Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Note

Risk Methods and Tools for Identity Management Systems

Deliverable D3.1 in Petweb II

Note no DART/06/13
Author Ebenezer Paintsil
Date January 7, 2014

The author

Ebenezer Paintsil is currently a researcher at Norwegian Computing Center (NR). He received MSc and LLM from University of Oslo and begun his PhD 2010. He worked on privacy and security risks analysis in identity management systems and was part of the part of the Norwegian Information Security Laboratory (NISlab) at University of Gjovik.

Norwegian Computing Center

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
Office address
Gaustadalléen 23
NO-0373 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Title	**Risk Methods and Tools for Identity Management Systems – Deliverable D3.1 in Petweb II**
Author	**Ebenezer Paintsil**
Quality assurance	Wolfgang Leister, Lothar Fritsch
Date	January 7, 2014
Publication number	DART/06/13

Abstract

The objective of this report is to test two classic risk analysis methods, namely Mehari and AICPA/CICA, using identity management scenarios in order to determine their suitability for risk analysis in IDMSs. In addition, the report compares these two classic methods to the Conflicting Incentives Risk Analysis (CIRA) method and the Executable Model-Based Risk Analysis Method (EM-BRAM) developed under the PetWeb II project. The comparison shows that the two classic risk analysis methods are useful for determining administrative and management controls for IDMSs. They are expensive because their main inputs for the analysis are obtained from extensive assessment of an organization and collaboration with system stakeholders. Their risk analysis method is based on subjective intuitions of risk assessors and therefore less accurate for security decisions. On the other hand, the EM-BRAM is useful for determining technical privacy and security risks in IDMSs. It analyzes technical systems rather than administrative and management procedures. EM-BRAM reduces subjectivity by relying on system characteristics for the risk analysis. There are indications that it is less expensive because the main inputs for analysis are a system specification and predetermined risk model. The CIRA method is useful for analyzing stakeholders' risk based on their perceived incentives. It is similar to the classic risk analysis methods except that it could reduce subjectivity by trading a risk assessor's subjective probabilities for a stakeholder's perceived incentives.

Keywords	risk analysis, tools, identity management, comparison
Target group	Participants
Availability	Open
Project	PetWeb II
Project number	320426 – NFR 193939/S10
Research field	Privacy and Security
Number of pages	40

Contents

1 Introduction

Identity management systems (IDMSs) create and manage identities of end-users (Jøsang and Pope, 2005). IDMSs have three main stakeholders – the system end-users, who create or obtain and show credentials; the identity provider (IdP), the organization that issues the credentials to end-users; and the service provider (SP); the organization that provides services or resources to end-users after verifying their identities. SPs may be referred to as relying parties (RPs).

The choice of an IDMS has severe consequences on the way personal data is used, stored, combined and misused. The PETWeb II (Privacy-respecting Identity Management for e-Norge) project aims at providing scientific support for the choice of identity management approaches, in particular by supporting the analysis of specific technical and regulatory risks relating to the choice of an identity management approach.

The analysis of specific technical and regulatory risks requires suitable tools to be successful. Currently, we have over 200 classic IT-Security risk management methods (Matulevicius et al., 2008) and numerous tools. Many of these tools focus on analyzing the administrative processes and management procedures in organizations. These tools are developed for organizations of different sizes and business models (Smojver, 2011). In addition, they cover different phases of risk analysis and concentrate on different aspects, problems or business areas (Taubenberger et al., 2011).

Risk analysis can assist system stakeholders to choose a privacy enhancing IDMS based on their privacy and security preferences (Lund et al., 2011). It can enable system stakeholders to be aware of their privacy and security risks as they use a particular IDMS. The classic IT-Security risk management methods and tools can assist management and system administrators to understand the safety and security of their organizations. However, the extent to which they can assist system stakeholders to select a privacy and security enhancing system has not been duly established. Hence, the objective of this report is to test the extent to which the classic risk analysis tools can be employed to analyze security and privacy risks in IDMS. We then compare the outcome of the test to the Conflicting Incentives Risk Analysis (CIRA) method (Rajbhandari and Snekkenes, 2012a) and the Executable Model-Based Risk Analysis Method (EM-BRAM) for IDMSs (Paintsil and Fritsch, 2013) developed under the PetWeb II project. The CIRA method analyzes risk from stakeholders' perspectives while the EM-BRAM analyzes risk from systems' perspective.

The rest of the report is structured as follows: Section 2 introduces the two classic risk analysis methods and tools. In addition, it provides an overview of the IDMSs' scenarios and how the two methods were tested on them. Section 2.4 discusses the application of the classic risk analysis methods to federated IDMSs. Section 3 introduces the executable model-based risk analysis method. Section 4 introduces the conflicting incentives risk analysis method. Section 5 presents a comparison of the two different risk analysis methods developed under the PetWeb II project to the classic risk analysis methods. Finally

Section 6 concludes the report.

2 Mehari and AICPA/CICA Tools

This section introduces the Mehari (Jouas et al., 2012) and the AICPA Risk Analysis Tool (AICPA/CICA, 2010). We chose these two tools because they are freely available and complement each other. While Mehari enables extensive security risk analysis, the AICPA/CICA Risk Analysis Tool focuses on privacy risk analysis.

2.1 Mehari

MEHARI stands for Méthode Harmonisée d'Analyse des Risques – Harmonised Risk Analysis Method. It is a method for risk analysis and risk management created by CLUSIF (French association of information security professionals) (Jouas et al., 2012).

The main objective of Mehari is to identify all risks in an organization, quantify the level of each risk, and take measures to reduce the risk to an acceptable level. It implements tools to track risks and their levels and to ensure that each risk is mitigated. Mehari implements the ISO27005 (ISO, 2008b) risk analysis framework in full. This means Mehari provides specific method for risk assessment, treatment and management processes.

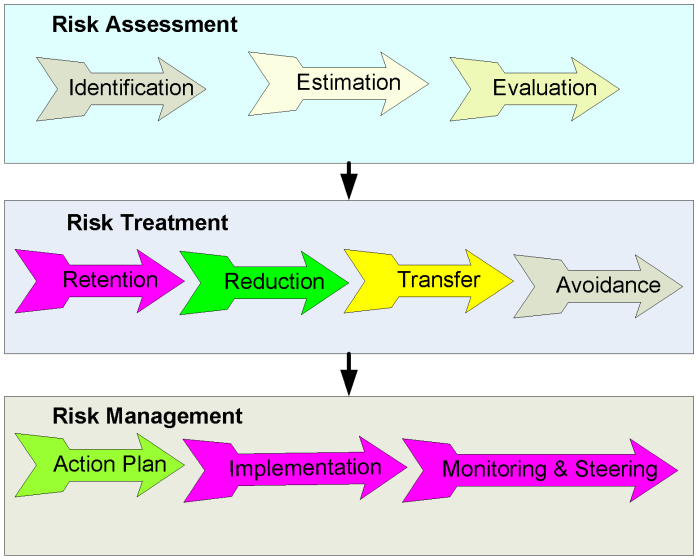

Figure 1. Mehari (Jouas et al., 2012)

Figure 1 shows the Mehari risk management stages and processes. The first stage is the risk assessment. Risk assessment consists of risk identification, estimation and evaluation. The risk identification identifies and characterizes elements of risk to enable risk estimation. It identifies assets, vulnerabilities of each asset, asset damage and threats (Jouas et al., 2012).

Mehari classifies assets into two groups – primary and secondary. Primary assets are categorized into three main groups – IT services, data necessary for the services to function

and management processes. The secondary assets are physical or concrete equipment, tools, processes or services required to meet the functional needs of an organization. The primary asset is the main input for the risk tool.

After the identification of assets, the intrinsic vulnerability of these assets is determined. Intrinsic vulnerability refers to a weakness in a system that can be exploited by an adversary. The damage that may occur as a result of exploitation of the unavailability, lack of confidentiality or integrity is also identified. Type of events or threats that can exploit vulnerabilities in the identified assets are also identified. The risk identification results in a list of risk and scenarios to evaluate.

The risk estimation establishes the metric for determining the impact and the likelihood of the risk occurring. In addition, it involves the development of effectiveness scales for the different risk reduction factors. This reference model or metrics is employed to estimate the risk in the organization.

The estimated risk is evaluated in order to determine whether the risk is acceptable. This is done with well structured process in order to ensure reliability.

The second stage of the risk analysis is the risk treatment process, in which the risk assessor takes a decision whether to transfer, reduce, avoid, or retain the risk.

The final stage focuses on risk management. It involves all processes that facilitate implementation of decisions regarding the risk treatment and monitoring of the effect of these decisions and improving them if necessary.

2.2 Risk Analysis in Identity Management Systems with Mehari Tool

This section describes the risk assessment in a Webmail IDMSs using the Mehari tool. We analyze a WebMail scenario in a medium size organization. The webmail system allows employees to access their email online and outside the organization's local area network. The system administration unit is the owners of the webmail system in the organization. It runs and manages the system.

We begun the analysis of the webmail system by establishing the context and the scope. We limited the scope to only the system administration unit. We took the head of the unit through an initial training to enable the head understand the Mehari method and tool. This was followed by risk identification. Risk identification is a crucial part of the Mehari method but occurs outside the Mehari tool. It identifies the primary and secondary assets as well as processes, goals and expected results. In addition, the risk assessor together with the system administrators identifies possible malfunctions of assets and their seriousness levels. Table 1 shows the results of the risk identification.

Primary Asset	Process	Goals and Expected Results	Malfunction	Seriousness Level	Secondary Asset
Data	Database	Store, process and allow retrieval of data such that webmail can function	Unable to function as intended	2-serious	Database server
Services	Authentication	Identify and authorize users in order to prevent unauthorized access	Unable to function as intended	2-serious	The exchange authentication software
	Web service (IIS)	Enable the email services run on the web in order to allow global email access	Unable to function as intended	2-serious	Server, the exchange authentication software
	Backup	Backup emails to prevent future emergencies	Unable to function as intended	1-not significant	Backup server and software
	Webmail service	Allow global access of emails	Unable to provide mail service	2-serious	Exchange server
	WAN	Allow external access to the webmail	Unable to function as intended	2-serious	Routers or gateway
	LAN	Enable local access to the webmail	Unable to function as intended	2-serious	Switches
	Disposal of equipment	Ensure that no data is leaked	Unable to function as intended	1-not significant	Personnel and routines (doc)
	IT services	Support the webmail service	Unable to function as intended	3-serious	Procedures, wiki
	Anti-virus	Protect the server from viruses to avoid disruption of the webmail services	Unable to function as intended	3-very serious	Antivirus server and software
Management processes	Personal Data	Enable security of personal data	Unable to protect personal data	3-very serious	Procedures, tools and necessary resources
	Financial communication	Ensure secure communication of financial record	Unable to secure financial communication	Unable to protect secrecy of financial data	Procedure and tools
	Computing system	To secure the computing system	Unable to secure computing systems	2-serious	Tools and procedures

Table 1. Risk Identification Table

In Table 1, the primary assets identified are data, services and management processes. The second column of the table shows the processes for various categories of assets. The goal and expected results describe the goals of each process and the expected outcome if the goal is achieved. Column four of the table describes possible malfunctions that could occur in the process. The seriousness level describes the seriousness of a malfunction. For simplicity, only one value is stated for each process instead of the range 1 to 4. The last column is the secondary assets for each process. They describe specific assets that support the processes.

The next stage is the risk estimation and evaluation. Mehari provides Microsoft Excel tool support for risk estimation and evaluation. The tool has many worksheets but we focus on only the risk assessment tools or worksheets which are the Intro, T1, T2,T3, Classif, Expo and the Scenario worksheets.

The Intro worksheet describes the risk management modules, plans, parameters and permanent elements available for the Mehari method. It allows the risk assessor to select appropriate modules, plans or parameters for the risk analysis. This work focuses on risk assessment, so we select the stake analysis and classification, and the risk analysis modules.

Table T1		CLASSIFICATION OF DATA																														
Business processes, domains of application or activity, Common services	FONCTION (description)	Application data (data bases)			Application data individually sensible (transient,			Shared Office data			Personal Office data			Personal docu ments		Listings or prints	Electronic mail			Snail mail Fax			Archived docu ments		Digitalized archives			web data on-line (external or internal)		
		A	I	C	A	I	C	A	I	C	A	I	C	A	C	C	A	I	C	A	I	C	A	C	A	I	C	A	I	C
	Asset type	D01	D01	D01	D06	D06	D06	D02	D02	D02	D03	D03	D03	D04	D04	D05	D07	D07	D07	D08	D08	D08	D09	D09	D10	D10	D10	D11	D11	D11
Business Process																														
Domain 1 : System Administration Unit	Secondary	2	2	2	1	2	1				2	2	2	2	2		2	2	2									2	2	2
Domain 2 :																														
Domain 3 :																														
Domain 4 :																														
Domain 5																														
Domain 6 :																														
Domain 7 :																														
.../...																														
Domain N																														
Transverse Processes																														
Overall Management & policy																														
Classification		2	2	2	1	2	1				2	2	2	2	2		2	2	2									2	2	2

In order to add or suppress a business domain or process, use the line "add" or "suppress" functions.
The classification level is a value from 1 to 4, the maximum in each column is automatically copied out in the "classification" line and reproduced into the "intrinsic impact table" (tab: Classif) for each type of data and criteria (A, I or C).

Figure 2. T1 Worksheet (Jouas et al., 2012)

Figure 2 shows the T1 worksheet of the Mehari tool. The data in the table (T1) was supplied by the head of the system administration unit of the organization with the help of the risk assessor. Columns with labels A, I, C are for estimating the effect of loss of availability (A), integrity (I) and confidentiality (C) respectively. T1 focuses on data used to support business or system processes in an organization. This process is repeated for the other columns in T2 and T3. The tables for T2 and T3 are not shown.

Figure 3 depicts the intrinsic impact worksheet (Classif). It shows the impact of the loss of availability, integrity or confidentiality of the assets necessary for running of the webmail processes in the organization. The Mehari tool automatically generates the impact table

Intrinsic Impact table					Asset selection
Data and information assets		**A**	**I**	**C**	
Data and information					
D01	Data files and data bases accessed by applications	2	2	2	1
D02	Shared office files and data				0
D03	Personal office files (on user work stations and equipments)	2	2	2	1
D04	Written or printed information and data kept by users and personal archives	2		2	1
D05	Listings or printed documents				1
D06	Exchanged messages, screen views, data individually sensitive	1	2	1	1
D07	electronic mailing	2	2	2	1
D08	(Post) Mails and faxes				0
D09	Patrimonial archives or documents used as proofs				0
D10	IT related Archives				0
D11	Data and information published on public or internal sites	2	2	2	1
Service assets		**A**	**I**	**C**	
General Services					
G01	User workspace and environment				0
G02	Telecommunication Services (voice, fax, audio & videoconferencing, etc.)				0
IT and Networking Services					1
R01	Extended Network Service	2	1		1
R02	Local Area Network Service	2	2		1
S01	Services provided by applications	2	2	2	1
S02	Shared Office Services (servers, document management, shared printers, etc.)				0
S03	Users' disposal of Equipments (workstations, local printers, peripherals, specific interfaces, etc.) **Nota : Applies to a massive loss of these services, not for one or few users.**	1	2		
S04	Common Services, working environment: messaging, archiving, print, editing, etc.	2	2		1
S05	Web editing Service (internal or public)				1
Management process type of assets		**E**			
Management Processes for compliance to law or regulations					
C01	Compliance to law or regulations relative to personal information protection	1			1
C02	Compliance to law or regulations relative to financial communication	1			1
C03	Compliance to law or regulations relative to digital accounting control				0
C04	Compliance to law or regulations relative to intellectual property				0
C05	Compliance to law or regulations relative to the protection of information systems	1			1
C06	Compliance to law or regulations relative to people safety and protection of environment	1			1

Figure 3. Mehari Classif Worksheet (Jouas et al., 2012)

in Figure 3 from the worksheets T1,T2 and T3. The assets selection column in the impact table allows the risk assessor to select assets that are directly relevant for the analysis. An asset selection value of 1 means the asset is relevant for the risk analysis otherwise the asset is not relevant.

The values in Figure 3 ranges from 1 to 4. The value 2 is interpreted as medium impact and 4 as very high impact.

Table of events : types of events and natural exposure

Family type	*Code type*	*Event description*	*Code*	*Natural exposure (standard CLUSIF)*	*Natural exposure (decided)*	*Natural exposure (resulting)*	*Selection*
Absence of personnel due to an accident	AB.P	Absence of personnel from partner	AB.P.Pep	3		3	0
		Absence of internal personnel	AB.P.Per	2		2	0
Absence or unavailability of service, due to an accident	AB.S	Absence of service : Air conditioning	AB.S.Cli	2		2	0
		Absence of service : Power supply	AB.S.Ene	3		3	0
		Absence of service : Impossibility to have access to the premises	AB.S.Loc	2		2	0
		Absence or impossibility of application software maintenance	AB.S.Maa	3		3	0
		Absence or impossibility of information system maintenance	AB.S.Mas	2		2	0
Environmental serious accident	AC.E	Lightning	AC.E.Fou	2		2	0
		Fire	AC.E.Inc	2		2	0
		Flooding	AC.E.Ino	3		3	0
Hardware accident	AC.M	Equipment breakdown	AC.M.Equ	3		3	1
		Accessory equipment breakdown	AC.M.Ser	3		3	0

Figure 4. Mehari Expo Worksheet (Jouas et al., 2012)

The Expo worksheet in Figure 4 allows the risk assessor and the system stakeholders to select the relevant events that may threaten the relevant assets identified in Figure 3. In Figure 4, the directly relevant events are set to 1 while others are set to 0. After the selection, the Mehari tool automatically update the scenario worksheet in Figure 5.

	Consideration of Security services if 1 :																		
DESCRIPTION				Intrinsic values			security measures				decided values			calculated values					
	Direct Selection	Type AEM	Type AICE	Impact	Exposure	seriousness	Dissuasion	Prevention	Confining	Palliation	Confinability	Impact	Likelihood	Impact	Likelihood	seriousness	Accept (A) or transfer (T)	Seriousness for plans	
Accidental erasure of files of data, due to a production incident	0	A	A	2	3	2	1	1	1	3	1			2	3	0		0	
Erasure, due to an error, of files of data, by a user authorized legitimately, connected from the internal network	0	E	A	2	3	2	1	1	1	3	0			2	3	0		0	
Erasure, due to an error, of files of data, by a user authorized illegitimately, connected from the internal network	0	E	A	2	3	2	1	1	1	3	0			2	3	0		0	
Erasure, due to an error, of files of data, by a user not authorized, connected from the internal network	0	E	A	2	3	2	1	1	1	3	0			2	3	0		0	
Erasure, due to an error, of files of data, by a member of the production team, connected from the internal network	0	E	A	2	3	2	1	1	1	3	0			2	3	0		0	
Erasure, due to an error, of files of data, by a member of the maintenance team , connected from the internal network	0	E	A	2	3	2	1	1	1	3	0			2	3	0		0	
Malicious erasure of files and backups of data, by a user authorized legitimately, connected from the internal network	1	M	A	2	2	2	1	1	1	3	0			2	2	2		2	
Malicious erasure of files and backups of data, by a user authorized illegitimately, connected from the internal network	1	M	A	2	2	2	1	1	1	3	0			2	2	2		2	

Figure 5. Mehari Scenario Worksheet (Jouas et al., 2012)

Similarly, the relevant scenarios are selected from the "direct selection" column in Figure 5. The intrinsic "seriousness" column of Figure 5 determines the risk of the each

scenario before security control is applied while the "Calculated values" seriousness determines the risk after an application of security measures in the "Security measures" columns. Each risk is evaluated with build-in security measures. Figure 6 shows the metric for the seriousness level.

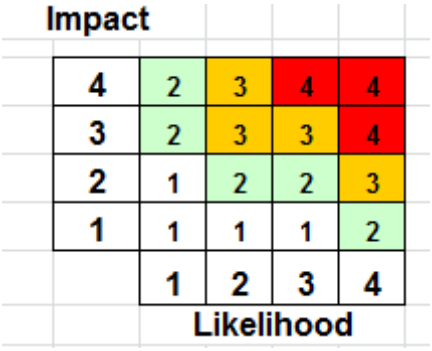

Figure 6. Mehari Seriousness Worksheet (Jouas et al., 2012)

2.3 AICPA/CICA

This section shows how the AICPA/CICA (AICPA/CICA, 2010) privacy risk assessment tool can be used to analyze the risks of a webmail system in an organization. The AICPA/CICA privacy risk assessment tool is developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) to help CPAs and Chartered Accountants (CAs), management, owners and other privacy professionals to analyze privacy risk effectively and comprehensively. Unlike Mehari, the AICPA/CICA method is meant for privacy risk analysis. The scenario for the analysis is the same as the one in Section 2.2.

2.3.1 Risk Analysis of a Webmail Identity Management System

The AICPA/CICA (AICPA/CICA, 2010) tool consists of two main excel tables – the risk assessment and the scoring tables. The risk assessment tool uses ten principles and 73 criteria for the analysis. The snapshot of the risk assessment tool or table is shown in Figure 7.

The scores in Figure 7 were provided by the head of the system administration after initial training. During the training, the risk assessor who has a legal background introduced and guided the head of the system administrator to provide the input. The stakeholders examined and analyzed the implications of various documents necessary for the analysis. The method or tool requires ten users. However, for the purpose of our evaluation we focus on one user only. In addition, we consulted other stakeholders in the organization for their inputs.

Figure 8 is the scoring summary table. The table automatically aggregates the individual scores and generates the average score for each privacy principle. Figure 8 shows the average score of the analysis on Row 5 – "Average Score -14 Criteria". The average score is between 2 and 8. The results shows that the organization has high likelihood of failure (6.1), medium impact (4.6) and cost of mitigation (4.4).

	A	B	C	D	E
1	AICPA and CICA GAPP Privacy Risk Assessment Tool				
2	Scoring Input Template for 73 GAPP Criteria				
3	Instructions:				
4	1. Use a separate Scoring Input Template for each person participating in the assessment.				
5	2. Enter a risk score for each GAPP criteria. (2=Low Risk, 5=Medium Risk, 8=High Risk)				
6	3. Do not change the file name when you save the file.				
7	4. Copy the completed Scoring Input Template into the AICPA Privacy Folder.				
8					
9			Scoring: 2=Low Risk, 5=Medium Risk, 8=High Risk		
15	GAPP - 73 Criteria	Criteria Description	Likelihood of a Control Failure	Business Impact	Effort/Cost to Mitigate
16	1.0 MANAGEMENT (14 criteria)	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.			
17	Privacy Policies (1.1.0)	Policies are defined for: notice, choice/consent, collection, use/retention/disposal, access, disclosure, security, quality, and monitoring/enforcement.	5	8	2
18	Communications to Internal Personnel (1.1.1)	Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	8	2	2
19	Responsibility and Accountability for Policies (1.1.2)	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	8	2	5
20	Review and Approval (1.2.1)	Privacy policies and procedures, and changes thereto, are reviewed and approved by management.	8	5	5

Figure 7. AICPA/CICA Risk Assessment Tool (AICPA/CICA, 2010)

	A	B	C	D	E
1	Privacy Risk Assessment Scoring Summary - Management Principle AICPA and CICA GAPP				
2					
3			Scoring: 2=Low Risk, 5=Medium Risk, 8=High Risk		
4	1.0 Management	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.	Likelihood of a Control Failure	Business Impact	Effort/Cost to Mitigate
5	14 Criteria	Average Score - 14 Criteria	6.1	4.6	4.4
6	Privacy Policies (1.1.0)	Policies are defined for: notice, choice/consent, collection, use/retention/ disposal, access, disclosure, security, quality, and monitoring/enforcement.			

Figure 8. Scoring Summary Table (AICPA/CICA, 2010)

2.4 Application of Mehari and AICPA/CICA in Federated IDMSs

Federated IDMSs have at least two administrative domains or organizations – service provider (SP) and the identity provider (IdP) domains. Mehari and AICPA/CICA methods focus on risk analysis in a single organization. This means the federated scenario may require risk analysis in at least two different organizations. The cost involved in the analysis is likely to increase because of the number of organizations involved. Mehari and AICPA/CICA methods do not prescribe any method for combining the risk results from multiple domains. Hence the global risk assessment picture cannot be determined with these methods.

Moreover, how laws and regulations are implemented within and across administrative domains will be critical to the risk analysis.

In the Mehari risk analysis method, business processes regarding shared office data, prints, emails and archiving may be very relevant in the federated IDMSs. In addition, external network, application, shared office, telecommunication, web editing services and working environment would become more relevant.

Risk scenarios are created for a single organization and therefore may require modifications. Additional events such as absence of personnels, power and air condition will be important for the analysis because of the large amount of resources involved in running a federated system.

3 Executable Model-Based Risk Analysis Method

This section introduces the executable model-based risk analysis method (EM-BRAM) for IDMSs developed as part of the PetWeb II project.

Privacy enhancing IDMSs can facilitate successful service delivery in both organizations and government institutions (McKenzie et al., 2008). Organizations can gain competitive advantage and reduce financial losses if they can enhance privacy and security in IDMSs. Similarly, government institutions can gain better trust of their citizens if they can do the same.

The objective of risk analysis is to identify and assess all risks in order to suggest a set of controls that will reduce these risks to an acceptable level (Gerber and von Solms, 2001). Information security requires an analysis of requirements for the protection of information assets and application of appropriate controls or countermeasures to ensure the protection of these information assets (ISO, 2008a). The EM-BRAM is meant to do the same. It identifies possible privacy and security risks contributing factors in IDMSs and analyzes if these factors exist in a targeted IDMS so that identified countermeasures can be implemented to reduce the system's risk to an acceptable level.

EM-BRAM is a model-based risk analysis method Lund et al. (2011). Model-based risk analysis methods employ graphical models to mainly facilitate participation, risk com-

munication and documentation and thereby enhance the risk analysis process. They structure and present information at an appropriate level of abstraction for communication among all system stakeholders.

3.1 Risk Identification and Modeling Phase

EM-BRAM relies on the characteristics of information flow to develop a security and privacy risks model for IDMSs. We refer to information that flow in an IDMS as tokens. Tokens are technical artifacts providing assurance about an identity (Paintsil and Fritsch, 2011). They are personal data sources and gateways to resources (Naumann and Hogben, 2009). A token can be an identifier such as username, a claim such as a password, an assertion such as SAML tokens, a credential such as a X.509 certificate or combinations of these.

New Protection Goals	Category of Factors	Factors
Confidentiality, Unlinkability	Frequency & duration of use	one-time, multiple times, life time
Integrity, Confidentiality, Intervenability	Provisioning	created, updated, deleted or archived attribute with: limited personal data, overloaded personal data, sensitive personal data
Unlinkability	Purpose of use	application specific, single sign-on, multiple services, context specific, silo
Intervenability, Unlinkability	Assignment & Relationship	forced, self, jointly-established, role, pseudonym
Confidentiality	Secrecy	inferable, public, obfuscated, revocable, recoverable,
Confidentiality	Claim Type	password, crypto key, biometric, challenge-response, single-claim, multiple-claims
Availability, Confidentiality	Mobility	copyable, remotely usable, concurrently usable, immobile
Availability	Value at Risk	loss, misuse, disclosure, disruption, theft, replacement value
Transparency	Obligation & Policy	policy absence, policies present

Table 2. Mapping of the Risk Factors and the New Protection Goals

The risk model for IDMSs is based on the simple and user-friendly use and misuse cases (UMCs) (Sindre and Opdahl, 2004). UMCs make human judgments more informed and systematic (Alexander, 2002; Elahi and Yu, 2009). They appeal to the industry because of the substantial connection of use cases to existing system development processes (Okubo et al., 2009). However, UMCs lack privacy constructs and quality goals, hence we the extended UMC modeling approach to include them. We refer to the new modeling approach as an extended misuse cases (EMCs) modeling approach (Paintsil, 2012b).

EMCs extend misuse case diagram with the terms "asset", "goal" and the privacy construct "right" in order to model privacy and security risks in IDMSs. In addition, the model is refined and implemented using colored petri nets (CPNs) (Jensen and Kristensen, 2009) as shown in Figure 11. The CPNs model is executable (can be simulated) and can communicate or represent the dynamic behaviors of actors and adversaries to all system stakeholders.

We obtain the results in Table 2 from the Delphi study. Table 2 is a taxonomy of risk contributing factors for privacy and security risks analysis in IDMSs. Each of the risk contributing factor is explained in Paintsil (2012a).

The third and second columns of the table show the risk contributing factors and their categories respectively. The first column of the table maps the risk factors to the new protection goals (NPGs) Rost and Bock (2011). The mapping aligns the risk contributing factors and their categories to the NPGs in order to show that the taxonomy is relatively comprehensive. Furthermore, the mapping can aid communication among legal and technical experts involved in privacy and security risks analysis Zwingelberg and Hansen (2012).

The NPGs provide technically convertible principles that cover both security and privacy protections Rost and Bock (2011),Zwingelberg and Hansen (2012). The NPGs extend or complement the classical security goals – integrity, availability and confidentiality, by adding central privacy concepts which are transparency, unlinkability, and ability to intervene (Intervenability).

Transparency requires that the purpose of data processing is comprehensible by all stakeholders Rost and Bock (2011), Zwingelberg and Hansen (2012). Unlinkability verifies if personal data collected for a particular purpose is being used for another purpose or personal data is unlinkable to any other set of privacy-relevant data outside a domain or context. The ability to intervene (intervenability) gives the data subjects or parties the ability to control or intervene in the processing of their personal data.

The NPGs complement each other but conflicts can arise in their implementation Zwingelberg and Hansen (2012). Identifying and understanding such conflicts are a prerequisite for developing adequate and a balanced risk analysis model.

Figures 9 and 11 depict the risk model for the EM-BRAM (Paintsil, 2012b). The modeling approach is based on the EMCs modeling. An EMC model identifies the use and misuse cases and how they align with security goals or requirements. It models risk categories (in Table 2) that enforce privacy as "rights" while that of security as "assets".

Risk factors are represented by misuse cases. They are factors that can contribute to risk in IDMSs. These factors can be vulnerabilities or threats. Note that the meaning of misuse cases is slightly altered to simplify the EMC model. Similarly, use cases represent controls or countermeasures. Factors that protect a system goal(s) are presented by use cases or countermeasures while those that threaten a system goal are the misuse cases.

Figure 9 shows a generic model of the EMCs model. Here, an asset is what we want to

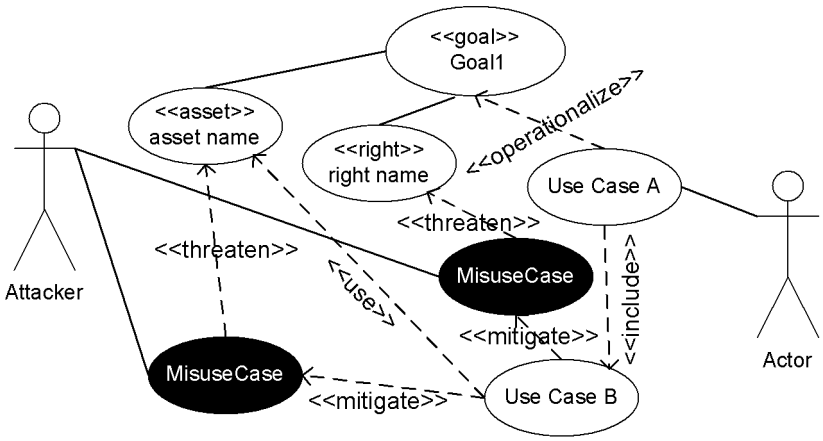

Figure 9. Extended Misuse Cases Modeling Paintsil (2012b)

protect or something that may advance a system goal. An asset is represented by its name and the stereotype $\ll asset \gg$. A use case may use an asset as a data object or a resource to accomplish a task (Okubo et al., 2009). This is represented by the dotted line and the stereotype $\ll use \gg$. The second extension is the "right". It is represented by its name and the stereotype $\ll right \gg$. "Right" incorporates privacy concepts into the model. While security modeling focuses on assets' or protection of security goals, privacy on the other hand focuses on both security and right protection (Mitrano et al., 2005; Paintsil, 2011). Hence, the stereotype $\ll right \gg$ distinguishes the model from the traditional security models.

A misuse case may threaten a right or an asset Sindre and Opdahl (2004). A use case may mitigate a misuse case and may help operationalize a system goal. Goal operationalization is represented by the stereotype $\ll operationalize \gg$. A system goal is operationalized if all its known misuse cases are mitigated with appropriate use cases or countermeasures. A goal represents the reasons why we need to protect an asset or a right from misuses. A goal is represented by a name and the stereotype $\ll goal \gg$. It may consist of sub-goals. If a goal is associated with an "asset" or "right" then it means that the goal is intended to protect the asset or the right from misuses.

Figure 10 shows an example EMCs model for the "Value at Risk" and the "Mobility" risk categories or factors identified during the risk identification phase of the risk method. They are explained as follows:

Token Mobility. The Token Mobility risk category indicates the degree of mobility of a token. The degree of mobility refers to how easy it is to copy a token or its content, the physical constraints regarding the movement of the token, among others. For example, the content of a low cost RFID tag with no additional security could easily be read by anyone. In contrast, a more expensive RFID tag that comes with additional security may ensure that only authorized readers have access to its content. Various forms of mobility create risk in IDMSs. We assess the contributions of token mobility to privacy and security risk according to the following:

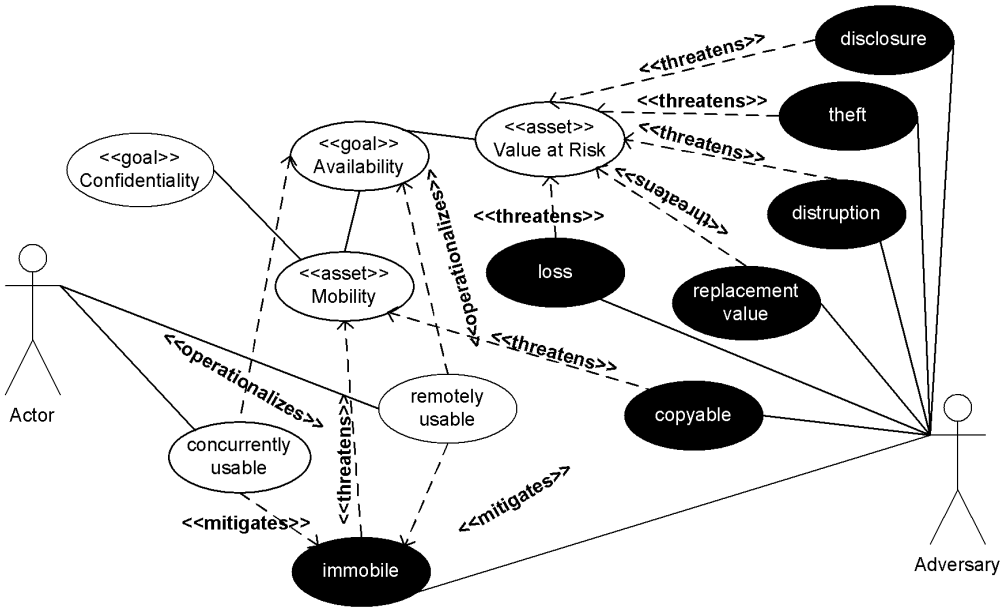

Figure 10. Executable Extended Misuse Cases Model for Mobility and Value at Risk Category

1. *Copyable*: the token can be copied with limited effort.
2. *Remotely usable*: the token can be used for remote identity management.
3. *Concurrently usable*: the token can be used concurrently in many parallel sessions, transactions, or applications.
4. *Immobile*: a token is not 'mobile', if it must be physically presented.

Token Value at Risk. Finding assets and the value of the assets at risk is an important part of risk analysis ISACA (2009). Tokens are assets and their value at risk can contribute to privacy and security risks. Thus, we can quantify the risk of using tokens by assessing the significance of the token or the value of the token to the operation and security of an IDMS. We classify the value at risk Peterson (2006) as follows:

1. *Loss*: determines how much is at risk when a token is lost.
2. *Misuse*: determines how much is at risk when a token is used in wrongful ways.
3. *Disclosure*: determines how much is at risk when a token or token-related information gets known by someone else.
4. *Disruption*: determines how much is at risk when a token does not function.
5. *Theft*: determines how much is at risk when a token is stolen.
6. *Replacement value*: cost (effort, resources, time) to replace a token.

The EMC model in Figure 10 has two goals – "Availability" and "Confidentiality" goals. The "Value at Risk" category is aligned with the "Availability" security goal while the "Mobility" category aligns with the "Availability" and "Confidentiality" goals. The "Copy-

able" misuse case threatens the "Mobility" of tokens (asset) which in turn affects confidentiality of tokens. The "remotely usable" and the "concurrently usable" mitigate the "Immobile" misuse case and operationalize the "Availability" goal.

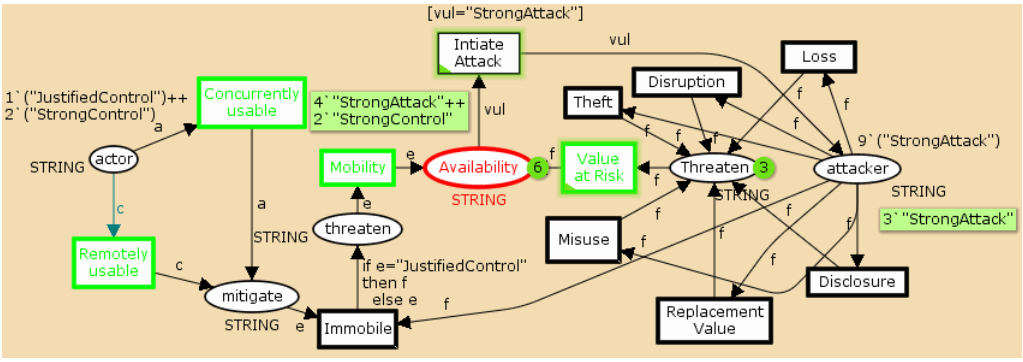

Figure 11. Colored Petri Nets Implementation of Executable Extended Misuse Cases Model

The EMC modeling can be refined and implemented with CPNs in order to precisely communicate the dynamic system behavior of system agents to stakeholders. Figure 11 is an example of the refined and precise version of an EMC model in Figure 10 with CPNs. The CPNs implementation converts the static EMC model to an executable risk model capable of precise and dynamic risk communication Jensen and Kristensen (2009). The CPNs model in Figure 11 implements the "Mobility" and "Value at Risk" risk categories explained above and focuses on the availability security goal.

In Figure 11, actors and adversaries are represented by places. The countermeasures for the actor are the use cases or the CPNs transitions (colored green). The misuse cses for the attacker or adversary are the black colored transitions. The "include", "mitigate", "threaten" and goals such as availability are modeled as places. Some of the misuse cases have countermeasures others are not. For example, token "loss", "theft", "disclosure", "misuse" and "replacement" misuses have no corresponding use cases or countermeasures. An adversary can always violate a security goal through these unmitigated misuse cases. The transition "Initiate Attack" is to enable or illustrate the continual attack by the adversary through the unmitigated misuse cases.

The initial markings "JustifiedControl" and "StrongControl" correspond to the perceived strength or capabilities of the actor's action. On the other hand, the initial marking "StrongAttack" corresponds to the perceived strength or capabilities of the attacker's actions. The token movement corresponds to the progress of an attack or the effect of the actor's countermeasures McDermott (2000). If an attacker's token reaches a goal (place) then the actor's countermeasure was ineffective.

In Figure 11, the multi-set 4'"StrongAttack" ++ 2'"StrongControl" indicates the behavior of the attacker (adversary) and the actor. If the actor's countermeasure is strong then he will operationalize or reach the system goal else the attack will succeed.

The execution of the risk model in Figure 11 can enable stakeholders to observe the dynamic behavior of the actors and adversaries. The risk model can be extended with ad-

ditional concepts and animation tier to communicate risk more effectively (Jensen and Kristensen, 2009).

3.2 System Modeling Phase

The second phase in the risk analysis is system modeling. EM-BRAM depends on the behavior or the characteristics of a targeted system to analyze privacy and security risks. Consequently, we model and validate a targeted IDMS with CPNs (Jensen and Kristensen, 2009) before the risk verification.

EM-BRAM relies on CPNs modeling because they stand out among the model-based formal methods, i.e., methods that rely on abstract state machine or state space analysis (Almeida et al., 2011; Xu and Kuusela, 1998). CPNs can hide large portions of complex mathematics and have a high degree of automation, thus making it relatively easy to learn and use. They provide tools for verification, validation and automatic analysis of system models (Jensen and Kristensen, 2009). CPNs tools are able to model, debug and test a large scale, critical and complex concurrent systems. They are suitable for a system that requires a large number of possible executions.

CPNs are graphical language supported by a tool with the capabilities of a high-level programming language. It includes time concepts making it suitable for performance analysis. They have a concise mathematical definition which contains very few but powerful primitives making it easy to learn, use and to develop strong analysis method by which properties of system models can be proved (Wang and Dagli, 2011). It is flexible in terms of token definition and manipulation. Various elements such as use cases, messages and task can be represented by different types of tokens.

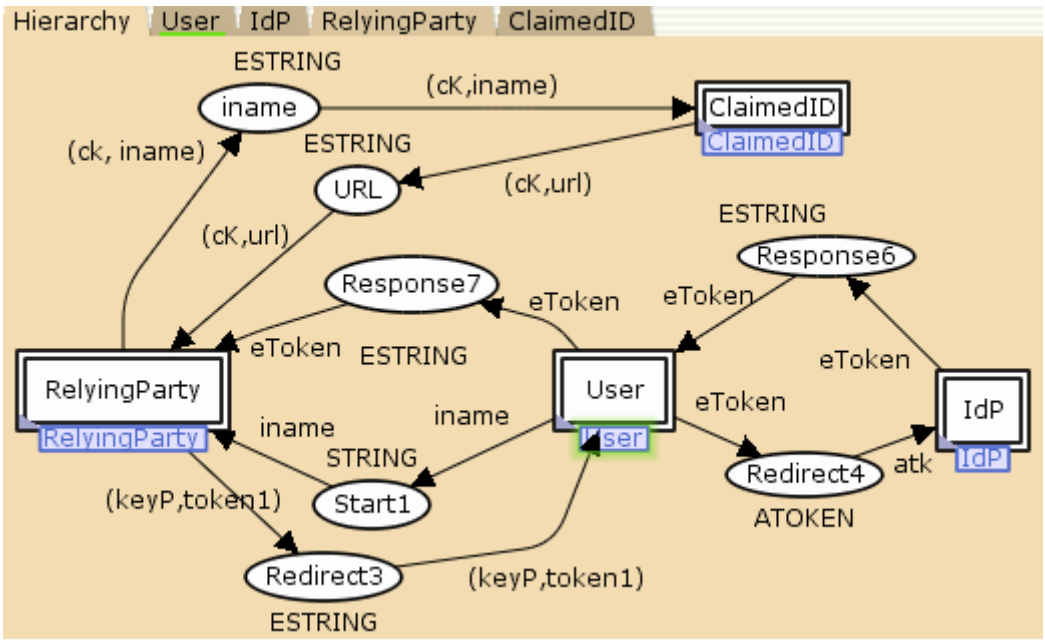

Figure 12. Hierarchical CPNs Model for OpenID

An example of a CPNs' system model for an OpenID IDMS is shown in Figure 12. It is a

hierarchical CPNs model for an OpenID IDMS scenario, as described by (Recordon and Reed, 2006). We use the hierarchical CPNs to make a large and complex system model manageable and compositional.

CPNs' models consist of **places, transitions (events), input and output** arcs. We represent the places by ellipses, transitions by rectangles, input/output arcs by directed arcs (Jensen and Kristensen, 2009). A place may hold a collection of tokens and may represent system conditions. A CPNs token is a variable with data type and a value. We refer to the data type as color set and the values as token colors. The set of tokens on all the places at a given moment represents the system state or marking. The transition represents the events or actions that can cause a system to change state. An arc serves as data input and output for a transition. It enables a transition to remove one or more tokens from an input place to an output place. When this happens, we say that the transition is fired.

The transitions with double lines are the substitution transitions. They are used to divide large model into sub-models. The substitution transitions represent the system agents – "User", "IdP", "'ClaimedID"' and "RelyingParty". For example, all the events and states in the entity "User" agent is represented by the "User" substitution transition in Figure 12. Here, the "RelyingParty" substitution transition is the service provider and the "IdP" is the IdP. The subsitution transitions are replaced by the detailed sub-models. An example of detailed sub-model is shown in Figure 13. Figure 13 depicts the "User" sub-model for the OpenID IDMS. The "Browser1" is the first transition to execute in the sub-model. It takes the "URL" from the "InitStart" place and sends it to the "RP". The "RP" is an output port so it sends the URL to the top-level substitution transition "RelyingParty" in Figure 12.

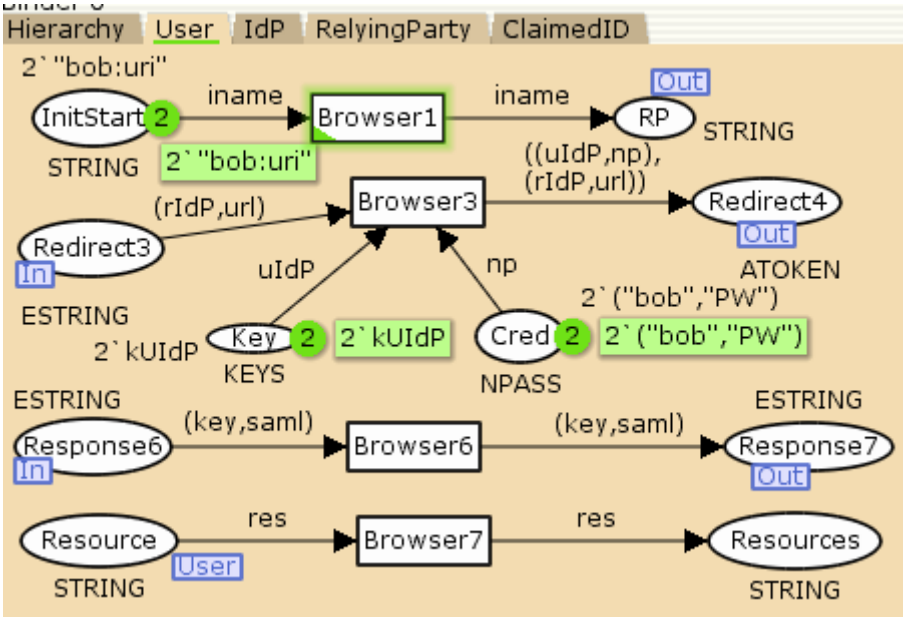

Figure 13. OpenID End-User Model

In Figure 12, the numbered places enable information flow among the system agents. For example, the place "Start1" allows information to flow from one sub-model to another.

3.3 Risk Verification Phase

The third phase of the EM-BRAM is risk verification. Here, we determine the existence of a possible risk in a targeted IDMS in order to select the appropriate privacy or security countermeasure from the EMC model to mitigate it.

The main objective of risk analysis is to identify and assess all risks in order to suggest a set of controls that will reduce these risks to an acceptable level (Gerber and von Solms, 2001). Traditionally, risk analysis requires estimation of likelihood of a threat manifesting and its impact. In cases where there is little data to validate the likelihood of a threat manifesting and its impact, risk assessors rely on their experience and subjective intuitions to estimate the likelihoods and impacts. This way of analyzing risk is not adequate to reduce the technical risk of a system or an organization to an acceptable level (Campbell, 1998; Gerber and von Solms, 2001).

EM-BRAM is not a classic or traditional risk analysis but a requirement analysis Gerber and von Solms (2001). Requirement analysis determines security requirements of a system and deduces the most suitable set of security controls from these requirements. EM-BRAM relies on the EMC risk analysis model above to perform a requirement analysis on a given IDMS in order to determine the countermeasures needed to secure the system.

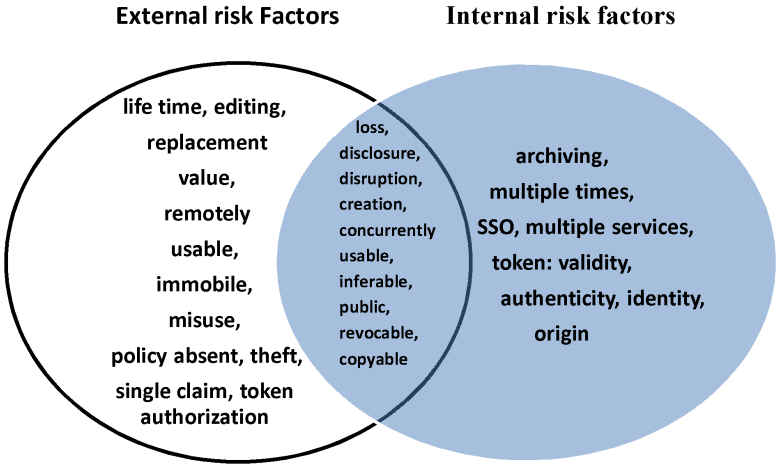

Figure 14. External and Internal Risk Factors (Paintsil, 2012a)

The misuse cases obtained from the risk identification and modeling phase (the first phase) are used as the inputs for the risk analysis or verification. The misuse cases are categorized into external and internal factors as shown in Figure 14. The internal characteristics serve as the inputs for the risk analysis of a given CPNs' model of an IDMS.

Figure 14 represents the potential risk contributing factors for IDMSs. The internal factors are those under the control of IDMSs while external factors are outside the control of the IDMS. While internal risk factors are verified with CPNs modeling in order to determine the appropriate privacy or security controls, the external factors may guide policy formulation. The intersection represents both internal and external factors.

We discuss the internal factors as follows:

Multiple times: In an IDMS, the activities of an end-user may be linked or profiled when she uses a token multiple times. Hence multiple uses of tokens create linkability or confidentiality risk.

Single sign-on/multiple services: A token used for multiple purposes or services may be subjected to illegal processing or abuse. IDMSs that support single sign-on (SSO) allow tokens to be used for multiple services sometimes in multiple domains upon a single authentication (Bauer et al., 2005). Although SSO reduces human error, it leads to sharing of valuable information across services or domains (Maler and Reed, 2008).

Creation/archiving: The creation risk factor verifies if a token is created with sensitive personal data and its number of attributes is sufficient to protect the security and privacy of an end-user. A token created with limited or less sensitive attribute may enhance privacy because personal attributes are minimized (Maler and Reed, 2008). Similarly, archiving a sensitive or excessive collection of personal attributes may lead to privacy risk.

Public/inferable/revocable: A token's secret is public if it can be found in an unauthorized or public database. Revealing a token secret to an unauthorized entity creates risk in the IDMS. A token's secret is inferable if it can be guessed or deduced. We can determine if a token's secret is inferable by computing its entropy (NIST, 2006; Ratha et al., 2001). The entropy of a token is given by $H_t = -\sum_{i=1}^{N} p_i \log(p_i)$ where $p(i)$ are the probabilities of individual characters in the token's secret string and N is the characters space. The entropy of a password secret is given by $H = n \log_2 b$ where b is the character space and n is the password length (NIST, 2006). For example, the character space for an English keyboard is 94. The entropy of a biometric template can be found in the work by Ratha et al. (2001).

When a token's secret is the user of the token could be identified or confidential information may be made available to unauthorized persons. A token's security can be revoked by either external or internal entity.

Copyable/concurrently usable: If the content of a token is not protected from adversaries then it can be copied. For example, the content of a low cost RFID tag with no additional security could easily be read by anyone with an appropriate reader but a high cost RFID tag that comes with additional security may ensure that only authorized readers have access to its content. A token is "copyable" if its content can be read by an unauthorized agent. This risk can occur externally or internally.

Concurrent use of a token may contribute to privacy and security risks if the token is stolen or disclosed without the knowledge of the token owner. On the other hand, concurrent use of token can enhance availability since the token can be used concurrently in many parallel sessions.

Loss, disclosure/disruption: The value at risk or how much is at stake when a token is lost, disclosed or disrupted is determined by these factors. Sharing a token in an IDMS can lead to a conflict situation where a token can be lost. In order to mitigate loss of tokens, the IDMS must be free of conflict. Token loss can also occur externally.

A token can be disclosed inside or outside an IDMS. For example, if a token is not encrypted in an IDMS its content can be disclosed. The cost of disclosure may depend on the application using the IDMS. A token can be disrupted in an IDMS if there is a deadlock in the system. This risk can occur externally if the token fails to function.

To enhance security, an IDMS should have a mechanism for checking the authority who issues a token if the token is a credential. The credential should contain the necessary data to facilitate the authentication. If the token is a mere assertion then the IDMS should provide a different mechanism to ensure the authenticity of the assertion. In order to enhance token security, there should be a means of ensuring the validity, identity and authenticity of the token (Mac Gregor et al., 2006).

Token's origin: Refers to the origin of a token. The authority who issued the token should be clearly identified.

Token's authenticity: Determines if a token belongs to the entity presenting it to the IDMS. Authenticity of a token must be checked in order to mitigate privacy and security risks.

Token's identity: Determines if a token identifies the subject or the entity possessing the token. The IDMS should have a mechanism for identification.

Token's validity: Determines if a token has not expired, its lifespan is within the validity period or has passed the validity test.

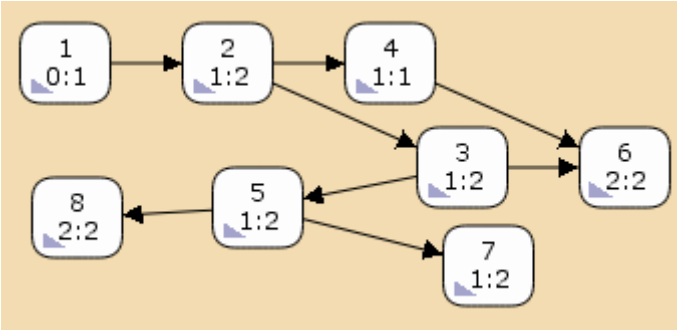

Figure 15. State Space Graph

The risk verification is based on state space analysis. Consequently, we begin the verification by generating the state space with CPNSTools (Jensen and Kristensen, 2009) from the system model in Section 3.2. The generated state space for the OpenID system model

is depicted in Figure 15. We analyze the risk in the system by running queries on the state space of the system in order to verify whether the identified risk contributing factors exist in the targeted IDMS. The queries and ML predicate functions search through every execution state of the IDMS model to verify if a risk condition exist. For example, the following CPNs query can be used to verify whether a token is used for multiple services or single sign-on (SSO).

```
fun multipleUse()=fn n=>size(Mark.RelyingParty'Resource 1 n)>1;
```

The place "RelyingParty'Resource" in Figure 12 stores all the tokens or assertions received by the "RelyingParty". To verify multiple use of token, we use the query "PredAllNodes(multipleUse())" to find the upper integer bound of all the nodes where tokens on the "RelyingParty'Resource" place is greater than 1. The result shows that multiple use of tokens occurred at node 52. This means the end-user can be profiled by the relying party, hence we have profiling or linkability risk. The ML function multipleUse() is defined above.

Each of the risk factors identified above is verified with ML queries and functions and the result is shown in Table 3.

Factors	**Risk Value**	Meaning
multiple times	Yes	Tokens can be linked or profiled by a SP
single sign-on/ multiple services	Yes	Tokens may be linked or profiled by ClaimedID Token is not profiled outside the trusted domain
creation	- No	Not considered or modeled Token has no sensitive attributes
archiving	Yes	Token can be archived by Relying parties/SPs
public	No	Token secret is kept private between end-users and IdP
inferable	Yes	Tokens' secret can be guessed by Relying Party/SPs
copyable	No	Tokens cannot be copied
concurrently usable	Yes	Token can be used concurrently
loss	No	Tokens cannot be lost in the IDMS
disclosure	No	Tokens cannot be disclosed in the IDMS
disruption	No	Tokens are not disrupted by conflict or deadlock in the IDMS
origination	-	Not considered or modeled
authentication	No	Tokens' authenticity test did not fail
identification	No	Tokens include the identity of the end-user
validation	-	Not considered or modeled

Table 3. Risk Analysis Report

Table 3 shows the summary report of the risk identified in a high level OpenID IDMS after verifying the internal risk factors or misuse cases. We are unable to verify some of the risk factors because of the high level specifications used in the analysis. All the risk factors can be verified if we use a low level system specifications.

We use the EMC risk model to determine the appropriate countermeasure for the identified risks. For example, if a token is used multiple times then an one-time token is an appropriate security countermeasure or control.

4 The Conflicting Incentives Risk Analysis Method

The Conflicting Incentives Risk Analysis (CIRA) method (Rajbhandari and Snekkenes, 2012a) is one of the risk analysis methods developed in the PetWeb II project. CIRA models risks in terms of conflicting incentives where risk analyst subjective probabilities are traded for stakeholder perceived incentives.

CIRA provides an approach in which the input parameters can be audited more easily. In CIRA, the risk owner is the stakeholder whose perspective is taken when doing the analysis. It focuses on risks at the managerial level rather than the technical level. It shows how ideas from game theory, economics, psychology, and decision theory can be combined to yield a risk analysis process.

Traditionally, risk assessment requires estimation of likelihood of a threat manifestation and the impact of it. In cases where there is little data to validate the likelihood of a threat manifestation, risk assessors rely on their experience and subjective intuitions to estimate the likelihood. This way of analyzing risk is not adequate to reduce the risk of a system or an organization to an acceptable level (Campbell, 1998; Gerber and von Solms, 2001). Therefore, CIRA trades risk assessors' subjective probabilities for stakeholders' perceived incentives. It believes that risk analysis can be improved if a stakeholder's incentive is replaced by the probabilities of a risk assessor.

4.1 Summary of the CIRA Method

The Conflicting Incentives Risk Analysis (CIRA) (Rajbhandari and Snekkenes, 2012b, 2013) method identifies stakeholders, actions and perceived expected consequences that characterize the risk situation. In CIRA, a stakeholder is an individual that has some interest in the outcome of actions that are taking place within the scope of significance. There are two classes of stakeholders: the strategy owner and the risk owner. Strategy owner is the stakeholder who is capable of triggering an action to increase his perceived benefit. Typically, each stakeholder has associated a collection of actions that he owns. The risk owner is the stakeholder whose perspective we consider when performing the risk analysis, i.e., he is the stakeholder at risk.

CIRA focuses on the human-related risks. This corresponds to understanding the incentives of the stakeholders that influence their actions. An incentive is something that motivates a stakeholder to take an action to increase his expected/ predicted utility. By utility, we mean the benefit as perceived by the corresponding stakeholder. Utility comprises of utility factors. Chulef et al. (2001) identify the utility factors relevant for our work. Each factor captures a specific aspect of utility, e.g., prospect of wealth, reputation, ego. Thus, utility can be approximated as the sum of weighted values for utility factors using Multi Criteria Decision Analysis.

After context establishment, the steps as listed in Table 4 are used for data collection (1-9) and analysis (10-13). The steps are briefly explained below. The details on the application of the method is provided by Rajbhandari and Snekkenes (2013).

Table 4. Procedure in CIRA

	Steps
1.	Identify the risk owner
2.	Identify the risk owners' key utility factors
3.	Given an intuition of the scope/ system- identify the kind of strategies/ operations which can potentially influence the above utility factors
4.	Identify roles/ functions that may have the opportunities and capabilities to perform these operations
5.	Identify the named strategy owner(s) that can take on this role
6.	Identify the utility factors of interest to this strategy owner(s)
7.	Determine how the utility factors can be operationalized
8.	Determine how the utility factors are weighted by each of the stakeholders
9.	Determine how the various operations result in changes to the utility factors for each of the stakeholders
10.	Estimate the utility for each stakeholder
11.	Compute the incentives
12.	Determine risk
13.	Evaluate risk

1. Identify the risk owner.
First, we determine the risk owner.

2. Identify the risk owners' key utility factors.
This step consists of determining the key utility factors for the risk owner. We can provide a list of utility factors for the risk owner to choose from.

3. Given an intuition of the scope/ system – identify the kind/ classes of operations/ strategies which can potentially influence the above utility factors.
In this step, we identify the strategies that can influence the utility factors of the risk owner. E.g., to determine the strategies, we can look into activities that cause security and privacy problems.

4. Identify the roles/ functions that may have the opportunities and capabilities to perform these operations.
This step consists of identifying the roles (e.g., CEO, system admin, hacker) capable of executing the above determined strategies.

5. Identify the named strategy owner(s) that can take on this role.
In this step, we pinpoint the strategy owner(s) that are in the position of executing the above strategies.

6. Identify the utility factors of interest to this strategy owner(s).
This step consists of determining the key utility factors for the strategy owners. Like before, we can provide a list of utility factors for the strategy owners to choose from.

7. Determine how the utility factors can be operationalized.
For each identified utility factor, we determine the scale, measurement procedure, semantics of values and explain the underlying assumptions, if any. Note that different flavors of the metrics may exist for an utility factor. Depending on the context, the metrics should be chosen.

8. Determine how the utility factors are weighted by each of the stakeholders.
We ask the stakeholders to rank the utility factors based on its importance. Then, for collecting the weights for the utility factors the following question is asked- "Given that you have assigned a weight of 100 to utility factor #1, how much would you assign to utility factor #2, #3 and so on (on a scale of 0-99)?".

9. Determine how the various operations result in changes to the utility factors for each of the stakeholders (start with risk owner).
For each of the identified utility factors, we determine the initial and final values after the strategies of the players are executed (for the utility factors' valuation, we utilize the metrics).

We use the additive utility function of Multi-attribute Utility Theory (MAUT) to estimate the utility. The additive utility function for a given player is defined to be the weighted average of its individual utility functions (Clemen, 1996) given as:

$$U = \sum_{k=1}^{m} w_k \cdot u(a_k) \tag{1}$$

where, m is the number of utility factors of the player, w_k is the assigned weight of utility factor a_k and $\sum_{k=1}^{m} w_k = 1$, and $u(a_k)$ is the utility function for the utility factor a_k.

10. Estimate the utility.
We use the techniques from MAUT to estimate the utility for each of the strategies for each player using Equation 1. We make the simplifying assumption that utility is linear.

11. Compute the incentives.
We need to compute the incentives, i.e., changes in utilities, for each of the strategies for each player. The change in utility Δ is the difference between the utility of the player in the state resulting from strategy use and the initial state.

12. Determine risk.
This can be achieved by investigating each of the strategies with respect to sign and magnitude of the changes determined in the previous step.

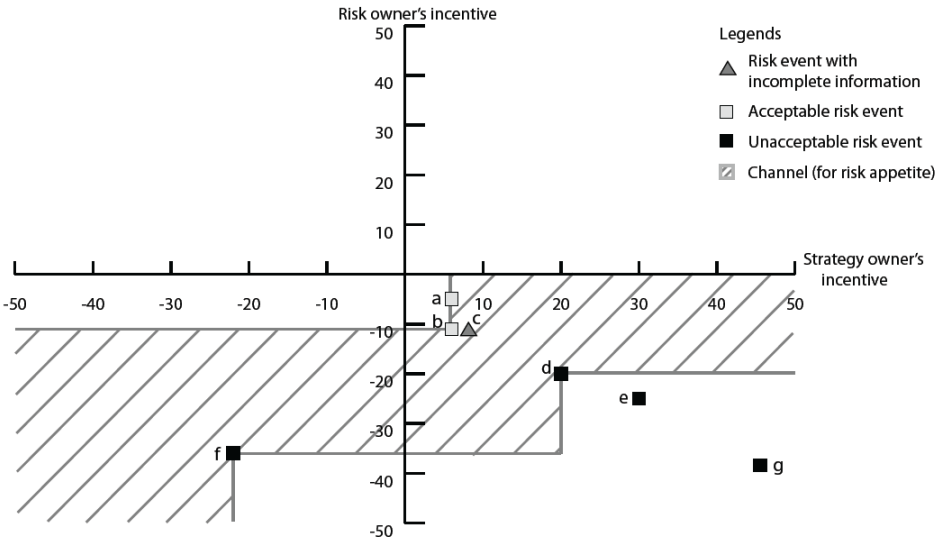

Fig. 1. The Incentive graph

Figure 16

For example, if in a scenario, a Strategy Owner X uses a Strategy1 and it results in a negative change of -36 in utility for a risk owner (Alice) and a gain of 48 for himself. Then in this case, 48 is the strength of the force that motivates X (Strategy Owner) to send Alice to an undesirable state and -36 is the magnitude of this undesirability and the combination of these is the risk (-36, 48). Figure refcirag depicts the stakeholders' risk for the example scenario.

13. Evaluate risk.

In this step, we identity the risk acceptance and rejection criteria for the risk owner to determine whether a specified level of risk is acceptable or not. In our model, we make the simplifying assumption that all strategy owners will need the same time to act if they have the same magnitude of incentive. Strategies will be executed in decreasing order of utility as perceived by each of the strategy owners.

5 Comparison of Risk Analysis Methods and Tools

This section compares the methods developed in the Petweb II project to the two classic risk analysis methods (Mehari and AICPA/CICA) tested in this report using SANDIA classification scheme (Campbell and Stamp, 2004).

The SANDIA classification scheme consists of approaches, levels, and method types. The approaches can be temporal, functional, or comparative. A temporal approach focuses on technical security. It depends on an understanding of a system being investigated and may require formal system modeling. It estimates risk based on the actual system tests and analysis.

A functional approach is between the temporal approach and the comparative approach. It has less focus on technical security than the temporal approach but requires more system-specific understanding than the comparative approach. The functional approach focuses on understanding threats to a system and how to mitigate these threats. It employs threat models rather than formal system models to analyze risk.

The comparative approach focuses on management or non-technical security. It represents an explicit risk analysis standard. The standard or procedure is then compared with that of a system owner.

The two categories of levels of the SANDIA classification scheme determine the capabilities or skills required to execute a risk analysis method and the extent to which a risk assessor need to understand the system under investigation.

The method types add additional characteristics to the approaches. The following sections show how the classification scheme is applied to compare the four methods discussed in this report.

5.1 Applicable Approaches

This section compares the approaches used by the methods discussed above under the SANDIA classification scheme. Figure 17 depicts the classification of the approaches used by the four methods discussed in this report.

Approach		
Temporal	**Functional**	**Comparative**
EM-BRAM	**CIRA**	**Mehari, AICPA/CICA**

Figure 17. Applicable Approaches of the SANDIA Scheme

The EM-BRAM (Paintsil and Fritsch, 2013) falls under the temporal approach where the performance of an IDMS as a consequence of the application of certain tests is the result of the method. EM-BRAM focuses on technical security and depends on the understanding of the technical system. EM-BRAM is likely to produce technically accurate results because a technical system model is analyzed for privacy and security risks. The security controls for the protection of IDMSs are determined after thorough analysis of the a technical system model. Thus, security controls are not chosen based on subjective intuitions of a risk assessor.

The CIRA (Rajbhandari and Snekkenes, 2012a) falls under the functional approach where the understanding of the technical system or model is less important. Functional approaches rely on risk models rather than a technical system model or specification to determine the necessary security controls for a system or an organization. They estimate risk based on guess work or subjective intuitions of risk assessors or system stakeholders. Administrative, policies and management procedures are the main the focus of the analysis. Functional approaches may employ statistical modeling to reduce the subjec-

tivity in the risk estimation. The outcome of functional risk analysis approaches are very useful for management and financial decision making in organizations but less useful for technical security (Campbell, 1998).

The Mehari (Jouas et al., 2012) and AICPA/CICA (AICPA/CICA, 2010) methods fall under the comparative approach. Comparative approaches or methods implement an explicit risk analysis standard such as ISO 27005 (ISO, 2008b), best practices such as OECD or audit scheme such as COBIT ISACA (2009). No explicit system model or risk model is required for the risk analysis. A risk assessor compares the owner's system and/or procedures with the standard (Campbell and Stamp, 2004). The risk assessors estimate risk based on their subjective intuition and employ no formal approach to reduce the subjectivity in the risk estimation. This means the result obtained with these methods may be highly unreliable for administrative and management decisions. Comparative approaches are less useful for technical security.

5.2 Levels of Expertise

This section compares the expertise needed to use the methods discussed above for risk analysis under the SANDIA classification scheme.

Level		
Abstract (expert)	**Mid-level (collaborative)**	**Concrete (owner)**
EM-BRAM	**CIRA, Mehari, AICPA/CICA**	

Figure 18. Levels of Expertise Need for Risk Method

Figure 18 depicts the classification of the levels of expertise required for various risk analysis methods. Generally, the successful application of any security or risk method depends on the capability to execute a method and the knowledge of the system. The EM-BRAM (Paintsil and Fritsch, 2013) requires thorough understanding of IDMSs and an expert to execute the method therefore it falls under the abstract or expert levels. This means the EM-BRAM could be expensive because of the need for experts and thorough knowledge of IDMSs. However, EM-BRAM reduces costs by employing graphical and easy to learn CPNs tools for system modeling and analysis. In addition, the input for the analysis is predetermined, therefore a risk assessor does not need to spend much time on the risk modeling. System models can be re-used with slight modification. The graphical tools used in the EM-BRAM can enhance communication among system stakeholders.

The others methods are mid-level or collaborative. This means that system stakeholders and experts need to work together to execute this method. In a large system or organization, obtaining the initial input could be time consuming and expensive. The cost of implementation is even higher in a system that involves multiple organization such IDMSs. Thus, the CIRA, Mehari and AICPA/CICA methods require extensive preparation while the EM-BRAM may require little preparation. In addition, effective risk communication is required to get the best out of the method because experts and non-experts speak dif-

ferent languages. However, none of the methods in this category has communication enhancing tool support.

5.3 Method Types

This section compares the method types used by the methods above.

Classes								
Engagement	Exercise	Compliance Testing	Sequence	Assistant	Matrix	Principles	Best Practices	Audit
EM-BRAM				CIRA		Mehari, AICPA/CICA		Mehari

Figure 19. Method Types of the SANDIA Scheme

Figure 19 depicts the method types of the SANDIA classification scheme. The method types of engagement, exercise, and compliance testing fall under the temporal approach. Engagement means that the risk analysis expert set the boundary for the analysis and makes most of the decisions. In addition, the expert takes full control of the system under investigation. The exercise means the system owner set the boundary of the risk analysis. The expert and the system owner work together or collaborate in order to analyze the system. Compliance testing requires no risk expert. The system owner develops and tests the system under investigation.

The method types of sequence, assistant, and matrix fall under the functional approach. The method type of sequence consists of a series of steps, usually posed as questions, and sometimes in a form as complex as a flowchart. The assistant method type consists of a list of threats, assets and vulnerabilities. The system owner works through the process prompting him to populate the list with appropriate values. The matrix method type depend on table lookup to estimate risk.

The method types of principles, best practices, and audit fall under the Comparative approach. The Principles method types are high level risk analysis principles such as the OECD recommendation. The best practice method types are more specific list of risk analysis practices. Audit method types are more specific than the best practice.

Following this scheme, we classify the EM-BRAM under the engagement method type, CIRA falls under assistant method type, while Mehari and AICPA/CICA are principles. In addition, Mehari also can be defined as auditing.

All the methods in this report focus on security, except EM-BRAM. The adequacy and suitability of a risk analysis method depends on the objectives and purposes of the analysis (Lund et al., 2011). In addition, privacy requirements complement that of security but conflicts can arise in their implementation (Zwingelberg and Hansen, 2012). Therefore, a security-oriented risk analysis method is not necessarily suitable and adequate for privacy risk analysis.

5.4 Summary Comparison of the Risk Analysis Methods and Tools

Method	Purpose	Input	Effort	Outcome	Scalability
EM-BRAM	Technical risk analysis and decisions	System specification and risk model	Technical expertise but less time consuming	List of vulnerabilities	Yes
CIRA	Non-technical risk analysis and decisions	stakeholders, strategies, utility factors, weights, initial values	Expertise and time consuming	Strength of stakeholders incentive or changes in utility	No
Mehari	Management risk analysis and decisions	Policies, procedures, assets and processes	Expertise and more time consuming	Intrinsic impact, intrinsic seriousness (risk), and calculated seriousness	No
ACIPA, CICA	Non-technical or legal risk analysis and decisions	Predefined questions	Expertise and less time consuming	Average risk scores	No

Table 5. Comparison of the Risk Analysis Methods and Tools

The EM-BRAM method focuses on technical privacy and security risks analysis. It requires system specifications and a risk model as inputs. It also requires experts to perform the analysis however the amount of time require for the analysis may be less than other methods because of the kind of input required. The risk model is predefined and therefore the only effort is how to convert a system specification to CPNs model. Moreover, the CPNs modeling is made relative easy by means of graphical CPNs tools. The system modeling can be reused with slight modifications. The output of the method consists of technical privacy and security risks in an IDMS and appropriate controls to mitigate the risks.

The CIRA method focuses on non-technical security risk analysis. The input of the method comes from procedures, policies, processes and stakeholders' incentives. Understanding such non-technical procedures in an organization could be more time consuming and will require more effort than obtaining a technical specification. In addition, none of the inputs for CIRA method is predetermined. CIRA method requires an expert to lead the risk analysis and therefore could be expensive. The risk analysis results cannot be reused because requirements are specific to each organization. The output of the method is non-technical security risks and control decision. Privacy risk analysis in this is highly restricted.

The Mehari method focuses on non-technical security risk analysis. The input of the method comes from procedures, policies and processes. Understanding such non-technical procedures in an organization can be rather time consuming and will require more ef-

fort than obtaining a technical specification. In addition, none of the inputs for Mehari method is predetermined. The inputs depend on the requirements of a targeted organization. This means risk analysis results are not reusable. Mehari method requires an expert to lead the risk analysis and therefore could be expensive. The output of the method is non-technical security risks and control decisions. Privacy risk analysis in this is highly restricted.

The AICPA/CICA method focuses on non-technical security risk analysis. The input of the method are predefined questions hence less effort and time are required to apply the method. AICPA/CICA requires an expert to lead the risk analysis and therefore could be expensive. The output of the method is non-technical privacy risks and control decisions. Security risk analysis in this is highly restricted.

EM-BRAM is good for technical privacy and security risks analysis while the other methods are good for non-technical privacy or security risk analysis. Both EM-BRAM and AICPA/CICA may require less effort and time. Finally, EM-BRAM is more scalable than other methods, since they can analyze risk in one organization at a time.

5.5 Method Selection

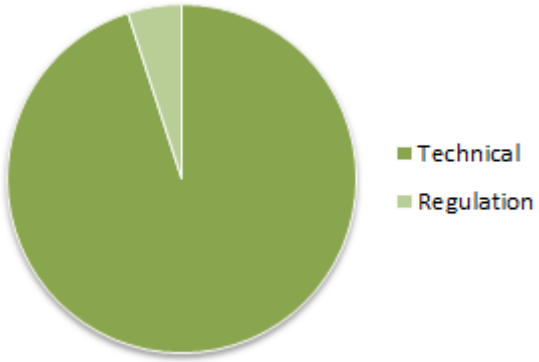

Figure 20. Executable Model-Based Risk Analysis Method

Figure 20 depicts the focus of the executable model-based risk analysis method (EM-BRAM) developed under the PetWeb II project. EM-BRAM focuses on technical risk analysis in order to determine technical security and privacy controls for IDMSs. EM-BRAM is recommended for technical risk analysis in IDMSs.

Figure 21 depicts the focus of the conflicting incentive risk analysis (CIRA) method developed under the PetWeb II project. CIRA requires identification of utility factors for the risk analysis. The identification of these utility factors are informed by business and regulatory needs of system stakeholders. Consequently, CIRA is adequate for improving business and regulatory compliance for stakeholders.

Figure 22 depicts the focus of the AICPA/CICA risk analysis method. The main objective of the method is to ensure that an organization is privacy compliant. Consequently, it is suitable for ensuring privacy compliance in organizations.

Figure 23 depicts the focus of the Mehari risk analysis method. Mehari has three main

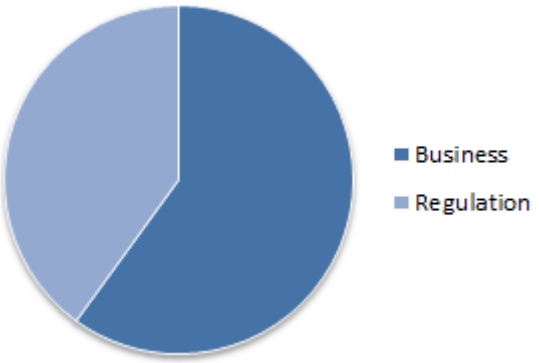

Figure 21. Conflicting Incentives Method

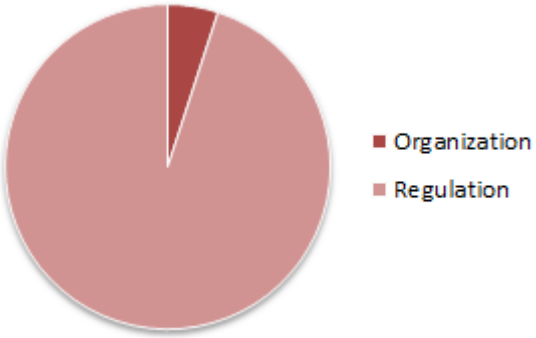

Figure 22. AICPA/CICA Method

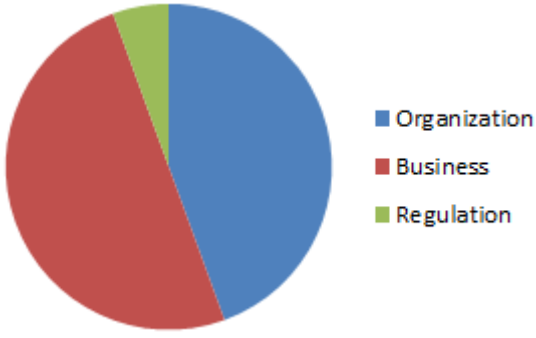

Figure 23. Mehari Method

area of concern – organization, business processes and regulation. It pays little attention to regulation but focuses more on analyzing the overall security risk in organizations as well as business processes.

6 Conclusion

Risk analysis determines the necessary technical and non-technical controls for information security in an organization. Effective information security need to combine both technical and non-technical controls. This report analyzes two classic and two newly developed risk analysis methods and shows how they analyze security and privacy risks in identity management systems (IDMSs).

The executable model-based risk analysis method (EM-BRAM) is one of the methods developed under the PetWeb II project. It is the only method that focuses on technical security. The other methods analyzed in this report are non-technical. They focus on administrative process and management procedures. The conflicting incentives risk analysis (CIRA) method developed in the Petweb II project introduces a technique that can improve the risk estimation in the non-technical or classic risk analysis methods. In spite of the proposed improvement, scalability still remain a challenge in the CIRA method. In addition, how to combine risk analysis results from multiple organization is yet to be addressed in the non-technical methods. Identity management usually involves multiple organizations therefore methods that isolate organizations are inadequate. The EM-BRAM is scalable because many security domains can be analyzed in a single model.

None of the methods analyzed in this report combines both technical and non-technical risk analysis. Organizations who wish to undertake comprehensive risk analysis ought to identified their needs and as much as possible combine both technical and non-technical methods. No organization can be secure by using only one out of these two main methods.

References

AICPA/CICA (2010). *The AICPA/CICA Privacy Risk Assessment Tool*. American Institute of Certified Public Accountants / Canadian Institute of Chartered Accountants. Available from: http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/gen-accepted-privacy-principles/item10730.pdf. 7, 13, 14, 32

Alexander, I. F. (2002). Initial industrial experience of misuse cases in trade-off analysis. In *Proceedings of the 10th Anniversary IEEE Joint International Conference on Requirements Engineering*, RE '02, pages 61–70, Washington, DC, USA. IEEE Computer Society. 16

Almeida, J. B., Frade, M. J., Pinto, J. S., et al. (2011). *Rigorous software development : an introduction to program verification*. Undergraduate topics in computer science. Springer, London. Available from: http://opac.inria.fr/record=b1132575. 21

Bauer, M., Meints, M., and Hansen, M. (2005). D3.1: Structured overview on prototypes and concepts of identity management systems. Deliverable 1.1, Future of Identity in the Information Society. 24

Campbell, H. (1998). Risk assessment: subjective or objective? *ENGINEERING SCIENCE AND EDUCATION JOURNAL*. 23, 27, 32

Campbell, P. L. and Stamp, J. E. (2004). A classification scheme for risk assessment methods. Technical Report SAND2004-4233, SANDIA National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550. 30, 32

Chulef, A. S., Read, S. J., et al. (2001). A Hierarchical Taxonomy of Human Goals. *Motivation and Emotion*, 25(3):191–232. 27

Clemen, R. T. (1996). *Making Hard Decision: An Introduction to Decision Analysis*. Duxbury, 2nd edition. 29

Elahi, G. and Yu, E. S. K. (2009). Modeling and analysis of security trade-offs – a goal oriented approach. *Data Knowl. Eng.*, pages 579–598. 16

Gerber, M. and von Solms, R. (2001). From risk analysis to security requirements. *Computers and Security*, 20(7):577 – 584. 15, 23, 27

ISACA (2009). *The Risk IT Practitioner Guide*. ISACA, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA. isbn: 978-1-60420-116-1. 19, 32

ISO (2008a). ISO 27000 information security risk management. Technical report, International Organization for Standardization. 15

ISO (2008b). ISO 27005 information security risk management. Technical report, International Organization for Standardization. 7, 32

Jensen, K. and Kristensen, L. M. (2009). *Colored Petri Nets: Modelling and Validation of Concurrent Systems: Modeling and Validation of Concurrent Systems*. Springer-Verlag Berlin Heidelberg. ISBN:978-3-642-00283-0. 17, 20, 21, 22, 25

Jøsang, A. and Pope, S. (2005). User centric identity management. *AusCERT Conference*. 6

Jouas, J.-P., Buc, D., Corbier, O., Gagne, M., Pineault, C., Roule, J.-L., Taillon, C., Touboul, M., and Traversviaud, A. (2012). MEHARI 2010 – guide de développement d'une base de connaissances d'analyse de risque mehari. Technical report, Club de la securite de l'information français. Available from: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2011-Guide-developpement-base.pdf. 7, 10, 11, 12, 13, 32

Lund, M. S., Solhaug, B., and Stølen, K. (2011). *Model-Driven Risk Analysis, The CORAS Approach*. Springer, 1 edition. 6, 15, 33

Mac Gregor, W., Dutcher, W., and Khan, J. (2006). An Ontology of Identity Credentials - Part 1: Background and Formulation. Technical report, National Institute of Standard and Technology, Gaitersburg, MD, USA. Available from: http://www.jon.grimsgaard.no/rudrevyen/index.html. 25

Maler, E. and Reed, D. (2008). The venn of identity: Options and issues in federated identity management. *IEEE Security and Privacy*, 6:16–23. 24

Matulevicius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., and Genon, N. (2008). Adapting secure tropos for security risk management in the early phases of information systems development. In *CAiSE*, pages 541–555. 6

McDermott, J. P. (2000). Attack net penetration testing. In *Proceedings of the 2000 workshop on New security paradigms*, NSPW '00, pages 15–21, New York, NY, USA. ACM. 20

McKenzie, R., Crompton, M., and Wallis, C. (2008). Use cases for identity management in e-government. *IEEE Security and Privacy*, 6(2):51–57. 15

Mitrano, T., Kirby, D. R., and Maltz, L. (2005). What does privacy have to do with it?: privacy risk assessment. *EDUCAUSE*. 18

Naumann, I. and Hogben, G. (2009). Privacy features of european eid card specifications. Technical Report 1.0.1, ENISA. 16

NIST (2006). Electronic authentication guideline. Technical Report 1.0.2, NIST Special Publication 800-63. 24

Okubo, T., Taguchi, K., and Yoshioka, N. (2009). Misuse cases + assets + security goals. In *Computational Science and Engineering, 2009. CSE '09. International Conference on*, volume 3, pages 424 –429. 16, 18

Paintsil, E. (2011). Towards legal privacy risk assessment and specification. In *Proceedings of the 8th international conference on Trust, privacy and security in digital business*, TrustBus'11, pages 174–185, Berlin, Heidelberg. Springer-Verlag. 18

Paintsil, E. (2012a). Evaluation of privacy and security risks analysis construct for identity management systems. *Systems Journal, IEEE*, PP(99):1. 17, 23

Paintsil, E. (2012b). A model for privacy and security risks analysis. *IEEExplore*. 16, 17, 18

Paintsil, E. and Fritsch, L. (2011). A taxonomy of privacy and security risks contributing factors. In Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., and Zhang, G., editors, *Privacy and Identity Management for Life*, volume 352 of *IFIP Advances in Information and Communication Technology*, pages 52–63. Springer Boston. 16

Paintsil, E. and Fritsch, L. (2013). Executable model-based risk assessment method for identity management systems:using hierarchical colored petri nets. Accepted for publicaton. 6, 31, 32

Peterson, G. (2006). Introduction to Identity Management Risk Metrics. *IEEE Security & Privacy*, 4(4):88–91. 19

Rajbhandari, L. and Snekkenes, E. (2012a). Intended actions: Risk is conflicting incentives. In Gollmann, D. and Freiling, F., editors, *Information Security*, volume 7483 of *Lecture Notes in Computer Science*, pages 370–386. Springer Berlin Heidelberg. 6, 27, 31

Rajbhandari, L. and Snekkenes, E. (2012b). Intended Actions: Risk Is Conflicting Incentives. In Gollmann, D. and Freiling, F., editors, *Information Security*, volume 7483 of *Lecture Notes in Computer Science*, pages 370–386. Springer Berlin / Heidelberg. 27

Rajbhandari, L. and Snekkenes, E. (2013). Using the Conflicting Incentives Risk Analysis Method. In *SEC 2013*. (accepted for publication). 27

Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634. 24

Recordon, D. and Reed, D. (2006). Openid 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, DIM '06, pages 11–16, New York, NY, USA. ACM. 22

Rost, M. and Bock, K. (2011). Privacy by design and the new protection goals*. *DuD*. 17

Sindre, G. and Opdahl, A. L. (2004). Eliciting security requirements with misuse cases. *Requirements Engineering*, 10(1):34–44. 16, 18

Smojver, S. (2011). Selection of information security risk management method using analytic hierarchy process (ahp). *Central European Conference on Information and Intelligent Systems, CECIIS – 2011*. 6

Taubenberger, S., Jürjens, J., Yu, Y., and Nuseibeh, B. (2011). Problem analysis of traditional it-security risk assessment methods – an experience report from the insurance and auditing domain. In *SEC*, pages 259–270. 6

Wang, R. and Dagli, C. H. (2011). Executable system architecting using systems modeling language in conjunction with colored petri nets in a model-driven systems development process. *Syst. Eng.*, 14(4):383–409. 21

Xu, J. and Kuusela, J. (1998). Analyzing the execution architecture of mobile phone software with colored petri nets. *International Journal on Software Tools for Technology Transfer (STTT)*, 2:133–143. 10.1007/s100090050022. 21

Zwingelberg, H. and Hansen, M. (2012). Privacy protection goals and their implications for eid systems. In Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., and Russello, G., editors, *Privacy and Identity Management for Life*, volume 375 of *IFIP Advances in Information and Communication Technology*, pages 245–260. Springer Berlin Heidelberg. 17, 33