



HL7 Security Working Group
Security Risk Assessment
Cookbook

Version 1.4
Draft

12 January 2009



Record of Changes

Date	Version	Description	By
04/23/2007	0.1	Update	Suzanne Gonzales-Webb
04/25/2007	0.2	Quality Assurance Review/Revision	Craig Winter
04/27/2007	0.3	Update	Dan Anderson/S. Gonzales-Webb
04/27/2007	0.4	Quality Assurance Review/Revision	Craig Winter
04/28/2008	0.5	ISO/COBIT RA Harmonized	Dan Anderson
05/02/2007	0.6	Quality Assurance Review/Revision	Craig Winter
7/10/08	0.7	Accept all comments. Draft	Dan Anderson
8/25/2008	0.8	Adding in/making adjustments per returned comments from HL7 WG Security WG listserv members	Dan Anderson
8/27/2008	0.9	Peer Review	Suzanne Gonzales-Webb
08/28/2008	1.0	Quality Assurance Review/Revision	Craig Winter
12/23/2008	1.1	Update, Peer Review	Suzanne Gonzales-Webb, Diana Proud Madruga
01/09/2009	1.2	Update, Peer Review	Suzanne Gonzales-Webb
01/09/2009	1.3	Quality Assurance Review/Revision	Craig Winter
01/10/2009	1.31	Update, Peer Review	Suzanne Gonzales-Webb, Diana Proud Madruga
1/12/2009	1.4	Quality Assurance Review/Revision	Craig Winter

Comment [D1]: Since the ISO standard and the Cobit standard are nearly identical it was only necessary to add in the additional detail on the consequence category from ISO. Everything else remains the same. The term "Impact" in Cobit is directly equivalent to the term "consequence" in ISO.

Sgw: okay



Table of Contents

<u>Section</u>	<u>Page</u>
1 Introduction	1
1.1 The Problem	1
1.2 Defining and Managing Risk	2
1.3 Developing a Risk Management Framework	4
1.4 Scope	4
1.4.1 Scope of Risk Management	4
1.4.2 Value Statement	5
1.5 Objectives	5
2 Tools and Methodologies	6
2.1 Identify	6
2.2 Analyze	7
2.3 Prioritize	10
2.4 Plan (Strategize)	12
2.5 Execute	12
2.6 Monitor and Review	13
2.7 Document	14
3 How to follow the recipe steps:	14
3.1 Understanding the Problem	14
3.2 Identify, Analyze, and Prioritize	14
3.3 Escalate Issues	14
3.4 Issue Process:	15
4 Conclusion	17
5 Definitions	17
6 References	18

List of Tables

<u>Table</u>	<u>Page</u>
Table 1: Sample Likelihood Categories (Source: SSHA)	8
Table 2: Consequence Category Interpretation	9
Table 3: Sample Risk Map (Source: SSHA)	11
Table 4: Sample Risk Map with Mitigation Status	13
Table 5: Sample Risk Summary Document	16

List of Figures

<u>Figure</u>	<u>Page</u>
Figure 1: Sample Risk Category Wheel (Source: SSHA)	3
Figure 2: Risk Management Lifecycle (Source: SSHA)	6

Comment [DKA2]: Changed table 2 source from ISO/DTS 25238 to ISO/TS 25238 per comment from Glen Marshall

Sgw: ok

REMOVE COMMENT



1 Introduction

Healthcare today has some of the most diverse needs with regard to sharing of data and the need to securely move patient information among systems. Within Health Level Seven (HL7) there are multiple verticals that consider messaging, structures, data models, coding and the like. Security is the common thread that connects all of them.

1.1 The Problem

Increasingly, healthcare organizations and technology vendors are performing assessments (threat risk assessments, privacy impact assessments, business impact assessments, etc.) to ensure installed healthcare technology will have a positive impact on healthcare delivery. These assessments, often called risk assessments, are even mandated for healthcare delivery organizations in some countries. However, key decision makers have difficulty understanding the relevance of the risks identified. Therefore, discussions about how much risk is acceptable, what types of risk may arise from new technologies and how much to spend on mitigating risks is often overlooked. As a result, risk is not properly considered when determining technology strategies.

This Risk Assessment Cookbook is intended to create a unified HL7 Risk Management Process and educate the HL7 associated healthcare organizations and technology vendors about the concept of risk management with regard to healthcare information technology. This Risk Assessment Cookbook focuses primarily on healthcare information technology and the use of risk management in developing and implementing technology strategies.

“Why we need to advance into a new paradigm... The current endless list of security risks isn’t getting us anywhere....”

As healthcare technology grows more complex, the need for a unified approach to managing the risks inherent in new technologies grows with it. These risks include many different types of risks including: Information Technology (IT) security, privacy, safety, corporate risks and human factor. A holistic analysis is necessary to weigh the cost of preventative measures.

Diligent healthcare organizations as well as technology vendors have been working since the inception of healthcare technology to assess their own risk levels as best they can by performing threat risk assessments, privacy impact assessments, business impact assessments, security posture assessments, ad infinitum.

Risk management is about more than keeping hackers from stealing personal health information. Since Risk Management is mandatory in many countries, many attempts have been made to standardize the process; however, this standardization has not been fully realized. A Goal of this document is to provide a way for members to use a common risk framework for their risk assessment (RA) and escalate appropriately following the process outlined to avoid the RA gathering dust. The significance of this document is that the [ISO/TS 25238 Health Informatics-](#)

Comment [DKA3]: Changed ISO/DTS 25238 to ISO/TS 25238 per comment from Glen Marshall

Sgw: ok



Classification of Safety risks from health software and also ISACA (Information Systems Audit and Control Association) [(IS Auditing Procedure P1)-attached reference ISACA Risk Assessment] IS Risk Assessment Measurement derived from COBIT (Control Objectives for Information and related Technology) coming from the COSO (Committee of Sponsoring Organizations of the Treadway commission) Internal Control-Integrated Framework have been harmonized into one compact Risk Assessment framework.

Key decision makers have difficulty understanding the relevance of the risks identified, and often overlook them when determining technology strategy. As a result, discussions such as how much risk is acceptable, what types of risk may arise from new technologies, and how much to spend on mitigating risk are often ineffective due to lack of complete information. Security, privacy or other expensive technologies are invested in as a result of popular demand rather than cohesive vision, an important motivation for the creation of this Risk Assessment Cookbook.

This **Cookbook** presents best practice risk management tools to identify and address the risks inherent in healthcare technology in a coordinated manner.

1.2 Defining and Managing Risk

Risk is defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. (ISO/IEC PDTR 13335-1). The majority of risks reported mention negative impacts (such as those listed in Figure 1), however it is important to note that a risk can have an impact that is positive, (e.g., an opportunity to reduce wait times, provide patients with access to their health data, reduce medication conflicts through automated checks against a database). The risk level is measured in terms of a combination of the likelihood (probability) and impact (positive or negative) of an anticipated event. While traditional healthcare risks have always necessitated management such as errors in prescribing, errors in treatment, or patients' falling or wandering off. New sources of risk associated with information technology have also been introduced such as IT security and privacy, safety and availability of information when needed, corporate management of technology systems, and even human factor risks such as fatigue and difficult to read application interfaces (see Figure 1).

As healthcare technology grows more complex, the need for a unified approach to managing the risks inherent in new technologies grows with it. **Risk Management** is a combination of all the processes involved in realizing existing as well as newly identified opportunities in a manner consistent with public interest, human safety, and the law while managing adverse effects caused by the complexity of healthcare systems. It involves identifying, assessing and judging risks, assigning ownership, taking action to mitigate or anticipate them, and monitoring and reviewing progress. The outcome is a holistic analysis that weighs the cost of preventative measures and establishes a continuous process to manage them.

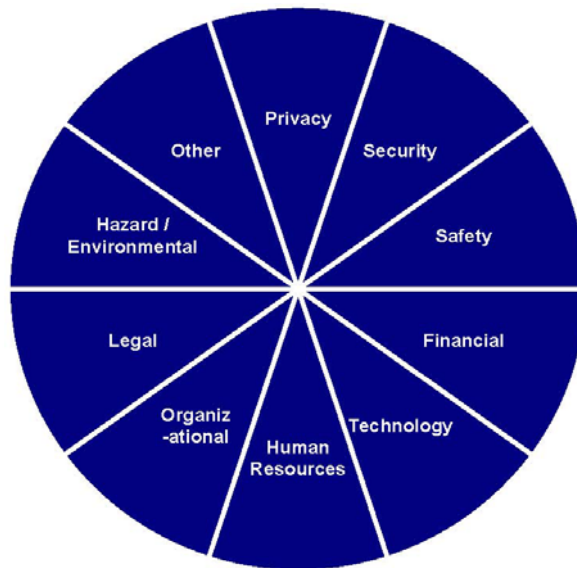


Figure 1: Sample Risk Category Wheel (Source: SSHA)

Effective risk management enables senior management, middle management, and technical and operational staff to:

- Improve business performance by informing and improving decision making and planning,
- Promote a more innovative, less risk adverse culture in which the taking of calculated risks in pursuit of opportunities is encouraged,
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance,
- Assist in meeting healthcare requirements and objectives,
- Facilitate partnerships with other healthcare organizations to address the issues inherent in interoperable systems and data sharing, and
- Benefit patients who are often shared among unrelated healthcare providers in terms of both the handling of their information as well as improving the safety of healthcare services.



This HL7 Risk Management Process will be used to identify issues, categorize them using a standard and accepted risk framework, and bring them to the attention of the Security Working Group (WG). The HL7 WGs will then utilize the consulting and oversight of the Security Working Group to standardize the much needed solutions and, at the same time, leverage the limited resources available.

1.3 Developing a Risk Management Framework

A risk management framework consists of risk management and prioritization tools that facilitate problem analysis and prioritization work throughout the risk management assessment lifecycle. This cookbook will provide examples of some popular tools used. The objective is to illustrate both how to do a risk assessment, as well as the fact that not all risk assessments can be applied to all implementations.

As with all assessment exercises, once a risk management framework is agreed upon, the real work must begin. Healthcare IT exists in an environment which is constantly identifying new issues and risks (primarily in, but not limited to, the security domain). An ad-hoc approach to addressing these is dangerous and creates many new risks, such as technology conflicts, obsolescence, and inadequate focus on prioritizing solutions according to greatest value. A prime example of this phenomenon is leveraging biometric technology for uses for which they were not intended. Instead, there must be a corporate-wide commitment to applying the risk management framework on a continuous basis. This is the proven method of benefiting from risk management activities.

1.4 Scope

This document is primarily concerned with laying out some straightforward risk management and prioritization tools to facilitate problem analysis and prioritization work.

1.4.1 Scope of Risk Management

The scope of the Risk Management cookbook is the universe of risk associated with information technology. Examples of risks that may pertain are:

- Confidentiality, Integrity, and Availability (CIA) information,
- Personal Health Information (PHI),
- Patient safety that may be affected by risks to information within an integrated environment,
- Technology risks (conflict, interoperability, availability),
- Obsolescence risks,
- Inappropriate or premature choices of technology solutions that jeopardize adoption, funding, and future initiatives,



- Trust between organizations (and their handling of information security),
- Authorization/Identification risks, and
- Identification of risks that cannot be addressed within HL7 that must be communicated to the appropriate stakeholders.

All Risks can be considered using this framework.

The task of the HL7 Security Working Group is to ensure that each Special Interest Group (SIG) and Working Group (WG) has a common Security framework for Risk Assessment that surfaces the results in a uniform methodology for prioritization, planning, and communication purposes.

This Risk Assessment Cookbook will provide examples of risk assessments (Section 3) that illustrate both how to do a risk assessment as well as the fact that not all risk assessments can be applied to all implementations.

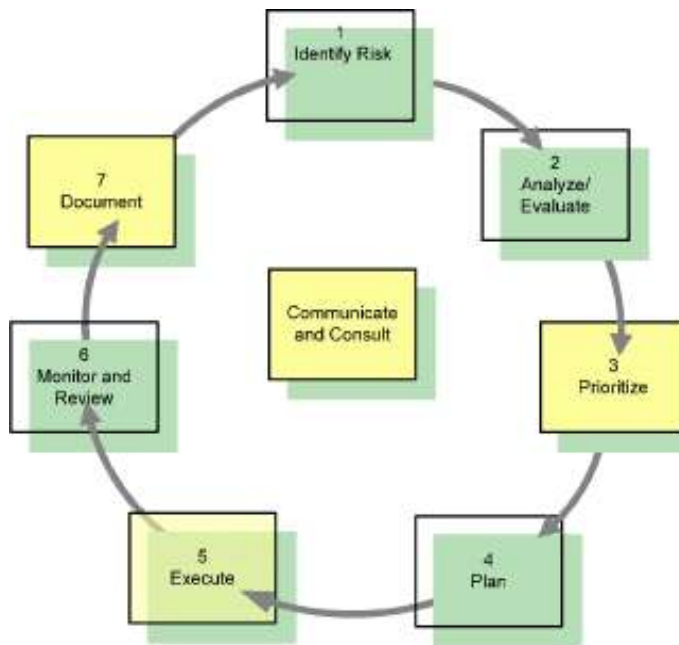
1.4.2 Value Statement

All healthcare organizations are faced with the difficult task of delivering timely and comprehensive healthcare while juggling the risks associated with that healthcare. This should not be thought of as a conflict but an opportunity to identify potential problems and solve or at least minimize them before they occur.

1.5 Objectives

Once risk management tools and methodologies are agreed upon, there must be some work done at the planning level to apply these tools *across the board*.

2 Tools and Methodologies



Scientific Method of Project Management

Figure 2: Risk Management Lifecycle (Source: SSA)

The risk management lifecycle consists of seven well-defined stages. The following sections describe the activities conducted at each stage and offer advice and tools for accomplishing them. (Note that the examples in this cookbook focus on risks associated with healthcare information technology, but clinical risks, human fatigue, and risks such as those introduced by poorly designed user interfaces must also be addressed in a complete risk management program.)

2.1 Identify

Prior to planning any security solutions, the entire gamut of risks pertinent to a new technology or architecture must be identified. The identification process usually includes leading facilitated brainstorming sessions with subject matter experts and summarizing the findings. It may also be helpful to consult published checklists from different types risk assessment standardization groups [e.g., International Standards Organization (ISO), Healthcare Insurance Reciprocal of



Canada (HIROC), Failure Mode and Effect Analysis (FMEA), UK Government's Risk Analysis and Management Method (CRAMM)].

An important hint to the identification process is that the information often exists in the minds of the subject matter experts. Asking pertinent questions such as:

- What are the assets that we are trying to protect?
 - What are possible threats and threat scenarios to those assets?
 - What are the vulnerabilities of the systems in place around these assets?
 - What are the risks resulting from these vulnerabilities?
- What are the categories of risk that we are concerned with?
 - Technical?
 - Strategic/commercial?
 - Organizational?
 - Human (user / patient / administrator)?
 - Political?
 - Financial/economic?
 - Environmental?

After the initial creation of a catch-all list of possible risks, vulnerabilities and threats by brainstorm or checklist method, the refinement process is simply to narrow down the list by removing out-of-scope, redundant, and non-critical elements.

2.2 Analyze

After a comprehensive list of risks is prepared and brief descriptions are recorded, the next step is to assign quantitative values of the business impact of each risk so that they can be compared.

A value from very low to very high (i.e., *vl-l-m-h-vh*) must be assigned in each of two traditional areas: likelihood and impact. In order that stakeholders understand the context of the evaluation, likelihood and impact tables should be developed that specify the definitions of each value (e.g., Tables 1 and 2 are used by Ontario's Smart Systems for Health Agency (SSHA), a large non-profit, IT service provider). Each organization must determine their own impact categories and create a hierarchy of severity to illustrate them such as in Table 1.



Table 1: Sample Likelihood Categories (Source: SSHA)

Probability		Likelihood Description
Very High	> 80%	This event will probably occur in the near future.
High	51% to 80%	This event is likely to occur in the near future.
Medium	21% to 50%	This event may occur in the near future.
Low	6% to 20%	This event is possible but highly unlikely to occur in the near future.
Very Low	0% to 5%	This event is not expected to occur in the near future.

Assignment to consequence categories¹

Hazards (potential for harm) which a health software product might present to a patient if it were to malfunction or be the cause of an adverse event shall be determined and the potential consequences of such hazards shall be identified. Each such consequence shall be assigned to one of the following consequence categories:

- catastrophic;
- major;
- considerable;
- significant; or
- minor.

Note that it will not be necessary to identify and categorize all possible consequences that could arise. The analysis to identify the realistic consequences and the likelihood of their occurring need be undertaken only to the extent necessary to assign, with confidence, the product to a risk class.

The consequence categories shall be interpreted as presented in Table 2. The descriptions have been created to suit the context of this document, but are consistent with those in other sectors and in other complementary disciplines and approaches. Where there is doubt on the margins of two categories the consequence shall be assigned to the category of worse consequence.

¹ Source: ISO/TS 25238 Classification of Safety Risks from Health Software (changed from ISO/DTS to ISO/TS)



Table 2: Consequence Category Interpretation

(Source: ISO/TS 25238) © ISO 2006 – All rights reserved

Consequence Category	Interpretation	
	Consequence	Number of patients affected
Catastrophic	Deaths.	Multiple
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term.	Multiple
Major	Death.	Single
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term.	Single
	Severe injury or severe incapacity from which recovery is expected in the short term.	Multiple
	Severe psychological trauma.	Multiple
Considerable	Severe injury or severe incapacity from which recovery is expected in the short term.	Single
	Severe psychological trauma.	Single
	Minor injury or injuries from which recovery is not expected in the short term.	Multiple
	Significant psychological trauma.	Multiple
Significant	Minor injury or injuries from which recovery is not expected in the short term.	Single
	Significant psychological trauma.	Single
	Minor injury from which recovery is expected in the short term.	Multiple
	Minor psychological upset; inconvenience.	Multiple
Minor	Minor injury from which recovery is expected in the short term; minor psychological upset; inconvenience; any negligible consequence.	Single

Comment [DKA4]: Changed ISO/DTS 25238 to ISO/TS 25238 per comment from Glen Marshall

Sgw: ok

In identifying the hazards which a health software product or product type may present to a patient, a hazard shall not be dismissed simply because it is believed that the design of the product is such that there are no circumstances in which the hazard would arise because of the particular product or general design features. The potential for harm (hazards) which the product could present shall be determined as if such design features and controls were not present or malfunctioned.

For a healthcare software product, as in the above paragraph, identifying hazards which may present to a patient (i.e., due to malfunction or be the cause of an unintended event despite the vigilance of the user or other events external), shall also not be dismissed simply because, even if



the hazard were to arise, no adverse consequences to a patient would occur. This aspect is addressed by the assignment of likelihood to the consequence.

2.3 Prioritize

Once risks are assigned impact and likelihood values they can be compared, using a tool such as a risk map (Table 3). In brief, the red, orange and yellow areas are where the organization must focus their mitigation efforts first. Items in the green and blue areas still qualify as risks, but are of lower priority until all greater risks are mitigated. Organizations must determine their own risk tolerance line (i.e., when to accept risks and when risk mitigations cannot be delayed).

Take for example the risk of flooding to an IT data center. While the potential impact of this risk could be huge, the likelihood of an actual occurrence of this risk in a dry climate (e.g., Arizona, USA) is very low. In addition, many data centers are designed to include some precautions (e.g., such as putting actual server rooms on well reinforced floors or well above ground level) so the impact of a flood would be reduced from “truly catastrophic failure to deliver” to “low impact on infrastructure.” As a result, the final risk rating of the “flooding to the IT data center of the well constructed Arizona data center” falls in the “blue” category and does not need to be addressed at the present time. The visual aid provided by the risk map is critical to adequate prioritization and planning.



Table 3: Sample Risk Map (Source: SSHA)

	<ol style="list-style-type: none"> 1. Scheduling and availability of radiation systems 2. Prescription conflicts 3. Prescription dosage errors 4. Patient location tracking and transfers 5. Spelling of patient name and other identifying information 6. Coding of medication order 					
Impact / Consequence	Very High		6			1 3
	High					
	Medium		4			2
	Low					
	Very Low					5
		Very Low	Low	Medium	High	Very High
	Likelihood					

Formatted Table



2.4 Plan (Strategize)

Once the risks are identified and prioritized, risks with an overall risk rating of 3-5 (yellow orange or red zones on the risk map) must be documented in a risk register, which will guide the assigning and eventual tracking of mitigation actions and ownership. Table 3 is a sample risk register that was developed using Microsoft Excel.

2.5 Execute

One of four tactics should be employed for addressing each identified risk:

- **Accept:** Weigh the cost of the risks versus the cost of mitigating it. Sometimes it is more prudent and more effective to create a disaster recovery plan than to try to mitigate the inevitable (or hard-to-avoidable).
- **Transfer:** Leverage insurance clauses, service level agreements, and other contractual documentation to transfer the cost or recovery from a risk away from the organization. A prime example of this is liability insurance.
- **Mitigate:** Buy software, provide training, optimize business processes, hire more people, write a profile, demand the use of encryption, or propose a controlled and well-documented activity that will reduce (not eliminate) the risk level such that it becomes either completely tolerable, or at least tolerable enough that the focus of efforts can move to the mitigation of other priority risks.
- **Avoid:** Sometimes there is too much risk associated with something and no effective way to mitigate the risk, so we choose to do something else and avoid the risk altogether.

Mitigation planning is another process that requires socialization with subject matter experts.

Mitigation plans must be weighed for cost (e.g., financial, time), pertinence to the actual problem, and greatest opportunity for improvement. Some mitigation plans can address multiple risks (e.g., digital certificates can respond to both risks associated with poor authentication as well as no repudiation) and an opportunity map (like a risk map) can be used in situations where mitigation plans require advanced prioritization.

For example: Car insurance with a high deductible is an example of partial transference and partial mitigation. Below the \$1000 deductible, things need to be either accepted or mitigated without the help of insurance. Above \$1000, the risk is transferred to the insurance company.



2.6 Monitor and Review

The risk register should be reviewed on a regular basis (monthly/quarterly/yearly) to track mitigation status. Risks in process of mitigation can be re-plotted to show their updated risk status and mitigation status (i.e., the risk tokens can be reassessed as less severe impact or likelihood as a result of the completion of certain mitigation milestones).

Table 4: Sample Risk Map with Mitigation Status

AUDITABLE UNIT	AUDIT RISK RANKING (from Example 1)	BUSINESS RISK FACTORS (RATE 0 OR 1)				BUSINESS RISK RANKING FACTOR	Total Risk Ranking
		FINANCIAL	STRATEGIC	OPERATIONAL	LEGAL COMPLIANCE		
Business	Risk weighting	5*	4*	3*	2*		
Treasury System	158	1	1	1	0	12	1896
Business Continuity	162	0	0	1	1	5	810
Payroll	165	0	0	1	0	3	495
Local area networks	159	0	0	1	0	3	477
Computer operations	146	0	0	1	0	3	438
Software licensing	123	0	0	0	1	2	246
Risk Assessment Compliance Factor (RACF)	152	0	0	1	0	3	456
Instructions							
1. For each Auditable unit fill out the Key Variable sheet							
2. Use the resulting total score in column B of this sheet for the risk weighting							
3. Fill out the rest of this spreadsheet indicating 0 or 1 for Financial, strategic, operational, or legal compliance							
4. Note the resulting total risk scores and prioritize low to high							



2.7 Document

Once mitigation plans are agreed upon, a risk summary document should be created with signoff for risk owners in order to provide accountability. A risk summary document can serve as a mitigation contract with a senior manager, as well as providing details and formal responsibility to a project manager assigned a specific task that may not have authorization to view all the risks contained in a risk register.

Keep this information for posterity! The risk register, risk map, and risk summaries serve both as an audit record of due diligence, as well as a valuable lesson for future risk analysis. The documentation created with the tools described in this section provides excellent audit records in the event of an incident and for investigations, as well as educational materials for planning new healthcare and technology activities.

3 How to follow the recipe steps:

3.1 Understanding the Problem

Understand the problem landscape by reviewing this cookbook and following the recipe to surface the risks for analysis.

3.2 Identify, Analyze, and Prioritize

Identify, Analyze, and Prioritize utilizing the HL7 Security Risk Template. Issue levels:

Low:	Minimal impact to resources or compromise of data.
Medium:	An escalation in seriousness to computing resources but no compromise or potential compromise of confidential information.
High:	Computing resources compromised and present a serious security risk, or confidential data has been compromised.
Non-Issue:	A non-issue will be documented as received, but no further analysis will be done.

3.3 Escalate Issues to the Security Working Group

Escalate issues following the escalation procedure as described below. Issue escalation is a critical component in proper risk assessment and mitigation.

- 3.3.1 At least two individuals shall be available when escalating from Medium to High level.
The Security WG chair or co-chair and the Security WG Issue Consultant as described below shall be available.
- 3.3.2 Issue response team:



- 3.3.2.1 **Issue Response Manager:** Typically the person who has performed the risk assessment from above and is bringing the issue to the Security WG.
- 3.3.2.2 **Communications Coordinator:** Appointed by the event manager and oversees the communication to the organization and issue team.
- 3.3.2.3 **Security WG Issue Consultant:** The person on the Security WG assigned by the Security WG chair or delegate who is responsible for consulting on the issue (may be the communications or event manager listed above, but not necessarily).

3.4 Issue Process:

- 3.4.1 Using the tools and methodologies for the Risk framework, the Issue Response Manager will perform a risk assessment to assign a value to the issue of low, medium, or high. The manager may use additional resources he deems necessary.
- 3.4.2 Review Issue Database (to be created) for similar issues. The Issue Response Manager will perform the risk assessment using the Risk Spreadsheet to fill out the Risk Summary Report.



Risk Summary Report Example: (A blank form is attached at the end of the document.)

Table 5: Sample Risk Summary Document

Risk Category				
Risk ID #	<from risk register>			
Issue/Risk Title	<short, illustrative title>			
Description	<Details please>			
Potential Risk Scenarios	<What would happen if risk is not resolved?>			
Risk Owner(s)	<insert name of lead who is responsible for ensuring that sufficient resources and time is allocated to mitigate this>			
Impact/Consequence Category	<use category from impact table>			
	Impact/Consequence	Likelihood	Risk Rating	
Related Opportunities	What opportunity does the organization have in mitigating this risk in the ways suggested?			
Risk Mitigation Activities	<please be detailed>			
Risk Mitigation Owner	<Person delegated authority to mitigate these risks by the accountable executive.>			
Risk Mitigation Timelines	<date that this risk will be mitigated by>			
The following responsible parties acknowledge this risk:				
<Name>		Date		
<Title>				
<Organization>				
<Name>		Date		
<Title>				
<Organization>				



- 3.4.3 Once the risk assessment is completed the Issue Response Manager will bring the issue to the Security WG Chair or designee.
- 3.4.4 The Chair or designee will review the issue and assign to an appropriate Security WG Issue Consultant who will analyze the issue, calling on additional resources they deem appropriate.
- 3.4.5 After the issue is analyzed, recommendations will be provided by the Security WG Issue Consultant.
- 3.4.6 The Issue Event Team members will convene to create an action plan that will include the various documents, a description of the issue, the proposed solution(s), and a time line for implementation.
- 3.4.7 The Communications Coordinator will communicate the results to the interested parties and projects will be undertaken.
- 3.4.8 The Event Manager will monitor, review and document the results and communicate them via the communications manager.

4 Conclusion

Risk management can help organizations in planning and implementing healthcare technology. A properly maintained risk management program will add value to decision-making and business processes, but it requires investments of time and resources. To assist in the development of a risk management program, HL7 has developed this Risk Assessment Cookbook. As well, future HL7 profiles will include a risk analysis section (Stage one of the risk management assessment lifecycle) to help implementers in conducting a complete risk management program. Vendors and service providers that are implementing HL7 profiles are encouraged to conduct a complete risk assessment activity on their products and services and share them with purchasers.

5 Definitions

Risk Risk is “The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.” (ISO/IEC PDTR 13335-1)

The possibility of an act or event occurring that would have an adverse effect on the organization and its information systems. The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to the assets can also be considered a risk. It is ordinarily measured by a combination of effect and likelihood of occurrence.



Inherent risk refers to the risk associated with an event in the absence of specific controls.

Residual risk refers to the risk associated with an event when controls in place to reduce the effect or likelihood of that event are taken into account.

Risk Assessment Measurement

Risk assessment measurement is a process used to identify and evaluate risks and their potential effect.

Risk Assessment Measurement Methodology

Risk assessment measurement is a methodology to produce a risk model to optimize the assignment of audit resources through a comprehensive understanding of the organization's environment and the risks associated with each auditable unit.

The objective of a risk model is to optimize the assignment of audit resources through a comprehensive understanding of the audit universe and risks associated with each universe item.

6 References



IHE_ITI_TF_White_Paper_Security_Cookb

IHE_ITI_TF_White_Paper_Security_Cookbook_PC_2006_08_30



ISACA Risk Assessment.pdf

ISACA Risk Assessment Measurement Document



Risk Summary Report.doc

Risk Summary Report Example



HL7 Risk Assessment.xls

HL7 Risk Assessment Example



ISO_TS_25238.doc

ISO/TS 25238 Classification of Safety Risks from Health Software

Contributors: Dan Anderson (Spectra Consulting Group), Mike Davis (VA), John Moerke (GE Healthcare), Gila Pike (Canada), Suzanne Gonzales-Webb (SAIC), Diana Proud-Madruga (SAIC)

Comment [DKA5]: Changed ISO/DTS 25238 to ISO/TS 25238 per comment from Glen Marshall

Sgw : ok