Integrating the Healthcare Enterprise

Cookbook: Preparing the IHE Profile Security Section

(Risk Management in Healthcare IT Whitepaper)

October 10, 2008

Contents

1 Introduction 3
1.1 The Security Considerations section of an IHE Profile is intended to help implementers make a security assessment of their product / information system in relation to implementing an actor in that profile. It is not a thorough standalone security assessment. The Security Considerations section of an IHE Profile should only deal with issues specifically relevant to the interoperability provided by the profile and not try to encompass every security aspect of the use cases identified in the Profile in Volume 1. 3
2 Risk assessment and mitigation for an IHE profile 4
2.1 Scope of IHE risk assessment 4
2.2 Method for risk assessment and mitigation 5
3 How to write a Security Considerations section 17
3.1 What should be integrated in IHE Technical Frameworks 17
3.2 Where to integrate security in IHE Technical Frameworks 17
3.3 Link with audit trail definition 18
3.4 When and how to update a security section 18

1 Introduction

All new IHE Profiles are required to have a Security Considerations section. This section communicates security concerns that the implementers need to be aware of, assumptions made about security pre-conditions and, where appropriate, key elements of a risk mitigation strategy to be applied. Historically, IHE Profiles have not addressed security considerations and thus implementers have had no direction. This document helps IHE Profile writers complete the Security Considerations section of their IHE Profile.

1.1 The Security Considerations section of an IHE Profile is intended to help implementers make a security assessment of their product / information system in relation to implementing an actor in that profile. It is not a thorough standalone security assessment. The Security Considerations section of an IHE Profile should only deal with issues specifically relevant to the interoperability provided by the profile and not try to encompass every security aspect of the use cases identified in the Profile in Volume 1.

To reflect that, the following section will be integrated at the beginning of each domain Technical Framework to outline the scope of security sections to implementers.

Add the following to all Technical Trameworks, Volume 1, in the "Overview of the Technical Framework" section:

A risk assessment, following security best practices, is done for each profile. The risk assessment identifies risks that may be introduced into a product which adds support for one or more actors in a given profile. The Security Consideration sections in the Technical Framework are based on the mitigations identified in each risk assessment.

The risks assessed are limited to risks relevant to IHE profiles and may not be exhaustive even within the scope of the profile. IHE risk assessments can be used as one input for the overall risk assessment done for the product or system.

There are many security related issues for a product that will not be addressed in this Technical Framework since they are out-of-scope for IHE.

As not all IHE profile writers are security experts, this cookbook is intended to provide basic knowledge on conducting a risk assessment and some "tricks of the trade" relevant to Security Consideration section writing. It is not only based on best practice in the field of risk assessment and mitigation but also on the experience of the ITI Technical Committee while compiling the Security Consideration section for new profiles during the year 5 cycle (mainly XCA and RFD).

This cookbook is specifically intended for IHE profile writers. Though it is based on best practice, it is not a complete method for thorough risk assessment of a package product. IHE does not endorse any use of this cookbook outside of the scope of IHE profile editing.

After presenting the basics of risk assessment and risk mitigation, the cookbook explains how to scope security consideration for IHE profiles and finally provides guidelines on the effective writing of the Security Consideration section.

2 Risk assessment and mitigation for an IHE profile

This section describes the tasks involved in preparing to write the Security Considerations section of an IHE profile. It describes how profile authors can use a spreadsheet template to assess and mitigate the risks introduced by the profile. This spreadsheet is then used to produce the Security Considerations section of the IHE profile as described in section 3.

2.1 Scope of IHE risk assessment

The first thing you need to understand while considering security in IHE profile is that you are not doing a complete risk assessment. Your profile (possibly along with other profiles) will be integrated in a product[1]. As a profile author, you know neither the final product nor the environment in which it will be used, so it would be impossible for you to make a complete risk assessment.

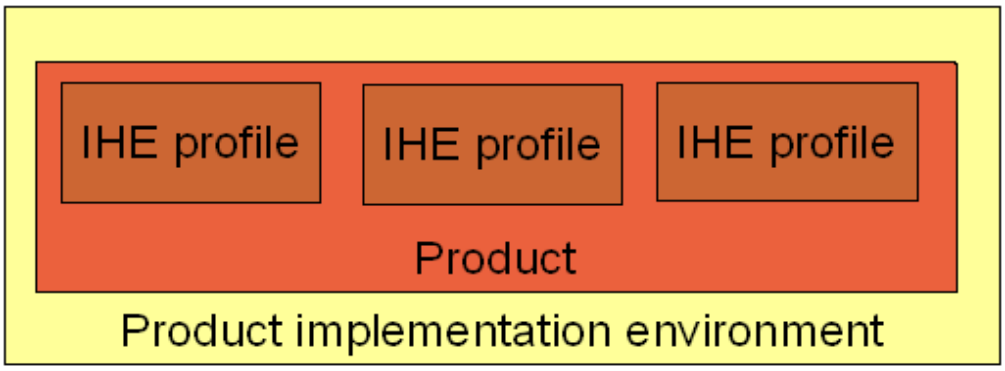


Figure 2.1-1: IHE profiles environment

However, as a profile author, you are the best suited to assess risks which may be introduced into a product which implements actor(s) and transaction(s) defined in your profile, and identify risk mitigation in a way that will help vendors in their own risk assessment for their products.

Any risk you analyze while editing your profile is a valuable input for implementers in their own risk assessment since they benefit from your deep understanding of the profile; but it will also be reviewed and completed by the security experts of the implementers. As a consequence, you shouldn't aim at exhaustiveness at all cost, but rather focus on the risks having an impact on what is defined in the profile. There is no way to automatically define the scope of an IHE profile risk assessment, but a good rule of thumb is to focus on the actors and transactions defined in the profile and add any elements[2] that appear to be needed as risks are assessed and scenarios are identified.

1 The term product is taken here in a general sense, it can designate any integrated software or piece of hardware using the profile.

2 Also called “assets” in the context of a risk assessment.

For example the scope used for risk assessment for the RFD profile (Retrieve Form for Data Capture) includes the actors defined in the profile but also takes into account specific use cases in which RFD will be used like double blind studies, as there may be specific risks linked to that use of RFD. Double blind studies would introduce a need to hide both the identity of the researcher and the identity of the patient not only hiding his/her name but also any specific treatment that might provide a clue as to who the patient is. As a result, the risk assessment for RFD has not only taken into consideration the actors of the profile but also included in the assessment the specific risk; one of the asset considered was "Relationship between forms manager and forms filler in a double blind study" with specific risk and mitigations associated (see RFD profile section 17.5 and RFD risk assessment for detail).

2.2 Method for risk assessment and mitigation

Risks assessment and mitigation is a three step process:

- list the various scenarios that could lead to an adverse event, detailing particularly which assets are impacted and what kind of impact the adverse event has; these are your risks;
- assess each risk in terms of likelihood and impact;
- specify mitigation(s) for the highly relevant risks.

In order to promote consistent security documentation across IHE domains, profile authors are advised to use the following table for their risk assessments. Instructions for use of the table follow. For ease of use, the excel version is available on IHE ftp

Characterization of risks			Assessment of risks		Mitigation of risks			
Scenario	Asset	Type of impact	Level of impact	Probability	Mitigation	New level of impact	New probability	Comments

ftp://ftp.ihe.net/IT_Infrastructure/

Table 2.2-1: Risk assessment and mitigation table

2.2.1 List risks

There is no single prescription that all IHE Profiles can follow. Various profiles will have different risks. For instance, the profile Consistent Time (CT)[3] communicating reference system time to all systems doesn't introduce the same risks into a product as a profile for transmitting personal medical data on patients like Query for Existing Data (QED)[4]. The general approach to use while assessing risks for a profile is to imagine scenarios where, while using the profile, something could "go wrong" (possible adverse consequences of an accident) or be made not to go as it should (possible malevolent objectives that could be achieved through an attack). A profile writer having some experience in risk assessment (either in general or in the context of IHE profile writing) might find it easier to start by listing the assets and then derive the scenarios out of that list or even start considering the risks through the possible type of impact. Those alternatives are

3 Included in IT Infrastructure Technical Framework.

4 Included in Patient Care Coordination Technical Framework.

totally acceptable as long as all the columns of the characterization part of the table are filled out. It is, however, advised for beginners to "prime the pump" by thinking about the scenarios.

As a guideline for that task, concentrate on scenarios that could potentially:

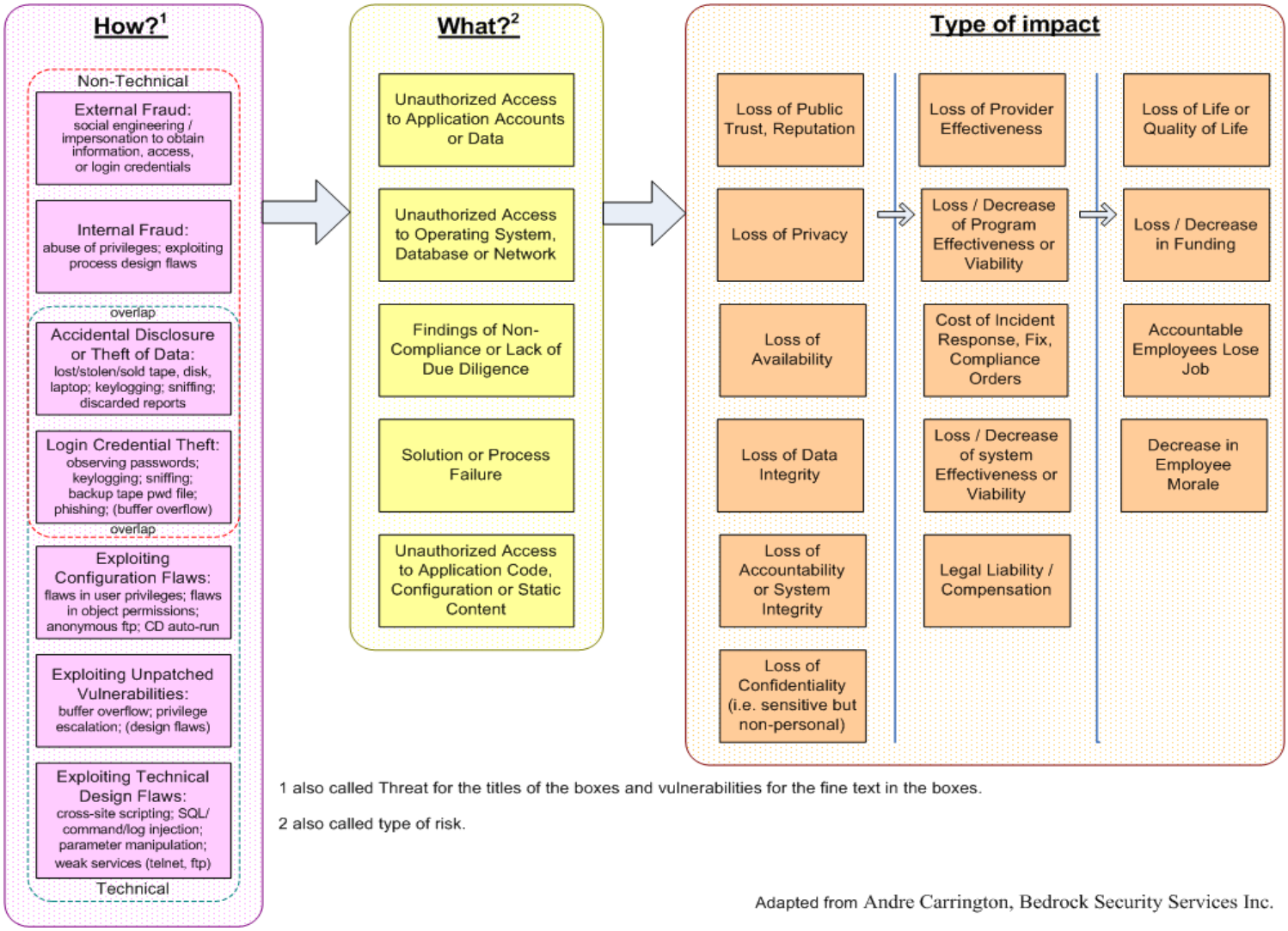
- endanger the patient (e.g. through lack of availability of data concerning his/her health or loss of integrity of those data);
- break the business model (leading to financial losses especially if one can benefit from it);
- lead to inappropriate disclosure of confidential data (which will lead to indirect financial losses).

It is suggested a scenario be expressed as a short "story" explaining *who*[5] is doing *what* through which means (*how*) to achieve what (*goal*) and what are the consequences (*type of impact*). Note that if the adverse event described in the scenario is an accident, the *who* and the *goal* are not used.

As an example, the following scenario is one of the scenarios used for the XCA (Cross-community Access) risk assessment: A malevolent journalist, looking for a scoop, exploits the fact that responses to queries are sent over a public network (i.e. the Internet). The journalist eavesdrops and gains access to metadata returned from the registry without being authorized, thus resulting in a loss of privacy.

Devising scenarios is mainly an intellectual work of imagination. The following diagram (fig 2) serves to help providing ideas on which to build scenarios. It lists the generic "what's", "how's" and "type of impact" that can be used when defining scenarios.

5 Generally it is merely expressed as a malevolent individual, but it sometime can be further specified.



1 also called Threat for the titles of the boxes and vulnerabilities for the fine text in the boxes.

2 also called type of risk.

Adapted from Andre Carrington, Bedrock Security Services Inc.

155 **Figure 2.2.1- 2: Generic scenario components**

When using figure 2, keep the scope of the profile you are writing in mind to describe relevant scenarios. Each system has its own specificities including (but not limited to) goal, functionalities or architecture. All the components listed in figure 2 may not be relevant for all profiles. For
160 instance, a system keeping track of users' identity is subjected to a risk of a user passing for an other user, whereas this risk doesn't exist for a system accepting only anonymous users (meaning that the component "login credential theft" isn't relevant as a how, and the component "Unauthorized access to application account or data" isn't relevant as a what).

The components presented in figure 2 constitute a generic list to be scoped down depending on the
165 profile considered, and can be expanded if additional scenarios are found[6].

6 You should list all the scenarios that you can think of (either with the help of the material or though of upfront), even the most ludicrous one (they will be discarded during risks assessment if they turn out to be irrelevant).

As a general guideline, the following table highlights, based on previous risk assessment for IHE profiles, the type of impact generally deemed relevant for each type of IHE profile.

Types of impact \ Types of profile	Content profile	Workflow profile	Infrastructure profile
Loss of public trust, reputation	Relevant	Very relevant	Relevant
Loss of privacy	Less relevant	Very relevant	Very relevant
Loss of availability	Less relevant	Relevant	Very relevant
Loss of data integrity	Very relevant	Relevant	Very relevant
Loss of accountability or system integrity	Less relevant	Less relevant	Very relevant
Loss of confidentiality (i.e. Sensitive but not personal)	Less relevant	Very relevant	Very relevant
Loss of provider effectivness	Very Relevant	Very Relevant	Relevant
Loss / Decrease of program effectivness or viability	Relevant	Relevant	Relevant
Cost of incident response, fix, compliance orders	Relevant	Relevant	Very Relevant
Loss / Decrease of system effectivness or viability	Relevant	Relevant	Relevant
Legal liability / compensation	Very Relevant	Very Relevant	Relevant
Loss of life or quality of life	Very Relevant	Very Relevant	Very Relevant
Loss / Decrease in funding	Relevant	Relevant	Relevant
Accountable employees loose job	Relevant	Relevant	Relevant
Decrease in employee morale	Less relevant	Less relevant	Less relevant

Figure 2.2.1- 3: Guidelines of impact relevance for IHE profiles

This table is a guideline devised from the editors' experiences to help you focus your efforts. Ideally, each impact should be analyzed to see if a scenario could lead to that type of impact.

If your profile relies on other profile(s) for functional reasons[7], it is advised to use the other profiles' risk assessments as input, but just don't copy them since your profile might introduce new risks.

Once the scenarios are listed, the assets impacted by each scenario should be listed along with the type of impact. Assets are the element of the profile affected by the adverse event. For IHE profiles, assets are mostly actors, contents and transactions.

As an output of this step, the characterization part (first three columns) of the spreadsheet presented in tab 1 can be filled out:

7 For instance, a content profile linked with a specific infrastructure profile like the XDS-MS content profile relying on XDS infrastructure.

Table 2.2.1-1: Listing of risks part of assessment and mitigation table.

Characterization of risks		
Scenario	Asset	Type of impact

- **Scenario:** a description of how the adverse event can happen
- **Assets:** the elements that the adverse events impact (actors, transactions and any elements deemed relevant).
- **Type of impact:** the description of the negative impacts on the assets.

Though a scenario can impact several assets, for ease of use during the risk assessment and risk mitigation stage, it is advised to duplicate scenario lines in order to have only one asset per line.

2.2.2 Assessment of risks

Once you have a list of the risks and the associated scenarios, each scenario has to be assessed for:

- **level of impact**,
- **probability of occurrence.**

The **level of impact** of the risk is a measurement of the consequences an adverse event may have.

The scale for assessing level of impact could be specific to an organization. The team doing the risk assessment for an IHE profile have to agree on the levels of impact to be used before starting the risk assessment and make its own table explaining the levels used. For consistency in IHE risk assessments we recommend using five risk levels (very high, high, medium, low, very low) see the table below for an example.

Table 2.2.2-2: Example of level of impact

	Reputation	Delivery interruption scope
Very High	Potential for reduction in SSHA mandate	May not be able to deliver on most critical requirements
High	Serious adverse attention from media, medical establishment and / or public	Major shortfalls in one or more critical requirements
Medium	Minor adverse attention from media, medical establishment and / or public	Minor shortfalls in one or more key requirements
Low	Loss of reputation among clients / partners	A few shortfalls in desired functionality
Very Low	Internal loss of reputation	System should still fully meet mandatory requirements

Adapted from SSHA

If during the assessment, difficulties arise in selecting the right level of impact, the following rules should be followed:

Very Low (VL)— Reserved for where the assessment is agreed to be unusually low. Very few variables qualify as "Very Low".

Low (L)— All assessors agree that the variable is judged to be "Low"

Medium (M)— The variable is neither "Low" nor "High" or there is disagreement by the assessors as to whether the variable is "Low" or "High".

High (H)— All assessors agree that the variable is judged to be "High"

Very High (VH)— Reserved for where the assessment is agreed to be unusually high. Very few variables qualify as "Very High".

Assessing the **probability of occurrence** is assessing the likelihood of the adverse event. This requires a little more detailed look into the scenario to ascertain whether the adverse event is accidental or voluntary (malevolent):

- the probability of occurrence of an accidental event (break-down of a component, system crash, human error) depends on the reliability of the system and its components, and the ease of use of the functionalities;

- the probability of occurrence of a voluntary adverse event depends on the ease of producing the adverse event (how much time is needed, how much skill is needed, how much it would cost) and the personal benefit that could be derived from the adverse event.

The scales for assessing probability of occurrence could be specific to an organization. The team doing the risk assessment for an IHE profile have to agree on the levels of probability to be used before starting the risk assessment and make its own table explaining the levels used. For consistency in IHE risk assessment, we recommend using five probability levels (very high, high, medium, low, very low) see the table below for an example.

Table2.2.2-3: Example of probability of occurrence

	Likelihood Description
Very High	This event will probably occur in the near future.
High	This event is likely to occur in the near future.
Medium	This event may occur in the near future.
Low	This event is possible but highly unlikely to occur in the near future.
Very Low	This event is not expected to occur in the near future.

Adapted from SSHA

If during the assessment, difficulties arise in selecting the right probability of occurrence, the following rules should be followed:

Very Low (VL)— Reserved for where the assessment is agreed to be unusually low. Very few variables qualify as "Very Low".

Low (L)— All assessors agree that the variable is judged to be "Low"

Medium (M)— The variable is neither "Low" nor "High" or there is disagreement by the assessors as to whether the variable is "Low" or "High".

High (H)— All assessors agree that the variable is judged to be "High"

Very High (VH)— Reserved for where the assessment is agreed to be unusually high. Very few variables qualify as "Very High".

As an output of this step, the assessment part (fourth and fifth columns) of the spreadsheet presented in Tab 1 can be filled out:

Table 2.2.2-4: Risk assessment part of risks assessment and mitigation table.

Characterization of risks			Assessment of risk	
Scenario	Asset	Type of impact	Level of impact	Probability

2.2.3 Mitigation of relevant risks for a profile

For each risk, identify associated mitigations and evaluate their effectiveness.

2.2.3.1 Identify highly relevant risks

Identifying relevant risks is done by separating the risks that should be avoided or limited (i.e. mitigated) from the risks that are not significant enough to justify mitigation. The level of impact, and probability of occurrence considered as not relevant enough, may vary from organization to organization. In general, risks with lower probability of occurrence and/or lower level of impact are considered non relevant in the context of the IHE profile (i.e. risks that will not be further analyzed in the context of the IHE profile).

According to security best practices, the definition of non relevant risks could be specific to an organization. The team doing the risk assessment for an IHE profile has to agree on which risk is relevant and which risk can be considered as non-relevant in the context of the IHE profile. For consistency in IHE risk assessment, we recommend using a matrix showing which risk are relevant and which can be considered as non relevant in the context of the IHE profile (see the table below for an example). The team doing the risk assessment has to agree whether the edge cases (e.g. the stripe cells in the example below) should be considered relevant or not.

Table 2.2.2-5: Example of matrix for relevant risks identification

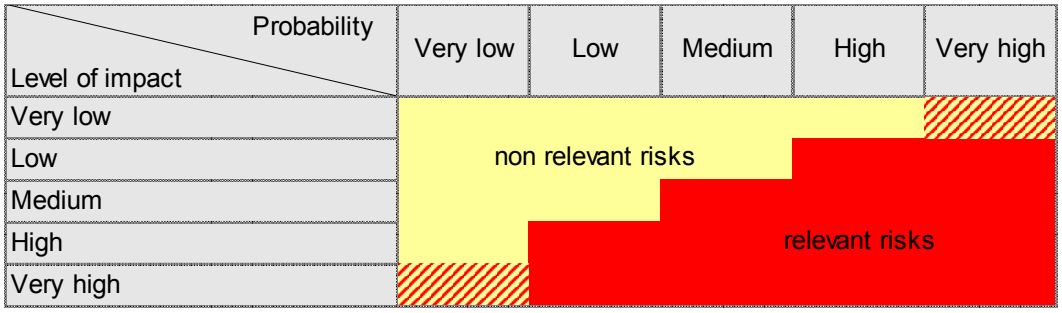


Table 2.2.2-6: Example of non-relevant risk identification

Any non relevant risk should be recorded in the spreadsheet as such using the columns devoted to risk mitigation as shown in the following example.

Characterization of risks			Assessment of risks		Mitigation of risks			
Scenario	Asset	Type of impact	Level of impact	Probability	Mitigation	New level of impact	New probability	Comments
					Considering the level of impact and the probability, that risk has been deemed non relevant ***in the context of the IHE profile*** *.*			

2.2.3.2 Identify mitigations

The purpose of risk mitigation is to act on relevant risks to get them to a bearable level either by:

- lowering the level of impact;
- lowering the probability of occurrence;
- both of the above.

Lowering the level of impact

Lowering the level of impact of a risk can be done either by limiting the scope of the "functionality" at stake (so that the risk will only impact a limited subset of the whole system) or by limiting the loss (for instance safeguard mechanisms or record of any action allowing easy rollback[8]).

For example, consider one of the risks for the NAV profile (Notification of Availability of Documents): interception of the notifications by unauthorized users leads to a risk of inappropriate disclosure of patients health data. To mitigate that risk, all health related data have been trimmed off from the notification sent to keep only the UUID of the documents. The risk of interception of the notification is not less likely, but an unauthorized users would not be able to make any use of the information (no health data and no possibility to retrieve the document since he/she is an unauthorized user) so the level of impact of the adverse event has been lowered.

Lowering the probability of occurrence

If the risk is accidental, lowering its probability of occurrence implies increasing the reliability of the system (in case of a breakdown) or its user-friendliness (in case of a human error). In general, accidental risks are closely related to the implementation environment. As an IHE profile author you will not have to define mitigation for environmental risks, but will leave their mitigation to product developers / product implementers (see below).

If the risk is voluntary (malevolent) the probability of occurrence can be reduced by either making the benefit less attractive[9] or increasing the difficulty of causing the adverse event.

For example, consider one risk identified for XCA: the eavesdropping of the communication leading to inappropriate disclosure of registry meta-data or repository documents. One of the mitigations used is encrypting the data exchanged, thus increasing the difficulty for eavesdropping and lowering its likelihood.

As an IHE profile author, you have three kinds of "mitigation" at your disposal:

- mandate or suggest grouping of actors with IHE security profiles;
- integrate specific mitigation in the profile as profile security feature;
- assign the mitigation of the risk to an identified agent (e.g. product developers, administrative procedures...).

Mandate or suggest grouping of actors with IHE security profiles

If the risk is not unique to the profile but is a risk already identified for other IHE profiles, this is the preferred mitigation, as it builds on the general IHE framework. The security profiles which could be used are:

- ATNA for:
  - system authentication (against unauthorized access from a system point of view),

8 Those are the most frequently used mitigations, others can be found depending on the functions considered.

9 This is often achieved by the same measures as reducing the scope of the risk.

  - protection of confidential data and/or privacy (against eavesdropping),production of audit trails (against unauthorized actions);
- XUA for conveying of an authentication (against unauthorized access from a user point of view);
- DSG for:
  - documents authenticity when a high level of assurance is needed (against unauthorized modification of the document),
  - accountability when a high level of assurance is needed (against repudiation of action);
- CT for sharing of consistent time (against attempt to thwart audit trails through desynchronization of actors' clocks);
- EUA for authentication within an enterprise (against masquerade).

All the referenced security profiles are in the ITI Technical Framework.

If the risks mitigated through a grouping affect all implementation of the profile, the grouping should be mandatory. If the risks mitigated through a grouping affect only specific implementation of the profile, the grouping should be optional and guidance should be given as to when to use this option.

For example, the profile Sharing Value Sets can be used to share public value sets which are not confidential, but it can also be used to share confidential value sets (e.g. protected by copyright). As the risk of eavesdropping is relevant only to some of the implementation (i.e. those sharing confidential value sets), the grouping with ATNA is optional for SVS.

Integrate security features in the profiles

If the risk is unique to the profile, mitigation can be achieved by building security features into the profile itself.

For example, consider one risk identified for XCA: the probing for valid patient IDs. This could be done by automatically sending queries and listing the IDs for those queries that do not generate an “unknown patient ID” error. One of the mitigations used is to treat non-valid patient IDs as valid IDs for patients with no documents (i.e. the query return “no document found” instead of “invalid patient Id”).

Integrating security features into an IHE profile can be complex as finding the right balance between risk mitigation and cost of the mitigation is particularly significant. You are advised to seek the guidance of security experts if you think some assessed risks should be mitigated that way.

Assign the mitigation of the risk to an identified agent (e.g. product developers, administrative procedures...)

Risks linked with a vendors’ development or implementation context should not be mitigated through IHE profiles. It is totally acceptable to leave the actual mitigation of a risk to product developers product implementers and or administrative procedures as long as this is clearly documented.

Note: If your profile relies on other profile(s) for functional reasons, use the other profile(s) risk mitigations as input for yours. Not only will this help you find the relevant mitigations, but it will also insure harmonization of security throughout IHE Technical Frameworks

2.2.3.3 Evaluate mitigations

Next, re-evaluate the **level of impact** and **probability of occurrence** after the mitigation is applied, and re-calculate the assessed risk level.

This step is closely linked with risk mitigations and you may go back and forth between defining risk mitigations and evaluating those mitigations.

As an output of this step, the mitigation part (last 4 columns) of the spreadsheet can be filled out.

Table 2.2.2.3-1: Risks mitigation part of the risks assessment and mitigation table.

Characterization of risks			Assessment of risks		Mitigation of risks			
Scenario	Asset	Type of impact	Level of impact	Probability	Mitigation	New level of impact	New probability	Comments

Comments are used to explain the effectiveness of the mitigation and the reason why the level of impact and/or the probability of occurrence has been reevaluated.

Some mitigations may have insignificant consequences on the level of impact and the probability of occurrence[10]; however, they might be needed for other mitigations to take place and should not be overlooked in the risk mitigation process. Explanation of their relevance despite non visible consequences on risk should be provided in the comments cell.

For example, maintaining a consistent time in all the actors of a profile doesn't mitigate a specific risk. It is however a pre-requisite for audit trails (which are a mitigation for several identified risk) as audit trails without a consistent time could not be compared during an investigation.

If the first mitigation does not reduce the level of impact and the probability of occurrence to an acceptable level, additional mitigations might be needed. When evaluating the effectiveness of such additional mitigations, you should take into account all the mitigations for each risk. This is best done by adding columns to the mitigation table.

Table 2.2.2.3-2: Extension of the mitigation part

Characterization of risks			Assessment of risks		Mitigation of risks							
Scenario	Asset	Type of impact	Level of impact	Probability	First Mitigation	New level of impact	New probability	Comments	Second Mitigation	New level of impact	New probability	Comments

The number of mitigations is not limited as long as they are effective and sound and they contribute to lower the level of impact and probability of occurrence of a risk to an acceptable level.

10 Possibly because the scale used to assess risk is not detailed enough.

It's possible that mitigations through IHE are not enough to lower the level of impact and probability of occurrence of a risk to an acceptable level. They should nevertheless be listed to help product developers and/or product implementers in their global risk assessment.

If the mitigation of a risk is left to the product developers and/or product implementers, it should be documented in the same table.

Table 2.2.2.3-3: Example of mitigation left to product developers / product implementers

Characterization of risks			Assessment of risks		Mitigation of risks			
Scenario	Asset	Type of impact	Level of impact	Probability	Mitigation	New level of impact	New probability	Comments
					No mitigation is provided through IHE for this risk, it is the responsability of the product developers and / or product implementers to mitigate or accept this risk			

3 How to write a Security Considerations section

Though the risks and mitigations table (presented in Section 2) contains necessary security steps and should be available to product developers and product implementers[11], it is too detailed to be included in IHE Technical Frameworks. The following sections will provide guidance as to how to integrate the outcome of a risk assessment into an IHE integration profile.

3.1 What should be integrated in IHE Technical Frameworks

When writing an IHE profile, you should focus on the relevant risks and how they have been addressed. The security section should be a literary presentation of the security constraints (e.g. mandatory or optional grouping with IHE security profile), the security features as well as a summary of the reasons why these constraints and features are required (risks addressed). It should also include a summary of the risks left to be mitigated by developers and implementers.

There is no right way to write a security section; you can organize the section as you see fit as long as all the relevant risks are accounted for and the corresponding mitigations are explained.

As an example of what and how to integrate in the security section, see section 17.5 of the RFD profile.

3.2 Where to integrate security in IHE Technical Frameworks

Specific sections are devoted to security in the IHE supplement template. The section in volume 1 is for risks and mitigations that are profile-wide whereas the sections in Volume 2 are for risks and mitigations that are transaction or content specific.

Mandated or suggested grouping of actors with IHE security profiles should be presented in volume 1 with the other possible grouping necessary to the profile.

It may happen that, for historical reason, there is a common security section in the Technical Framework your supplement will be integrated in (either for the whole Technical Framework or for a grouping of profiles in which you profile will be), the security section in your profile should then only deal with risks and/or mitigations that haven't been assessed in the existing section yet. Even if such a section exists and seems very comprehensive, the preparatory steps presented in section 3 should nevertheless be followed to be sure nothing has been overlooked.

Finally, some specific security features developed during risk mitigation could turn out to be new functionalities for your profile. If such, they should be described within the profile as any other functionality, but should be referenced by the security section.

For example, risk on patient privacy led to include a de-identification function in the Teaching File and Clinical Trial Export profile (TCE) which is included as a function in the profile outside of the security section.

11 The co-chairs of your domain's Technical Committee will provide guidance as to where to archive the completed risks assessment and mitigation table.

3.3 Link with audit trail definition

For most of the infrastructure and workflow profiles, the ATNA profile will play an important role in the risk mitigation plan. If so, you are also in charge of defining the audit records for your profile. When needed, audit records should be defined for each transaction of a profile and detail which events lead to the recording of audit trail and which data should be recorded. The risk assessment helps you in the definition of the audit trail as it outlines the adverse event you want to be able to identify through the audit trail.

For example, in XCA one of the mitigations against inappropriate disclosure of repository documents is the use of audit trails through grouping with ATNA actors. Audit trails should be defined for the XCA transactions dealing with repository documents to allow mitigation of that risk (i.e. finding in the audit trails who did access the inappropriately disclosed documents).

The audit trails defined should follow the formats defined for ATNA audit trails (see ITI TF-2: 3.20.7).

See ITI TF-2 section 3.15.4.1.4 on audit trails for provide and register document set or ITI TF-2 section 3.22.4.1.4.1 on audit trails for patient demographics for examples.

3.4 When and how to update a security section

Each time a profile is updated (through CP for instance), the profile author should assess whether the change affects the assessed risks. If so, the author should update the risk assessment and mitigation tables and possibly the Security Considerations section(s) to take the change into account.

White Paper Drafting Team

Drafting team:	Gila Pyke (SSHA)
	Glen Marshall (Siemens)
	John Moehrke (GE Healthcare)
	Robert Horn (AGFA)
	Lori Reed-Fourquet (e-HealthSign)
	Yaron Derman (SSHA)
	Steve Daniels (Siemens)
	Goeff Pascoe (Phillips)
	Manuel Metz (GIP-DMP)
	Lynn Felhofer (NIR)
	Karen Witting (IBM)
	James McInnis (Siemens)

Acknowledgements

The tremendous effort made by the members of the IHE ITI Planning Committee, who arranged several teleconferences at the onset of the process, and their valuable contributions are acknowledged with thanks. The significant contributions made by the Smart Systems for Health Agency Risk Management Department and representatives from the IHE ITI Planning Committee at these teleconferences greatly assisted in the creation of this document.

Bibliography

This bibliography lists helpful materials that can be used as a basis for devising scenarios.

http://www.crypto.com/bingo/pr

IEC 60812 Ed. 1.0: Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)

NIST SP 800-30: Risk Management Guide for Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

ISO 14971:2000: Application of risk management to medical devices http://konark.gsoi.med.ge.com/quality/QS/Regulatory_standards/ISO14971.pdf

ISO 17799 (2000) Information Technology - Code of practice for information security management

MIL-STD-1629A, Procedures for Performing a Failure Mode Effects and Criticality Analysis, November 24, 1980 Australian Standard AS4360:2004 Risk management

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework

Wikipedia: Risk Management http://en.wikipedia.org/wiki/Risk_management

OODA: Observe Orient Decide Act

IEC 61025 Fault Tree Analysis

IEC 61882 HAZOP Application Guide

Carnegie Mellon Software Engineering Institute, Software Risk Evaluation

