from the system is important in describing the purpose of a system. This document refers to these items as Information Requirements (IR).

ID	Description
IR-1	Participation Agreements – Participating airlines must adhere to the strict guidelines set forth in the letter of agreement to voluntarily participate. Participation in the sharing system must be based upon mutual understanding and trust. Memoranda of Understanding (MOU) must be signed by authorized representatives from every participant, including system vendors and/or administrators. Even though some records may provide information to identify the source, it is still up to the participants to comply with the existing MOU. Publication or making public of any information that is correlated to a source will normally be a violation. MOU terms are determined by the participants. It should be possible to immediately suspend or terminate the participation of violators.
IR-2	Just Culture – System data must not be used for investigation or enforcement action of any kind, against the information provider or any company. This condition must apply to both regulators and industry.
IR-3	Lessons Learned Repository – The system must store and provide access to safety lessons learned and corrective actions. This is the fundamental purpose of the system. The content of the system must conform to the definitions for lessons learned and corrective actions as described in section 1.3.
IR-4	Policy – Formal policies will be used to establish formal procedures for data quality, data security, dissemination, and de-identification.
IR-5	De-Identification - All identifying attributes must be removable from records prior to sharing outside of the originating organization. De-identification pertains to the removal of all descriptive information that could allow others to identify the information source. There can be no single source that is responsible for de-identification. The responsibility lies with the information provider. If any information is contained in a record that enables source identification, all users can assume it is based on the decision of the provider.
IR-6	Data Possession – Proprietary data must remain in the hands of the owner. Data providers insist upon full control of their information. This requires that information be distributed to provide the ability for each participant to retain possession and control of its data.

ID	Description
IR-7	Program Source – Relate Aviation Safety Action Program (ASAP) and FOQA information. Include pilot anecdotal information behind the objective FOQA data. Relate FOQA data to maintenance information in maintenance logs.
IR-8	Content – Types of data and information to be stored or referenced in the system include: operating safety, training, regulatory compliance, operational issues associated with specific airports and air traffic control, NAS, checklist procedures, specific aircraft system discrepancies, company size, type of operation, and issues with regulatory policies and procedures. All values associated with standard fields, required or optional, is text. This includes selection of standard codes and values. Clearly, a lot of LL/CA information exists currently in some format and medium, and there are automated systems in place which produce such data. A mechanism for capturing or referring to these resources is necessary. Further, concerns over data ownership and management may dictate what data and information a source organization may be allowed to, or may desire to store within an externally managed LL/CA Sharing System. In order to meet these needs, each LL/CA record will include links and attachments. A link will be specified as a URL, likely using the familiar *http* scheme referencing a document or resource available on a Web server, perhaps owned by the source organization. Maintenance of the document or resource targeted by the URL will be the responsibility of the organization submitting the LL/CA record. Documents and resources which the submitting organization is allowed to, or prefers to store within the LL/CA Sharing System may be specified as attachments and uploaded into the system. The distinction between links and attachments is the location of the resource, either external to the LL/CAS for links, or stored within the system for attachments. The contents of all links and attachments will be included in free text searches, provided the format of the resource is supported. Supported formats will include Microsoft Office documents and Adobe Portable Document Format (PDF).
IR-9	Data Sources – Information stored in the system should be well-documented recommendations by the airlines for experienced incidents and the associated corrective actions. Sources of information should include safety-related incidents, knowledge gained from some FOQA analysis and ASAP analysis, pilot experiences, ASRS, FAA database systems, information sent to airline directors of safety, lessons learned identified by training and safety departments, hazard reports, incident and accident reports, airfield audits, safety ramp audits, and internal audit results from the Internal Evaluation Program.

ID	Description
IR-10	Classification – Data categorizations must include aircraft types, types of flight operations, carrier size, etc. Records in the system will include a defined standard set of fields organized within defined categories. These metadata are themselves integral system data and will describe categories and fields, identifying fields which are required for each record. There will be a *text* field for storing a prose description of the event. However, information in a record will not be limited to the defined fields. Additional information may be captured and assigned a field, and ad hoc fields will be as searchable or browse-able as standard fields. Thus, the definition of a record is not static but is dynamically extensible to include additional information, field assignments, and categorizations as determined by the author or source of the data. When and where appropriate, fields will employ existing industry standards such as categories provided by ADREP 2000 (including ECCAIRS 4 descriptive factors based on ICAO's ADREP 2000 taxonomy) and the results of the CAST/ICAO Common Taxonomy team. Metadata for each field will specify whether or not its value is limited to a standard value or code. With such a wide range of potential data sources and subject areas, it is necessary to account for two extremes in styles of data and records which may lie somewhere in the continuum the extremes. At one extreme is a completely categorized record in which values for all standard fields are provided. Note a data browse capability, described below, will be based on values of these standard fields. Thus, a completely categorized record will be easily identified when a user browsers for LL/CA records. At the other extreme is a completely free form record, where only the required fields are provided in addition to a free text description of the event, its associated lesson learned, and any associated corrective actions. Note such a record will only be identified in a search operation. As described below, a search is a word or phrase search in the free text for records. The free text is accumulated from the values of all the record's fields.

2.2 Functionality

This will be an automated system for sharing safety related lessons learned and corrective actions among airlines and other organizations in the commercial aviation industry. Functional Requirements (FR) for the system revolve around the fundamental functions of storing, sharing, and managing lessons learned and corrective action data and information. Basic functions will support entry, edit, and removal of data. The system will include procedures for review of new or modified data. Further, the system will assist users in finding relevant data in two ways, by browsing for records with values for defined fields, and by free text searches.

ID	Description
FR-1	Content and Features – The focus or target users for the system will be airline directors of safety.
FR-2	User Console – Users will work from a single console that provides all authorized functionality.
FR-3	Lesson Management – Users will be able to manage lesson records including record entry, edit, deletion, and approval processing. Specific mechanisms will be provided for authorized users to enter new LL/CA records, edit or update existing records, and remove existing records. At least two methods for entering new data will be provided, one oriented to quick entry of data with little categorization (simple form), and another oriented to a more detailed or highly categorized record (full form). Additional data acquisition methods, such as a guided wizard could prove useful as well. Another area in which the wide variety of data sources and subject matters must be accommodated is data quality. Some users of the LL/CAS prefer a bulletin board where all information posted is accessible without any review. Others only want to see data that has been quality controlled via review by one or more domain experts. Thus, records must be tagged as either reviewed or not reviewed, and the user will have the choice of seeing either or both kinds of records when browsing or searching. A review process involving subject matter experts will be supported in the system. Only authorized reviewers (i.e., authenticated users who have been assigned the *reviewer* role) will have access to functionality for reviewing records. The status of a review will include a complete rejection, a request for more information or clarification from the author, and an acceptance. Note the notification capabilities of the system, described below, will add authors and reviewers in the workflow associated with the review process and obtaining the status of a review.

ID	Description
FR-4	Lesson Retrieval – Users must be able to query and sort via a user-friendly search engine. Resultant record lists will include drill-down capability to view lesson details. Browsing is a structured approach to identifying records of interest. Following a "query by example" metaphor, a browse screen will allow the user to enter or select values of each defined, standard field and will closely resemble the full form for categorized data entry. The rules for selecting from standard field values or codes will apply to the browse form as well. As values for one or more fields are entered, the user can choose to see the number of records with values meeting those supplied on the browse form. The user may continue to refine the set of selected records, culling undesired ones by entering values for more fields. When the user is satisfied with the browse selection, he/she may view a list of the selected records, as described below. After a browse or search, the user will be presented with a list of selected or matching records, if the operation is not canceled. The list will include record titles and any other (required) field values needed to distinguish the records. Any subset of the records (including all of them) may be tagged or selected for display. Records selected for display will be presented in a page. All fields for which values are stored in a record will be displayed for each selected record. The page will include navigation controls to go from a table of contents listing the records to and from the display of individual records.
FR-5	Translation – Include translation support for English and non-English speaking airlines.
FR-6	Data Mining - Provide data mining tools to facilitate easy query of useful information. A free text search capability will be provided as an alternative means of identifying records of interest. This models familiar Internet and Web searches with tools such as Google. All values of all fields associated with a record, including the *text* field, are included in the search. The search engine will include enhanced or advanced capabilities such as word proximity searches and alternate and repeating words. A search will result in a list of the matching records available for viewing.
FR-7	Trend Analysis – Trend graphing/charting can be done using various dimensions supported by the existing data set. The system will include agents that perform analysis such as identifying trends in incident data. Examples of such trends are identification of airspace issues at specific airports, problems with specific aircraft systems, and operational problems in general.
FR-8	Supports Aviation Safety Analysis – Analysis tools will support identification of airspace issues at specific airports, issues with specific aircraft systems, and operational problems.

ID	Description
FR-9	Automated System Messaging – The system should automatically disseminate periodic safety summaries to airline users. An important feature of the LL/CA Sharing System will be automatic notification by email of significant events. Notification events will include submission of a new record, modification of an existing record, and review of a record. A new or modified record may result in two kinds of notification. First, each record submission (new or modified) will result in notification of domain experts registered in the system as reviewers. Second, users may register to be notified upon submission and/or reviewed acceptance of records matching free text search criteria. Each record submission or review will be accompanied with a comparison of the record against all notification match criteria with subsequent notification of registrants as matches occur. Data entry and/or modification will include a field in which the submitter may enter an email address for notification upon review. When the record is reviewed by an authorized reviewer, the status of the review will be sent to the submitter if a notification address has been provided. Notifications associated with the review process will greatly improve the timeliness of the workflow and collaborations involved.
FR-10	User Message Brokering – For de-identified information, the system should provide a message board to allow the receiver to request follow-up information.
FR-11	Interview Approach - Employ the use of ‘Wizard’ technology to aid the user in submitting a lesson learned or corrective action artifact.

2.3 Users

User Requirements (UR) will come from two sources: airlines and system operations. Airlines users will always be associated with their airlines as a means of determining their access rights.

ID	Description
UR-1	User Classes – Users will be assigned to classes based upon their job responsibilities.
UR-2	Levels of Trust - Provide information sharing in multiple, progressively increasing levels of sharing capabilities and “trust”.
UR-3	Custom Configuration – Allow participating airline pairs to configure custom data access profiles.
UR-4	Access – Civil Aviation Authorities will not have access to or control of the lessons learned and corrective actions sharing process.

2.3.1 Classes

The following list summarizes the categories of user classes for the LL/CAS:

- Viewer – A users that can only query, browse and use analysis tools. This user may not alter the database in any way.
- Submitter – A staff member who coordinates the documentation of new lessons and can submit records. A submitter can edit only records entered by himself/herself.
- Reviewer – A subject matter expert [SMEs] assigned the role of review and approving new entries and edits. Reviewers can edit, review, and approve records submitted from their airline.

There is also a group of user classes responsible for system management with rights typical of these roles.

- System Administrator
- Database Administrator (DBA)

User Class	Query & Analysis	Enter & Edit	Review & Approve
Viewer	X		
Submitter	X	X	
Reviewer	X	X	X
System Administrator	X	X	
DBA	X	X	

Table 2-1 Capabilities by User Class

2.3.2 Levels of Trust

Airline safety officers establish professional and personal relationships through existing industry events. Many current information sharing activities are based upon these pre-existing relationships. There exists a level of professional respect and trust. Access to information will be managed via defined levels of trust. When there is a new participant in a lessons learned sharing implementation, they will be assigned a predetermined level of trust. The level will determine what information the user can access. Since even new participants will have pre-existing relationships, the trust level will be a local setting that is coordinated with the system administrator. Users can be categorized into one of the following example trust levels.

Trust Level	Description
Internal User	Shared information will be controlled locally within the distributed data store. Local users will all be recognized as such and be given access to all lessons within the local data set. Individual lessons may contain sensitive information necessitating access restricted to select users, even within an organization. Trust level attributes will be used to determine these rights.
Trusted External User	In many cases, users will have pre-existing relationships garnering higher greater trust. Trusted external users will benefit the most out of the sharing activity by receiving greater access to information.
External User	Most sharing relationships will evolve to this level of trust when there is no other existing relationship. Limitations will be based upon the information attributes present in the data store.
New External User	New users are individuals who are new participants to the sharing system. They are external to the local environment (i.e., they are from another airline). Rights may exclude permission to use analysis, trend, and mining tools.
Excluded User	In some cases, individual users or users from specific airlines may need to be excluded from segments of the database. This may include individuals who are from specific competitors or have proven themselves to be untrustworthy.

Table 2-2 Example Trust Levels

2.3.3 Custom Configuration

Individual users may consider applying custom rights to users. For example, a highly trusted colleague might be given rights to see information that is blocked as part of the de-identification process. Other rights might include custom configuration of access rights based upon stored information attributes. In this fashion, a user could be given rights to see lessons that would otherwise be blocked from the viewing. Custom configurations will have attributes for the following:

- Attribute or field level rights. This will allow users to be assigned rights to restricted fields. Reductions in field rights will also be possible.
- Record selection rights. Rights will be based upon record attributes such as subject matter (e.g., catastrophic accidents) and sensitivity (e.g., competitive advantage).
- Analysis rights. In some cases it may be necessary to exclude records that can be included in data sets used for analysis by external users. This will prevent others from completing a trend analysis that could prove to be disadvantageous to the data originator.

2.3.4 Access

The Lessons Learned and Corrective Actions system is intended to service the airline industry. To protect the individual airlines, Civil Aviation Authorities will be excluded from accessing the system and the databases.

3. System Requirements

3.1 Operations Requirements

Regardless of functionality, there are many requirements an operational system must meet in order to provide adequate security and control. This section identifies key operational requirements for LL/CAS.

The system is intended to be easily accessible to the range of potential users acting in the various roles established. The level of accessibility envisioned is such that the user will not need to install a specific set of software associated with the client, such as a client application. Rather, the Web application model where the user tool is a browser, and all data and control is downloaded from a Web server is the desired operational paradigm.

ID	Description
SR-1	The system must index proprietary data maintained on systems belonging to the information owner and provide access or retrieval of that data from the owner's network-accessible systems.
SR-2	The system must be simple, user-friendly, easy, readily available, and inexpensive to operate.
SR-3	The system should include a Web-enabled database application containing categorized information.
SR-4	The organization operating and maintaining the system must have no direct interest in the outcome other than sharing of safety information.
SR-5	The system must provide information in a timely manner such that the information is communicated to those who can use it before it loses value.

3.1.1 Distributed Architecture

Information owners must maintain possession of their data at all times. This necessitates the decentralization of data stores. Information owners will have the right to restrict or discontinue access based upon prevailing environmental conditions (e.g., legal proceedings, security breaches, or catastrophic events).

3.1.2 System Environment

The most prominent aspect of the system environment is the assumption of network connectivity, both for the application server and the user. The LL/CAS will be Web-based, and lack of network connectivity will preclude access to the system.

3.1.2.1 Application Server Environment

One or more servers will be required to host the Web application itself and DBMS for data storage. Data exchange among these hosts will require a network with a fairly high bandwidth. Given the inexpensive technologies which exist today, the local area network shared by the various server hosts should support 100 megabit per second Ethernet at a minimum.

Moreover, the application server will be accessible via the Internet. This will require a firewall host of some sort connected to the local area server network. At a minimum, the capacity of the internet connection should match commercial broadband technologies available today supporting as much as one gigabit per second throughput.

3.1.2.2 Client Environment

No assumptions are made regarding the platform on which the client runs with two exceptions. First, the client must use a browser supporting the HTML 3.2 (or later) standard. Second, the client must have an Internet connection. The minimum assumed connection is a dial-up modem supporting 33 kilobits per second. There is no limit on the speed of the client's Internet connection, as latencies in the various routers and switches off the Internet backbone will be the constraints on network performance regardless of the client's connection speed.

3.1.3 System Ownership

The system must be owned and maintained by an independent, non-regulatory organization with no vested interested in the content of the data and information stored in the system. Examples of qualifying government organizations would include NASA and the DOE National Laboratories. A commercial organization outside the aviation industry and specializing in information processing and/or Web application hosting would also qualify.

3.1.4 Performance

Although the LL/CAS would not classify as a "mission critical" resource for emergency or real-time operations, there are still performance requirements the system must achieve. Generally, the system should provide "24-7" operation or availability 24 hours a day, seven days a week. Exceptions for hardware failure and system upgrades should not exceed two to four hours of down time. If necessary, redundant fail-over systems must be available to ensure system availability within a six hour period.

At least two dozen simultaneous connected users must be able to access the system without highly degraded system response. It is not anticipated that all users will perform submissions and/or searches simultaneously and expect the same response as a single operation. However, submission time in the system (i.e., ignoring network connection speeds) should not exceed 30 seconds even if 24 users are submitting simultaneously. Search times are highly dependent on the volume of data and the nature of a search. Typically, searches should return within 10 seconds. In a highly loaded situation with 24 users actively using the system, searches should still complete within a minute. Browse operations should respond within a couple of seconds in normal operation and should never exceed 20 seconds, even under high loads.

Scalability is a critical system requirement. It must be possible to add additional processors or server boxes to improve performance and/or support additional users. Further, the additional performance number of users supported with the addition of server boxes should be close to a linear scale up to eight servers and should never fall below a 50% improvement for an additional box up to 16 servers.

Data downloads to a user's computer will always be highly dependent on the speed of his/her network connection. However, each Web page either generated or statically prepared, loaded as part of the application should load across a 33 kilobits per second modem connection within 15 seconds.

With the decreasing cost of hard drive storage media, constraints on system capacity are not likely. Nonetheless, the system must be capable of storing one million records plus attachments, and the system must be capable of indexing and searching all the data stored within the system and linked to data owner systems.

3.2 Platform Security

One of the most prominent requirements for a LL/CA Sharing System stated by interviewees is the need for de-identification of all data. This is merely one of many requirements related to system security. Enumerated below are explicit security requirements followed by a brief overview of existing technologies which may be applied to meet these requirements.

Ultimately, the goal of system security is to secure information related to an organization. Principal components of security are authentication and authorization, with encryption via integrity and auditing added for good measure.[7] The Authentication, Authorization and Accounting (AAA) working group of the International Engineering Task Force (IETF) is "focused on the development of requirements for Authentication, Authorization and Accounting as applied to network access."[8] These are the foci for IETF standardization efforts related to security.

3.2.1 Authentication

Authentication is the process by which users verify they are who they claim to be. Clearly, authentication is a requirement for any system wishing to control or limit access in any way via user identification. The most common authentication mechanism is for the user to supply some known secret, such as a password. Exchange of secret information is only secure if that information is not transmitted in clear text over a network connection. That is, any exchange of secret information must be protected by encryption.

There are ways of increasing the strength (in terms of security) of the authentication process. An example is a hardware authentication token which generates a one-time password. Prominent vendors of such devices and systems are RSA Security Inc. and Secure Computing Corporation. Further, the exchange of secret information may be substituted with a Public Key Infrastructure (PKI) system in which the user supplies a certificate. The certificate is verified via a chain of certificate authorities, which are systems representing companies or organizations which verify the certificate is valid. PKI represents a much stronger overall security mechanism but also costs the most in terms of management.

3.2.2 Authorization

Authorization is the process by which users are allowed access to resources and information based on some determined criteria. A common mechanism for access control is the use of roles defining sets of access permissions. Users are then assigned to one or more roles. The simplest of role mechanisms is the traditional user group.

The LL/CAS has at least three distinct roles into which users must be classified: browser, submitter, and reviewer. At a minimum, access to the system must be managed such that only authorized users are allowed to review record submissions, and only authorized users are allowed to submit records.

3.2.3 Encryption

Whereas authentication and authorization are closely related, encryption is somewhat independent, albeit a necessary part of a secure system. The purpose of encryption is to ensure no eavesdropper or network snooper can capture network traffic and determine how to infiltrate the LL/CAS. All network traffic between users operating a Web browser and the LL/CAS as well as all exchanges between servers providing data must be encrypted.

Encryption takes two forms, symmetric and asymmetric. Symmetric encryption uses a single key to encrypt and decrypt data. The key is itself a secret that must be shared in some secure manner

[7] Hiner, Jason, "Security hinges on authentication, authorization, and encryption," http://asia.cnet.com/itmanager/trends/0,39006409,39079141,00.htm.

[8] http://www.ietf.org/html.charters/aaa-charter.html

between sender and receiver prior to information exchange. Asymmetric encryption relies on a public-private key pair. The keys in the pair are mathematically related by distinct such that it is computationally infeasible to construct one from the other. Information encrypted with one may be decrypted with the other and vice versa.

One of the most common encryption mechanisms in use today is the Secure Sockets Layer (SSL), also known now as Transport Layer Security (TLS).[9] TLS uses asymmetric encryption in the negotiation process to determine a symmetric key to be used for some length of time, not longer than the duration of the connection or "session" between the specific client and server processes.

Virtual Private Network (VPN) technology is also a popular means for encryption. In a VPN each participating machine is brought into a group of machines forming a virtual network in which all communication proceeds. Some VPNs employ X.509 certificates used in PKI systems.

3.2.4 Auditing

An audit log of all system transactions and accesses of system resources is a necessary tool for any forensic analysis of a security incursion. Logs also help identify intrusion attempts. All LL/CAS servers must include authentication and authorization audit logs.

4. Impact Analysis

4.1 Operational Impacts

Operational and organizational considerations include the issue of local data storage versus storing data in the system. Local storage means the organization stores the data on their own machines and only stores the Web links to that data in the LL/CAS. The organization is responsible for backups and other data administration duties. In this option the organization maintains complete control of the data and can deny access at any time. By comparison, the organization that operates and manages the LL/CAS is responsible for data and information that is stored on the system.

From an operational standpoint, proactive security is a must. Audit logs will have to be inspected and other steps will have to be taken to ensure that there are no unauthorized accesses to the data. Intrusion detection and network security operations procedures are absolutely necessary.

4.2 Risks Assessment

Any data that crosses any network medium, wired or wireless, incurs some risk of being compromised no matter how good the encryption or security measures that are in place. One can never assume 0% risk. Therefore de-identification of the data is extremely important and should always be considered for all LL/CA records.

Further, the review process must include careful examination of potential consequences should a LL/CA record become available to unauthorized organizations. One of the reviewer's responsibilities is to determine if other organizations, such as manufacturers should further ratify details that are included in a LL/CA record. Also Web links that are stored should be reviewed thoroughly for only including appropriate content.

Liability issues should be carefully considered. Information that may be considered damaging to an organization presents some risk. There may be organic liability for the LL/CAS in the unlikely event that some information stored within it becomes compromised. It is prudent to ensure that the information is presented in a manner that does not lend itself to liability concerns. This risk will be minimized by ensuring that the individuals assigned to perform record reviews are well matched as SMEs of the information contained in each LL/CA record.

[9] IETF RFC 2246 is the standardization of version 3 of the SSL protocol developed by Netscape.

Printing courtesy of

AIRBUS