Economics of Identity and Access Management: a Case Study on Enterprise Business Services

Marco Casassa Mont, Yolanta Beres, David Pym, Simon Shiu

HP Laboratories
HPL-2010-12

Keyword(s):
economics, decision support, IAM, modeling, simulation, security, case study

Abstract:

Identity and Access Management (IAM) is a key enabler of enterprise businesses: it supports automation, security enforcement and compliance. However, most enterprises struggle with their Identity and Access Management strategy. Discussions on IAM primarily focus at the IT operational level, rather than targeting strategic decision makers' issues, at the business level. Organisations are experiencing an increasing number of internal and external threats and risks: there is scarcity of resources and budget to address them all. Decision makers (e.g. CIOs, CISOs) need to prioritise their choices and motivate their requests for investments. This applies for investments in IAM vs. other possible security or business investments that could be made by the organisation. In this context, a range of possible IAM investment options has an effect on multiple strategic outcomes of interest, such as assurance, agility, security, compliance, productivity and empowerment. We have developed a repeatable approach and methodology to help organizations work through this complex problem space and determine an appropriate strategy, by providing them with decision support capabilities. The proposed approach, validated in collaboration with security and IAM experts, couples economic modeling (which explores decision makers' preferences between the different outcomes) with system modeling & simulations to predict the consequences (likely outcomes) associated with different investment choices and map them against decision makers' preferences, in order to identify the most suitable investment options. We illustrate how this methodology has been applied in an IAM case study, in a business-driven context with core enterprise services. This work is in progress. We discuss current results and next steps. This paper provides a detailed description of the findings of the IAM case study. An executive summary is available in [35].

External Posting Date: February 6, 2010 [Fulltext] Approved for External Publication
Internal Posting Date: February 6, 2010 [Fulltext]

© Copyright 2010 Hewlett-Packard Development Company, L.P.

Economics of Identity and Access Management: a Case Study on Enterprise Business Services

Marco Casassa Mont, Yolanta Beres, David Pym, Simon Shiu
Hewlett-Packard Labs, Bristol, UK
marco.casassa-mont@hp.com, yolanta.beres@hp.com, david.pym@hp.com, simon.shiu@hp.com

Abstract

Identity and Access Management (IAM) is a key enabler of enterprise businesses: it supports automation, security enforcement and compliance. However, most enterprises struggle with their Identity and Access Management strategy. Discussions on IAM primarily focus at the IT operational level, rather than targeting strategic decision makers' issues, at the business level. Organisations are experiencing an increasing number of internal and external threats and risks: there is scarcity of resources and budget to address them all. Decision makers (e.g. CIOs, CISOs) need to prioritise their choices and motivate their requests for investments. This applies for investments in IAM vs. other possible security or business investments that could be made by the organisation. In this context, a range of possible IAM investment options has an effect on multiple strategic outcomes of interest, such as assurance, agility, security, compliance, productivity and empowerment. We have developed a repeatable approach and methodology to help organisations work through this complex problem space and determine an appropriate strategy, by providing them with decision support capabilities. The proposed approach, validated in collaboration with security and IAM experts, couples economic modeling (which explores decision makers' preferences between the different outcomes) with system modeling & simulations to predict the consequences (likely outcomes) associated with different investment choices and map them against decision makers' preferences, in order to identify the most suitable investment options. We illustrate how this methodology has been applied in an IAM case study, in a business-driven context with core enterprise services. This work is in progress. We discuss current results and next steps. This paper provides a detailed description of the findings of the IAM case study. An executive summary is available in [35].

1. Introduction

Identity and Access Management (IAM) solutions (providing provisioning, compliance and enforcement capabilities) are widely adopted by organizations to enable their businesses, support user management, access control and compliance as well as deal with related security risks.

However, most enterprises struggle with their Identity and Access Management strategy. It is not just an IT matter. Enterprises are experiencing an increasing number of internal and external threats: there is scarcity of resources and budget to address them all. Decision makers (e.g. CIOs, CISOs) are increasingly asked to prioritise and motivate their requests for investments. This applies for investments in IAM vs. other possible security or business investments that could be made.

The specific problem addressed by our work is how to enable these decision makers to make informed decisions about their IAM strategy and related investments. It is a matter of understanding and dealing with the *Economics of IAM*. IAM strategy directly affects organisations' business in terms of agility, productivity, user experience, security risks and compliance. It is challenging because it can be very difficult to determine how different combinations of technology and process will affect these business outcomes. Choices have to be made without knowing the future business needs and threat landscape. In general this is an example of a problem with multiple attributes, choices, outcomes and stakeholders with high degrees of uncertainty. However organizations see ongoing growth and changes in applications, resources, roles and users, which mean that security teams must regularly address this problem. Moreover, given the cost constraints, a more rigorous approach is needed both to make the case for appropriate investments and to show due diligence to regulators.

Recent work and research activities, e.g. [21,26,27,28,29,30], highlighted the limitations of techniques based on Return-of-Investment approaches, especially when adopted in security contexts, as the calculations do not adequately address the involved operational and dynamic aspects. Traditional consulting in this area is also often based either on generic risk assessment & common security practices (e.g. ISO2700x [22], CoBit [23], etc.) or driven by the agenda of selling portfolios of IAM products/solutions.

In this paper we describe our approach to this problem based on exploring decision makers' preferences on strategic aspects of relevance and using system modeling and simulation to identify and predict how different portfolios of IAM investments would suit these needs. As a significant example, we discuss how this approach has been used in an enterprise IAM case study, involving core business services provided by SAP applications. This approach has been validated by a few security & IAM experts. Our work still require refinements but the initial results are encouraging and provide a starting point for further research and investigations. Current results and next steps are presented and discussed.

The remaining part of this paper is structured as it follows: Section 2 provides an overview of the Economics of IAM. Section 3 introduces the Security Analytics methodology we used in our work, and specifically in the IAM case study - discussed in Section 4. Section 5, 6 and 7 provide the details of the various steps that have been carried out in the case study, respectively in terms of *Economic Elicitation of Strategic Preferences*, *Exploring the Impact of IAM Investment Options* (by means of *Modelling & Simulation)* and *Mapping Predicted Outcomes against Decision Makers' Preferences*. Section 8 discusses related work and our next steps. Finally, Section 9 draws our conclusions.

2. Economics of IAM

Decision makers operating in the IAM space (e.g. CIOs, CISOs) need to cope with different tension points at the business, security, governance levels and worry about the involved trade-offs. They need to make informed IT investment decisions in a complex, ever changing world. They would love to get decision support capabilities to easy their work.

To succeed in providing these capabilities, the *economics* that are at the base of strategic IT investment decisions need to be understood. We assume that there should be an economic framework within which the value of different investment outcomes can be explored and discussed. This involves identifying the major *business and strategic outcomes* of concern and determining the different stakeholders intuitive views for how these trade-off, and their preferences for overall outcomes. In this context *traditional IT metrics* are of relevance if they can help to ground the analysis, by factoring in measures from underlying IT systems and processes.

In the IAM space, our analysis of decision makers' concerns (leveraging interviews with CIOs/CISOs and security & IAM experts) has identified the following core strategic outcomes of relevance along with examples of related (IT) metrics: ***security risks*** (metrics: data breaches and incidents); ***productivity*** (metrics: correctly granted access rights); ***compliance to regulations*** (metrics: audit failures); ***costs*** (metrics: fixed and operational costs set by the financial controller).

Within an organization, different strategic decision makers usually have different priorities; a CISO might be specifically worried about security risks and involved IT costs; a business and application manager might be worried about user productivity; a governance manager might give top priority to compliance to regulation. These multiple objectives trade off with each other. For example, security risks can be addressed potentially at the expense of productivity. Compliance management can reduce the risk of audit failures but it might also negatively impact productivity. All of these aspects have budget implications.

It is important to identify the overall organization (or decision makers') preferences for achieving these objectives. Ideally the goal would be to encapsulate these preferences in a formal *"utility function"* of the company and/or the decision makers, so that a "comparative value" can be applied to each outcome. At a conceptual level, we might think of utility functions of the form:

$$\boldsymbol{U = \omega_1 f_1 (T1 - \overline{T1}\ ) + \omega_2 f_2 (T2 - \overline{T2}\ ) + \ldots + \omega_n f_n (Tn - \overline{Tn}\ )}$$

where $\boldsymbol{Ti}$ **(1 ≤ i ≤ n)** represent the outcomes of interest - for example, *security risks, productivity, compliance and costs*; $\boldsymbol{\overline{Ti}}$ **(1 ≤ i ≤ n)** represent the decision maker's targets for these outcomes. The functions $\boldsymbol{f_i}$ **(1 ≤ i ≤ n)** represent the decision maker's tolerance for variance from the targets. Finally, the weights $\boldsymbol{\omega_i}$ **(1 ≤ i ≤ n)** represent the decision maker's preferences between the component outcomes.

If the decision-maker is equally tolerant for going over or under target for a specific outcome, the $\boldsymbol{f_i}$ can potentially be represented as a quadratic function. This choice, which has a well-supported theoretical basis captures diminishing marginal utility. For example, if the outcome component is cost, overspending by £500 is just as bad as under spending by the same amount. If the decision maker's expresses asymmetry for exceeding the target for a component, then it is necessary to use functional forms such as Linex functions: $f(x)=(e^{\alpha x}-\alpha-1)/\alpha^2$. These functions capture this asymmetry appropriately. For example, the marginal utility of *compliance* and *productivity* might have a steeper gradient below target than above.

In the context of *IAM Economics*, one or more utility functions could be identified for the involved strategic decision makers and/or for the organization. Let us consider the example of a decision maker that (a) is concerned about *security risks, productivity, compliance and costs*, with different priorities, expressed with weights $\boldsymbol{\omega_i}$ and that (b) is equally tolerant for going over or under target for each outcome. A related utility function could be the following:

$$\boldsymbol{U = \omega_1 (SR - \overline{SR}\ )^2 + \omega_2 (P - \overline{P}\ )^2 + \omega_3 (CO - \overline{CO}\ )^2 + \omega_4 (C - \overline{C}\ )^2}$$

where the involved variables identify the decision maker's strategic aspects of relevance (**SR**: security risks, **P**: productivity, **CO**: compliance, **C**: costs) against the desired related stakeholders' targets.

In practice it is hard to identify and instantiate this utility function, purely from an abstract analytic approach, without taking into account the implications that potential IAM investments have on the organization i.e. the impact on operational and business processes, people behaviour, the underlying IT systems, existing and foreseeable security threats (e.g. internal and external threats perpetrated by employees, attackers).

We believe that it is possible to tackle this issue and provide strategic decision support to decision makers by (a) *explicitly eliciting their preference* on strategic outcomes of interest and (b) adopting *system modeling and simulation techniques* to explore and predict (estimate) the impact of investment choices for the organization and map these outcomes against the decision makers' preferences in order to identify suitable investment options. We believe this creates awareness of available strategic options and enables discussions at the business level. The next section introduces the adopted methodology.

3. Methodology for Strategic Decision Support

This methodology fundamentally integrates two main approaches: (1) executable mathematical models of the underlying systems and processes along with their dynamic threat environments; (2) methods from economics — specifically, utility functions and their associated dynamic analysis — together with empirical data-collection techniques.

Modeling and simulation have already been used in various fields (e.g. hydrology, land usage, manufacturing processes, environmental and social science) to provide decision support: surveys and data-gathering activities are also used to ground these models. However, their usage in security and IT, coupled with methods from economics is relatively new.

Recent work by the current authors and others, e.g. [10,11,25,27,28,30,31] has started to develop a methodology that integrates these two approaches and demonstrates its feasibility. Figure 1 provides an overview of the methodology whilst Figure 2 shows, in more details, the involved steps.

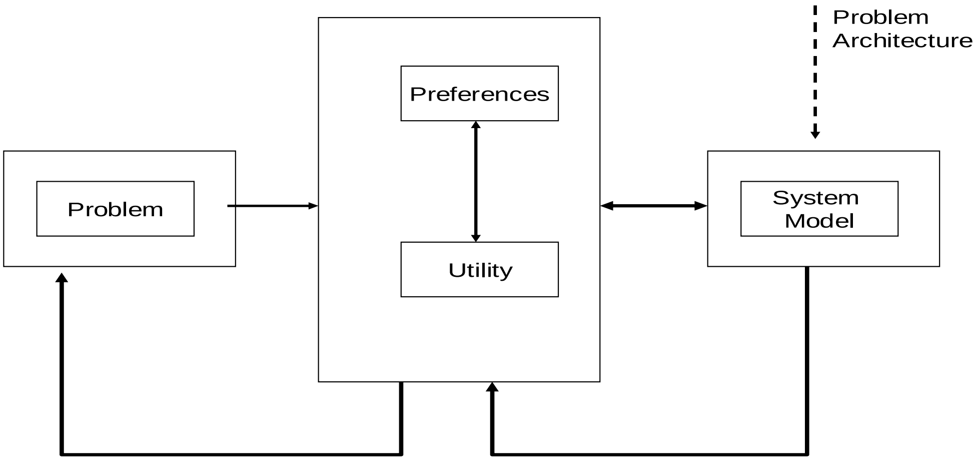


Fig. 1. Overview of the Methodology

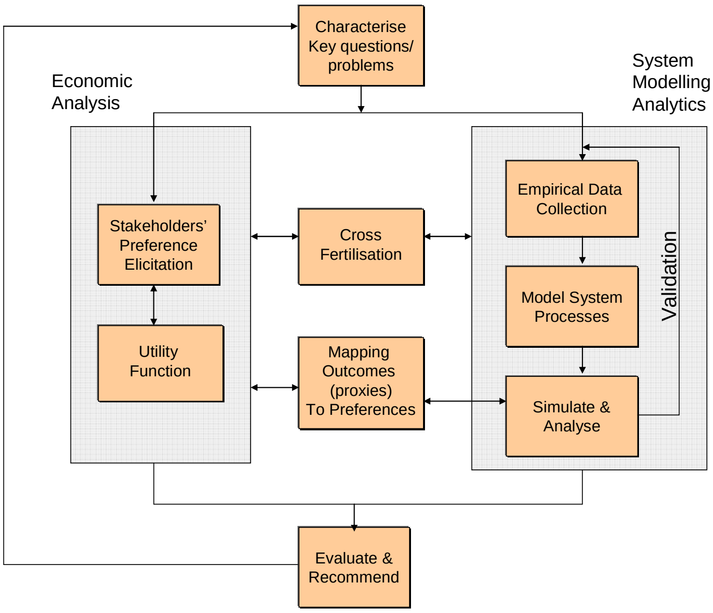


Fig. 2. Steps involved in the Methodology

After characterizing an investment problem, an economic model is built based on strategic preference elicitation; this drives a subsequent system modelling phase that helps to ground concepts in a specific organisational context; the resulting system model(s) provides predictions of the impact of various investment choices along with estimates of the utility functions' components. This finally helps to identify the most suitable approach and investment choice. Multiple iterations and cross-fertilisations activities (between the economic and system modeling areas) might be required to refine the model and provide effective support to decision makers.

In this context, strategic preferences are elicited from the decision maker by using targeted questionnaires, aiming at identifying priorities and potential suitable trade-offs. Executable mathematical models not only take into account these preferences and targets but also the constraints inherent in the problem e.g. architectural, policy, business & IT processes and user behaviors - in the context of organizational dynamic threat environments.

The behavior of the model can be simulated in the presence of a (stochastic) representation of the dynamic threat environments and across different investment choices. Its predictions can then be validated against the targets and preferences of the decision maker. These predictions can be thought as *proxies* (based on metrics and measures) to estimate utility function's components. The model may then be refined appropriately, as the decision maker's understanding of the appropriate targets and preferences in response to the initial problem may itself be subject to reassessment and refinement.

In the specific context of IAM, system modeling can be used to capture the effects and implications of making different IAM investment choices - in areas such as *user provisioning, compliance monitoring and security enforcement* - as well as their impact on the business and in mitigating security threats (e.g. internal & external attacks, ex-worker attacks, etc). This requires understanding the implications and explicit cause-effect relationships that exist between these IAM investment options and the processes and IT operational levels.

4. IAM Case Study

An IAM case study has been carried out in collaboration with three security & IAM Experts, to explore the feasibility of the outlined methodology to provide strategic decision support for IAM investments. The experts acted as strategic decision makers. This paper discusses *the outcomes we obtained from one expert*, whom played the role of a CIO/CISO, on behalf of a major customer.

This case study focuses on a large organization and considered the significant case where the decision maker has to make strategic IAM investment decisions to support core enterprise business services, underpinned by SAP Applications.

SAP applications [12] are widely used in the industry to provide: Customer Relationship Management (CRM), Supply Chain Management (SCM), Human Capital Management (HCM)/Human Resources (HR), Product Lifecycle Management (PLM) and Supplier Relationship Management (SRM) – see Figure 3.

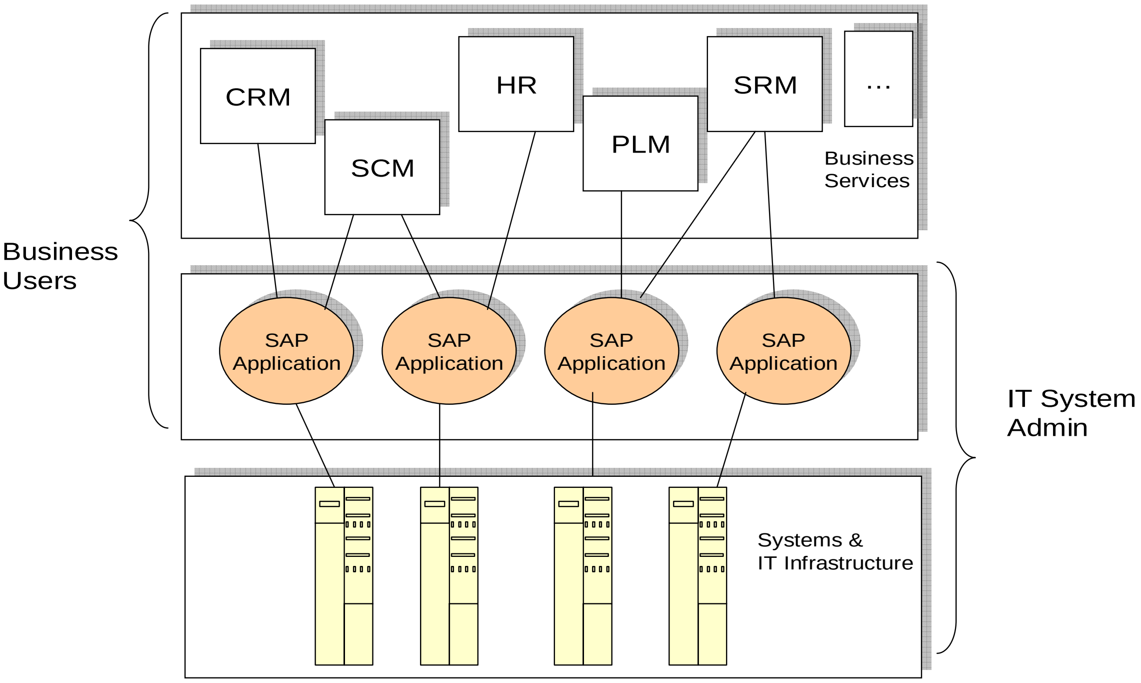


Fig. 3. Business Services Underpinned by SAP Applications

New users can join the organization and require access rights for these services; they can leave or change their roles. At the stake it is not only the accurate management of user accounts and rights, but also ensuring compliance to laws, mitigating security risks, enhancing productivity and coping with a limited budget. As discussed in Section 2, investment choices are dictated by priorities and strategic aspects of relevance for the decision makers. Various trade-offs are possible, each requiring a different mix of IAM investments.

In general, investments in the IAM space can be classified in terms of: *provisioning, compliance and enforcement* [6,25]. Investments in *provisioning* (e.g. user account management) have a direct impact on productivity. For SAP applications, this ranges from ad-hoc processes to automated solutions such as SAP Netweaver IAM and APPROVA products. Investments in *IAM compliance* (e.g. monitoring and checking solutions) have a direct impact on governance and compliance aspects (e.g. SOX compliance) but only marginally affect productivity. For SAP applications, this ranges from ad-hoc manual compliance checking to automated tools such as SAP KPI, APPROVA and VIRSA remediation. Investments in *IAM enforcement, provisioning and compliance* have an impact on mitigating security threats.

For each of these IAM investment areas we identified ***5 classes of investment levels***, in the [1-5] range, with an increasing impact in terms of effectiveness of the involved control points, policies and costs. The lowest investment levels usually involve *ad-hoc processes and manual approaches*. The intermediate levels involve *hybrid approaches, with degrees of automation and policy definitions*. The highest investment levels involve *strong automation and integration with security & business policies*. A detailed description of these investment classes is provided in Section 4.1.

The interviewed security & IAM experts highlighted the fact that (*IAM) **enforcement*** (e.g. authentication and IT system security controls for patching, anti-viruses, etc.) *is currently not a major concern*, at least for medium-large organizations; this is a relatively mature area, where the implications are reasonably understood and various investments have already been made. Based on our classification of investment levels, we estimated that the organization under analysis already made *enforcement investments* comparable to *level 4* i.e. corresponding to the presence of general security policies, deployment of suitable control points and IT security technologies as well as processes for the reassessment of policies and control points.

The case study focused on the problem where the decision maker is primarily interested in *exploring investment options and trade-offs* in the space of *compliance* and *provisioning* to achieve strategic outcomes of relevance. Sections 5, 6 and 7 describe how the methodology has been applied to provide decision support.

4.1 Analysis of IAM Investments

As anticipated above, the three common classes of IAM investments are:

- **IAM provisioning:** it is concerned with the management of users' accounts and access rights. This usually involves approval (e.g. getting management authorizations) and deployment steps. These steps are dealt with when a new user joins an organisation (and requires business access to SAP applications/business services), changes role or leaves the organisation. Different degrees of automation can be provided depending on the technological solutions that have been adopted.
- **IAM compliance:** it is concerned with monitoring aspects, to detect failures (e.g. to comply with SOX) and might include degrees of remediation capabilities.
- **IAM enforcement:** it is concerned with authentication, access control and authorization aspects, which are often coupled with other security enforcement control points, including: firewalls, anti-viruses, patching, vulnerability threat management, etc.

Various IAM control points, technologies and solutions are available for each of the above investment areas. For the purpose of this case study we specifically focused on a few *IAM provisioning and compliance* control points of relevance for SAP applications. A non-exhaustive list of these control points follows:

- **Oracle, SUN, etc. IAM provisioning solutions** [2]: these solutions provide user and administration management capabilities, including the possibility to associate access rights to user, based on approval processes, deal with their deployment and subsequent update;
- **SAP Netweaver IAM** [3]: this solution centrally manages user accounts (identities) in a complex system landscape. This includes both SAP and non-SAP systems. The solution provides an authoritative, single source of user information and enables self-service management of user information and authorizations using workflow technology;
- **SAP VIRSA** [4]: this tool supports the explicit management of Separation of Duties (SoD) and deals with conflict management, during the provisioning phase. It also supports governance and compliance checking to mitigate involved risks;
- **APPROVA Access Manager** [5]: this solution automates user access requests and role changes while performing an analysis of control violations. It also provides "what if" analyses of requests or implement a comprehensive compliant provisioning process;
- **SAP KPI management and SAP reporting tools**: these tools and solutions provides additional monitoring and reporting capabilities, based on predefined or configurable Key Performance Indicators (KPI)

Provisioning management solutions (ranging for ad-hoc processes to fully deployed IAM provisioning solutions, such as SAP Netweaver IAM and APPROVA products) aim at ensuring that user accounts and access rights are correctly provisioned and de-provisioned. They can provide different degrees of support for the involved approval and deployment phases [6]. They affect productivity (by minimising lack of access), security incidents (e.g. exploitations of wrong access/hanging accounts) and compliance (due to finding of access misconfigurations).

Compliance management solutions (ranging from ad-hoc manual compliance checking to automated compliance management tools such as SAP KPI, APPROVA and VIRSA remediation) can help to ensure that access control and security violations are identified and potentially remediated. They not only help minimize the audit failures, but also reduce the number of security incidents. These compliance solutions do not usually affect/improve productivity as they focus on identifying security violations rather than business issues.

The table below describe the meaning of the 5 classes of investment levels ([1-5] range), annotated with some specific examples of the technologies and control points (CPs) of relevance:

Type of IAM Investment	**Investment Levels**
Provisioning	1. Ad-hoc, manual approaches both for approval and deployment steps. *CP Technologies: NONE* 2. Manual approach to deal with approval and deployment but driven by common/centralised policies *CP Technologies: email (notifications)* 3. Automated approval approach and manual deployment, driven by centralised policies. Hybrid approach to user account removal *CP Technologies: web service-based approval notifications, integration with enterprise LDAP directory* 4. Automated approval and deployment approach (driven by common/centralised policies) *CP Technologies: general purpose* Oracle/SUN/etc. IAM provisioning solutions 5. Automated approval and deployment approach along with tools supporting further compliance controls, such as SoD, SOX compliance, etc. (driven by common/centralised policies) *CP Technologies: SAPNetweaver (integrated SAP IAM), VIRSA (SoD conflict management and provisioning), APPROVA Access Manager*
Compliance	1. Ad-hoc, manual auditing and compliance-checking approach. Ad-hoc remediation activities. *CP Technologies: NONE* 2. Manual internal compliance-checking approach but driven by centralised/common policies. Mainly ad-hoc remediation activities. *CP Technologies: Self-assessment forms* 3. Hybrid approach involving manual and degrees of automation of internal compliance checking. Mainly ad-hoc remediation activities. *CP Technologies: SAP KPI management,* *SAP reporting tools* 4. Automation of internal compliance checking. Degrees of automations of remediation activities. *CP Technologies: APPROVA and* *SAP KPI management* 5. Automation of internal compliance checking and remediation activities.

	CP Technologies: VIRSA (automated, total remediation)
Enforcement	1. Ad-hoc security practices and enforcement (authentication, access control/authorization, vulnerability threat management, etc.). Ad-hoc choices for control points and security approaches 2. Security practice based on common sense/good practice. General security policies. Ad-hoc interpretation and deployments of policies. 3. General security policies and guidelines on how to interpret and deploy them. **4. General security policies and guidelines on how to interpret and deploy them. Guidelines on recommended control points and IT security technologies. Degrees of reassessment of policies and control points.** 5. General security policies and guidelines on how to interpret and deploy them. Guidelines on recommended control points and IT security technologies. Methodological reassessment of policies and control points.

The following table summarises the potential technological control points that can be adopted by an organisation, based on various combinations of investment levels in the space of *provisioning and compliance*:

Provisioning Levels → **Compliance Levels**	**1**	**2**	**3**	**4**	**5**
1	NONE	Emails	Web service-driven notifications; Integrated enterprise LDAP	Oracle/SUN/etc. IAM provisioning solutions	Netweaver, VIRSA, APPROVA Access Manager
2	Self-assessment forms	Emails; Self-assessment forms	Web service-driven notifications; Integrated enterprise LDAP; Self-assessment forms	Oracle/SUN/etc. IAM provisioning solutions; Self-assessment forms	Netweaver, VIRSA, APPROVA Access Manager; Self-assessment forms
3	SAP KPI management; SAP reporting tools	Emails; SAP KPI management; SAP reporting tools	Web service-driven notifications; Integrated enterprise LDAP; SAP KPI management; SAP reporting tools	Oracle/SUN/etc. IAM provisioning solutions; SAP KPI management; SAP reporting tools	Netweaver, VIRSA, APPROVA Access Manager; SAP KPI management; SAP reporting tools
4	APPROVA + SAP KPI management	Emails; APPROVA + SAP KPI management	Web service-driven notifications; Integrated enterprise	Oracle/SUN/etc. IAM provisioning solutions; APPROVA + SAP KPI management	Netweaver, VIRSA, APPROVA Access Manager; APPROVA + SAP KPI management

			LDAP; APPROVA + SAP KPI management		
5	VIRSA	Emails; VIRSA	Web service-driven notifications; Integrated enterprise LDAP; VIRSA	Oracle/SUN/etc. IAM provisioning solutions; VIRSA	Netweaver, VIRSA, APPROVA Access Manager

5. IAM Economic Analysis: Elicitation of Preferences

The approach we adopted to elicit strategic preferences from the decision maker consists of *three phases*.

Phase 1 involved engaging, discussing and eliciting the set of *strategic aspects/outcomes* of relevance for the decision maker. The decision maker confirmed that ***Security Risks***, ***Productivity***, ***Compliance and Costs*** are at the top of their concerns**.** As discussed in Section 2, this determines the utility function components of the decision maker. A clear semantic has been agreed with the decision maker for each of these strategic outcomes, along with meaningful (IT) metrics to measure and estimate them:

Security risks	Predicted ***number of breaches/incidents*** (e.g. exploitations of credentials, unauthorised accesses, etc. due to internal/external attacks) that happens in 1 year timeframe. We looked for the max number of incidents the decision maker accepts happening and the min number of incidents they would be reasonably comfortable with
Productivity	Predicted ***ratio (percentage) of all user accounts (& related access rights) that the organisation would have liked to have been provisioned*** in 1 year. A productivity of 70% means that only 70% of all the accounts that should have been correctly provisioned actually have been provisioned.
Compliance	Predicted ***number of audit findings/violations*** (e.g. # SOX compliance audit violations) in 1 year. The lower the number, the higher is compliance.
Costs	Approximated costs in terms of ***budget ($) to be invested in IAM initiatives in 1 year timeframe***.

In **Phase 2**, for each of the above strategic outcomes, we asked the decision maker to tell us which values were “good enough” (min value, i.e. where they would not be interested in spending more money to achieve more) and which ones were “just acceptable” (max value, i.e. the level, below which they became extremely concerned to address the issue). This helped us to identify ***value ranges***.

The decision maker expressed the following preferences:

- **Security risks**: *min: 1, max: 3*;
- **Productivity**: *min 100%, max 100%*;
- **Compliance** (violations): *min: 1, max: 3*;
- **Costs**: *min: 500K $, max: 10M $*.

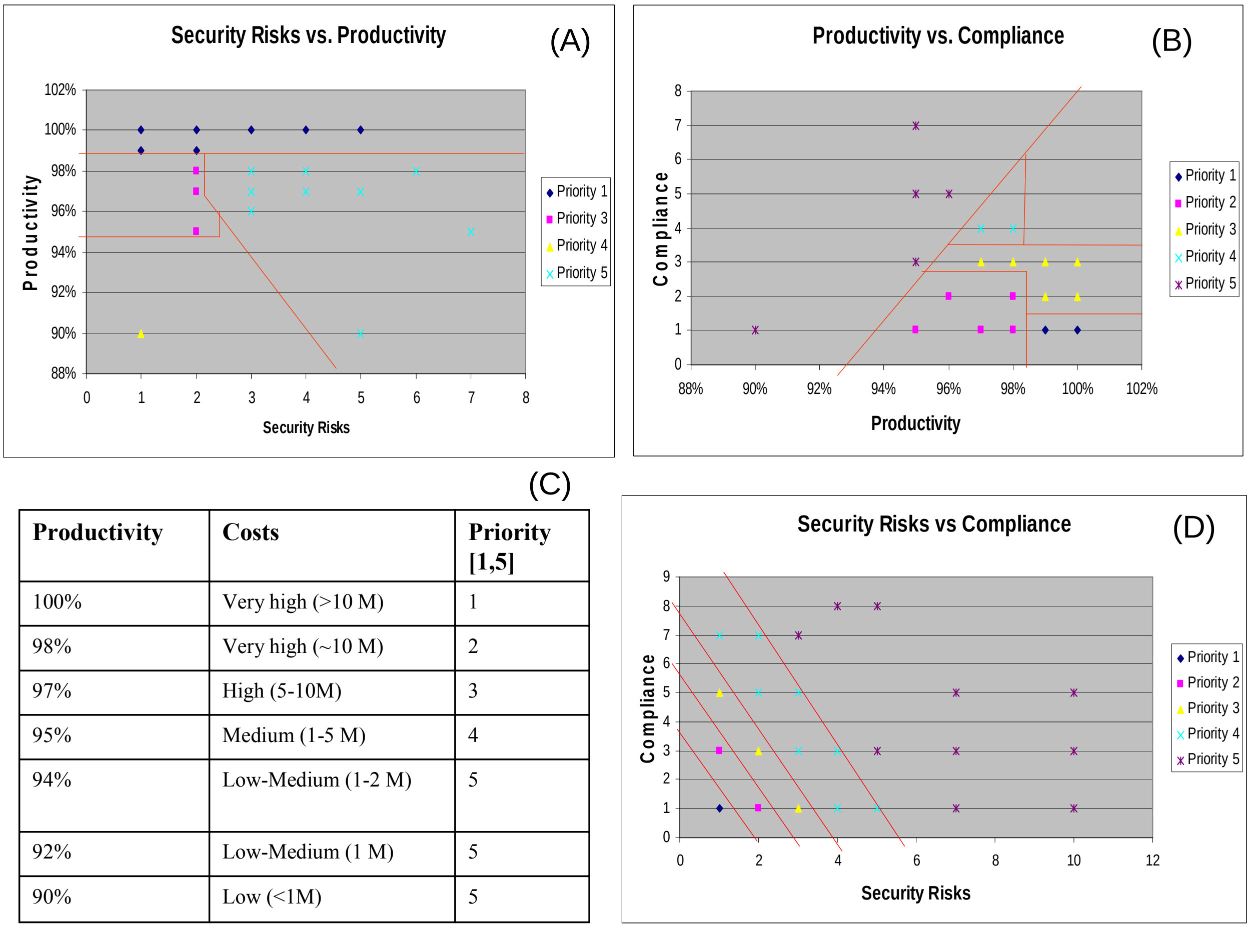
We deduced that for this decision maker ***productivity*** is a key priority whilst the ***cost*** factor is not a major issue. The decision maker showed some degrees of tolerance in terms of ***security risks*** and ***compliance violations***.

Finally, in **Phase 3** we asked the decision maker for their relative preferences between values of (paired) outcomes (e.g. productivity vs. compliance), to highlight tension points and quantify/qualify trade-offs. We created four questionnaires populated with values in the ranges chosen in *phase 2*: some "outlier" values were introduced, to further check for preferences. The explored trade-offs are shown below.

Security Risks vs. Productivity	Exploring how much the decision maker is willing to compromise security in order to improve productivity (or the way around)
Productivity vs. Compliance	Lack of compliance can sometime be acceptable to increase productivity and the way around (due to stronger controls and bureaucratic processes)
Productivity vs. Costs	Exploring how much the decision maker is willing to compromise in terms of productivity, based on the involved costs
Security Risks vs. Compliance	Exploring the relative preferences between security risks and compliance. Strong preferences in the compliance area indicate the attitude at accepting low security risks especially the ones causing audit failures

Section 5.1 provides the details about the type of questionnaires that have been generated.

We asked the decision maker to state their priorities, in the [1-5] range, ***where 1 meant the highest priority and 5 meant the lowest priority***. Figure 4 shows the results. The detailed outcomes of the preference elicitation process are discussed in Section 5.2.



Productivity	Costs	Priority [1,5]
100%	Very high (>10 M)	1
98%	Very high (~10 M)	2
97%	High (5-10M)	3
95%	Medium (1-5 M)	4
94%	Low-Medium (1-2 M)	5
92%	Low-Medium (1 M)	5
90%	Low (<1M)	5

Fig. 4. Results of Elicitation of Decision Maker's Relative Preferences

Each point in the (A), (B) and (D) graphs represents a pair of values (in the questionnaire) prioritized by the decision maker, based on their relative preferences. Various *sub-areas* of the graph have been identified based on these priorities.

Figure 4-(A) shows that the decision maker is willing to accept security risks as long as high productivity (99%-100%) is achieved — *no priority 2 preferences were expressed*. The graph (B) in Figure 4 also confirms the decision maker's bias towards productivity. However, graphs (B) and (D) show that compliance has a high priority too and the acceptable trade-offs against productivity and security risks. Finally, the table (C), in Figure 4, confirms that the decision maker willingness to make high IAM investments to achieve productivity.

Despite the current crude approach, the results show that it is possible to explicitly capture decision maker's strategic preferences and reason on them. These outcomes have been discussed and validated with the decision maker. The next steps of the methodology explored which IAM investments are most suitable to achieve these strategic outcomes.

The remaining part of this section provides details about the overall preference elicitation process, as well as the data we collected in the interview.

5.1 Questionnaire Templates and Preference Elicitation Details

In ***phase 2*** of the preference elicitation process, four tables where generated (and added to the questionnaire we submitted to the decision maker), to gather the value ranges for the involved outcomes of interest:

a) Table to elicit value ranges for **Security Risks:**

	Max (just acceptable)	**Min (comfortable with)**
Security Risks Number of incidents/breaches that happen in 1 year	?	?

Examples of range values	10	←→	1
	100	←→	10
	1000	←→	100

b) Table to elicit value ranges for **Productivity:**

	Just Acceptable	**Good Enough**
Productivity Ratio/percentage of all user accounts that you would have liked to have been provisioned, in 1 year	?	?

Examples of range values	10%	←→	50%
	30%	←→	70%
	50%	←→	90%

c) Table to elicit value ranges for **Compliance Violation:**

	Just Acceptable	**Good Enough**
Compliance violations number of audits findings (failures) in 1 year	?	?

Examples of range values	2	←→	1
	5	←→	2
	10	←→	5

d) Table to elicit value ranges for **Costs:**

	Minimum	**Max**
Costs budget ($) to invest in IAM initiatives in 1 year timeframe	?	?

Examples of range values	100K	←→	1M
	1M	←→	10M
	5M	←→	50M

In ***phase 3*** of the preference elicitation process, four questionnaires (consisting of tables and graphs) were created to explore decision makers' potential trade-offs, tension points between the aspects of relevance (security risks, productivity, compliance and costs), relative preferences and priorities: *Security Risks vs. Productivity; Productivity vs. Compliance; Productivity vs. Costs; Security Risks vs. Compliance.*

1) Security Risks vs. Productivity

Security Risks	**Productivity**	**Priority [1,5]**

2) Productivity vs. Compliance

Productivity	**Compliance**	**Priority [1,5]**

3) Productivity vs. Costs

Productivity	**Costs**	**Priority [1,5]**

4) Security Risks vs. Compliance

Security Risks	**Compliance**	**Priority [1,5]**

*Relative preferences in terms of **costs** have only been gathered in conjunction of the **productivity** aspect. High costs are usually involved when dealing with productivity issues rather than compliance, so it is important to explore trade-offs and preferences between productivity and costs. As mentioned in Section 4, we assumed that the organisation has already made appropriate investments in the space of enforcement, hence dealing with security risks.*

The above ***"templates"*** were used to instantiate the actual table that we submitted to the decision maker, filled with values generated from the information elicited in phase 2. Section 5.2 provides the details.

5.2 Preference Elicitation Results

This section provides the details about the results of the preference elicitation activity carried out with the decision maker, in particular how the data collected in *phase 2* has been used to drive *phase 3.*

5.2.1 Elicitation of Value Ranges - Phase 2

The outcomes collected from the decision maker during ***phase 2*** are the following ones:

	Max (just acceptable)	**Min (comfortable with)**
Security risks Number of incidents/breaches that happen in 1 year	**3**	**1**

	Just Acceptable	**Good Enough**
Productivity Ratio/percentage of all user accounts that you would have liked to have been provisioned, in 1 year	**100%**	**100%**

	Just Acceptable	**Good Enough**
Compliance violations number of audits findings (failures) in 1 year	**3**	**1**

	Minimum	**Max**
Costs budget ($) to invest in IAM initiatives in 1 year timeframe	**500K** **(SSO)**	**10m** **(IAM Lifecycle)**

5.2.2 Elicitation of Relative Preferences - Phase 3

The results obtained from *phase 2* were used to generate the questionnaires for ***phase 3***, to elicit relative preferences and priorities.

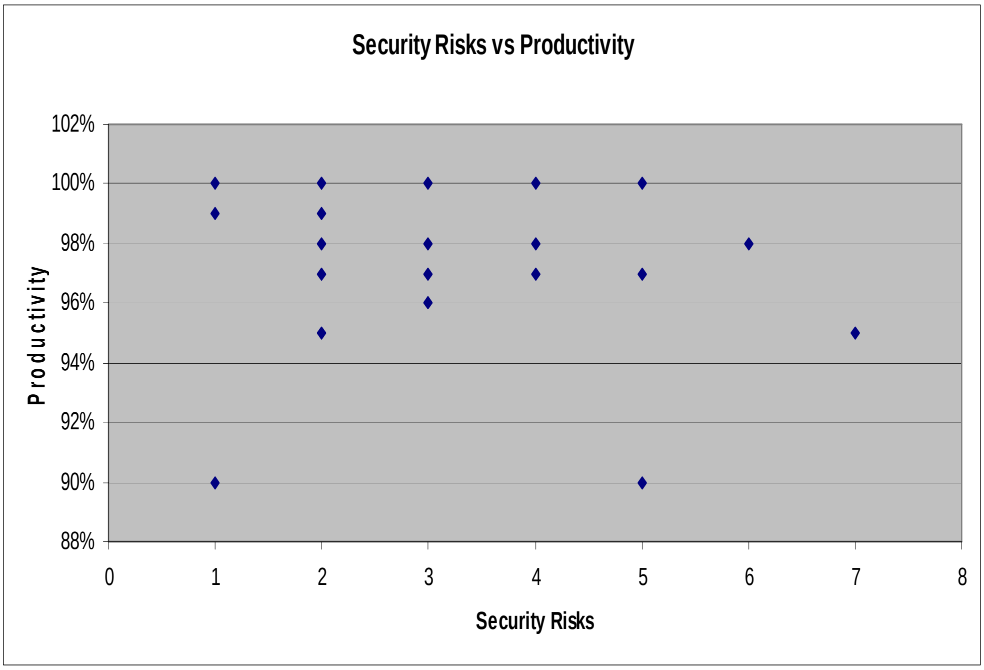
During this phase we learnt that the decision maker was more comfortable to express their relative preferences by reasoning on graphical figures, rather than on tables. As a result, four questionnaires were submitted to the decision maker consisting of both tables and related graphs:

1) Security Risks vs. Productivity

Security Risks	Productivity	Priority [1,5]
1	100%	
2	99%	
2	98%	
3	98%	

2	100%	
1	99%	
3	97%	
3	100%	
2	97%	
3	96%	
7	95%	
5	90%	
4	98%	
5	97%	
4	100%	
5	100%	
6	98%	
4	97%	
2	95%	
1	90%	

The correspondent graphical representation was:

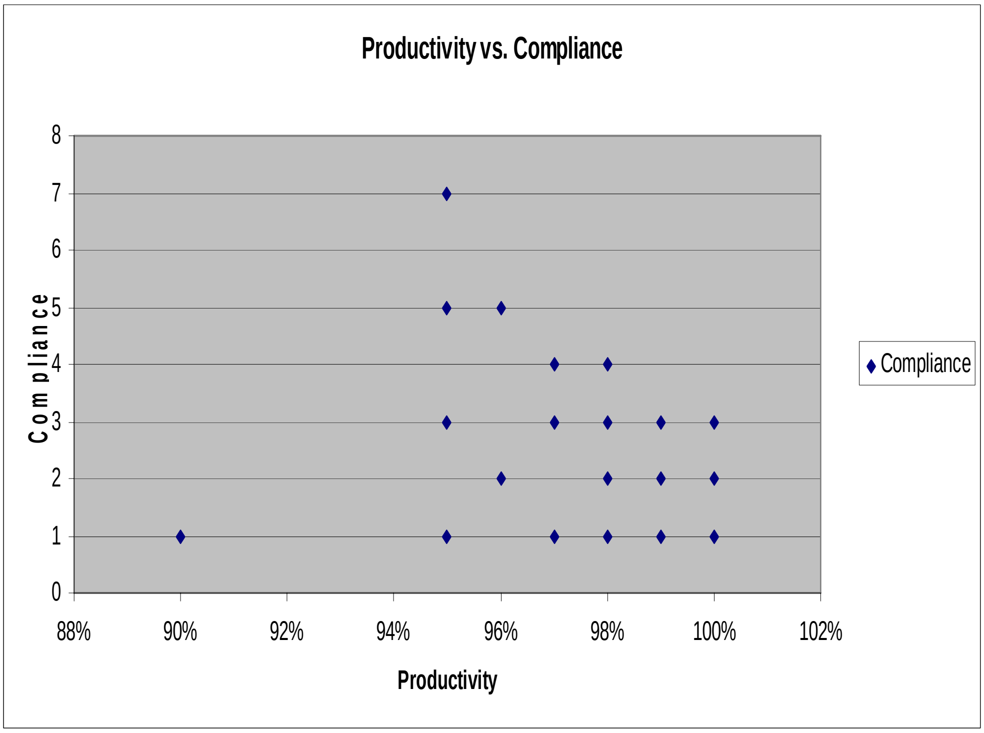


2) Productivity vs. Compliance

Productivity	Compliance	Priority [1,5]
100%	1	
99%	1	
98%	2	
97%	3	
96%	5	
95%	7	
100%	2	
99%	2	
98%	1	

98%	3	
97%	4	
95%	5	
100%	3	
99%	3	
98%	4	
97%	1	
96%	2	
95%	3	
95%	1	
90%	1	

The correspondent graphical representation was:



3) Productivity vs. Costs

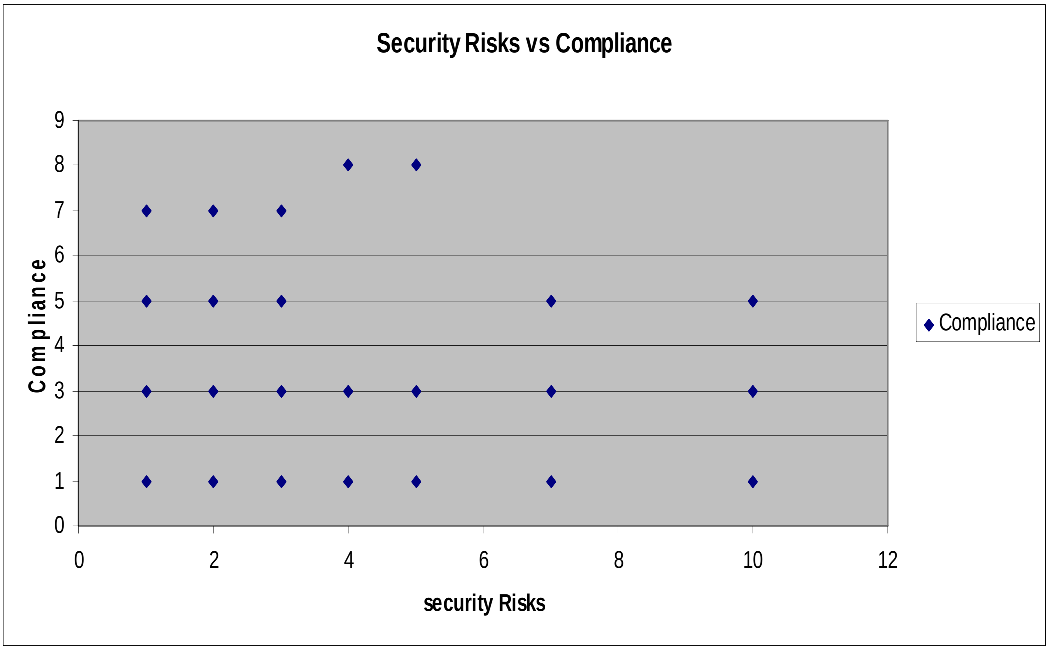
Productivity	Costs	Priority [1,5]
100%	Very high (>10 M)	
98%	Very high (~10 M)	
97%	High (5-10M)	
95%	Medium (1-5 M)	
94%	Low-Medium (1-2 M)	
92%	Low-Medium (1 M)	
90%	Low (<1M)	

4) Security Risks vs. Compliance

Security Risks	Compliance	Priority [1,5]
1	1	
1	3	
1	5	

1	7	
2	1	
2	3	
2	5	
2	7	
3	1	
3	3	
3	5	
3	7	
4	1	
4	3	
4	8	
5	1	
5	3	
5	8	
7	1	
7	3	
7	5	
10	1	
10	3	
10	5	

The correspondent graphical representation was:



The decision maker provided their input primarily by using the graphical diagrams (with the exception of the cost diagram) and by segmenting the space of relative preferences (represented as the set of dots in the graphs) into areas, each of them with an associated priority in the [1-5] range.

Figures 5, 6 and 7 show the outcomes we obtained from the decision maker. Each figure (followed by the correspondent annotated table) highlights the priorities expressed by the decision maker:

1) Prioritization of Relative Preferences for "Security Risks vs. Productivity"

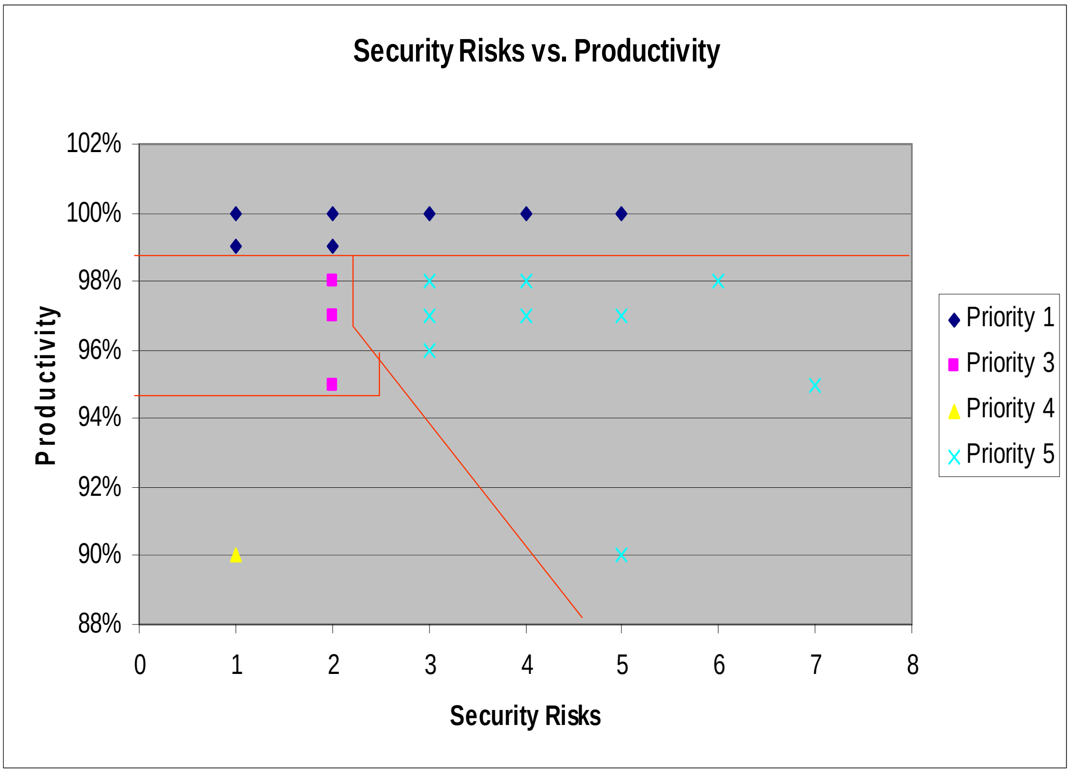


Fig. 5. Strategic Preferences - Comparing Security Risks vs Productivity

Security Risks	Productivity	Priority [1,5]
1	100%	1
2	99%	1
2	98%	3
3	98%	5
2	100%	1
1	99%	1
3	97%	5
3	100%	1
2	97%	3
3	96%	5
7	95%	5
5	90%	5
4	98%	5
5	97%	5
4	100%	1
5	100%	1
6	98%	5
4	97%	5
2	95%	3
1	90%	4

These outcomes confirm the relevance that productivity has for the decision maker. No real compromises have been made in terms of having better security with some degradation of productivity.

2) Prioritization of Relative Preferences for "Productivity vs. Compliance"

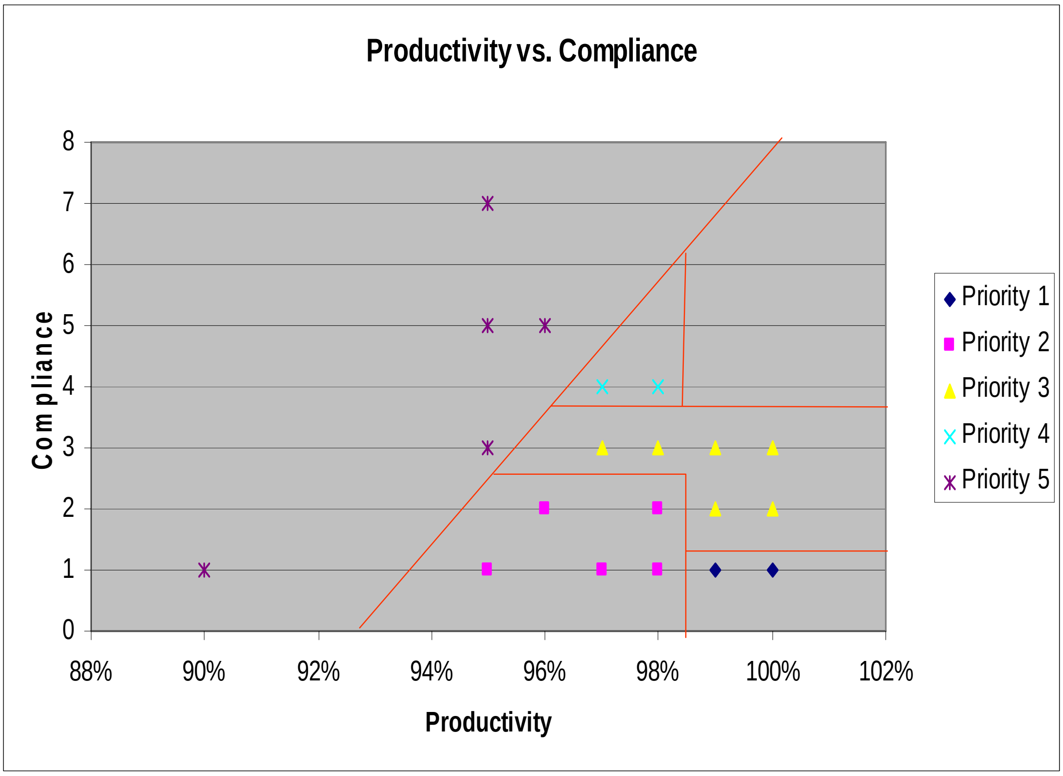


Fig. 6. Strategic Preferences - Comparing Productivity vs. Compliance

Productivity	**Compliance**	**Priority [1,5]**
100%	1	**1**
99%	1	**1**
98%	2	**2**
97%	3	**3**
96%	5	**5**
95%	7	**5**
100%	2	**3**
99%	2	**3**
98%	1	**2**
98%	3	**3**
97%	4	**4**
95%	5	**5**
100%	3	**3**
99%	3	**3**
98%	4	**4**
97%	1	**2**
96%	2	**2**
95%	3	**5**
95%	1	**2**
90%	1	**5**

These outcomes confirm the key strategic preference towards productivity. However, some flexibility has been demonstrated in trading productivity against compliance, despite this having lower priority (2).

3) Prioritization on Relative Preferences for “Productivity vs. Costs”

Productivity	Costs	Priority [1,5]
100%	Very high (>10 M)	1
98%	Very high (~10 M)	2
97%	High (5-10M)	3
95%	Medium (1-5 M)	4
94%	Low-Medium (1-2 M)	5
92%	Low-Medium (1 M)	5
90%	Low (<1M)	5

These outcomes highlight that the cost aspect is not really an issue for this decision maker. High costs are acceptable and sustainable as long as they allow the organisation to achieve high productivity.

4) Prioritization of Relative Preferences for “Security Risks vs. Compliance”

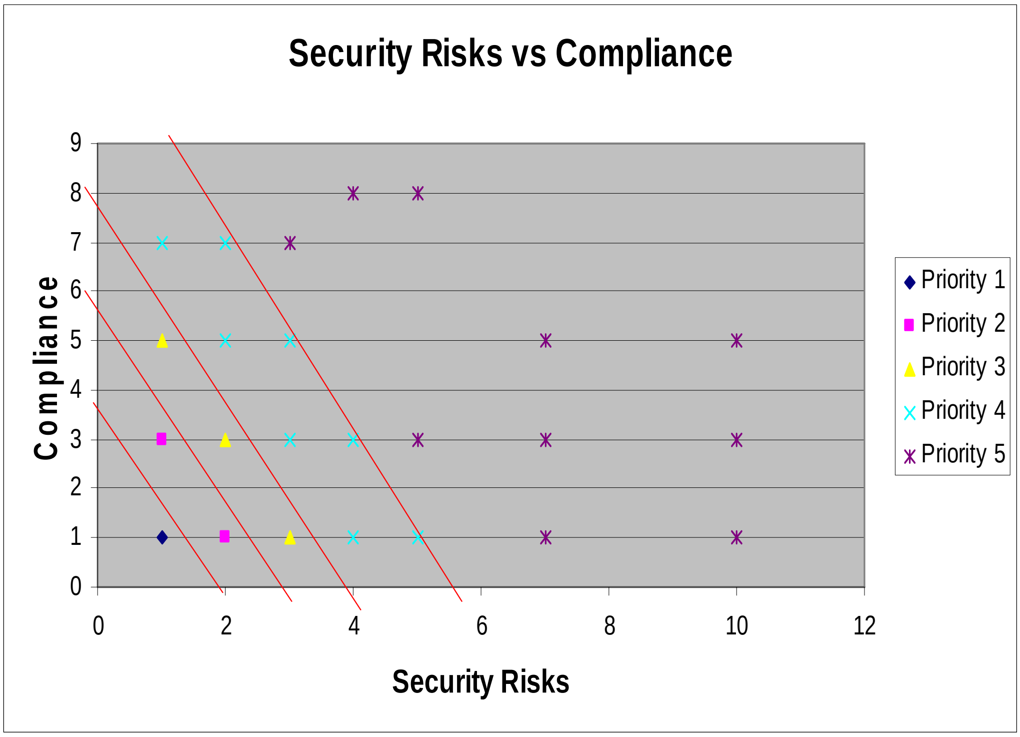


Fig. 7. Strategic Preferences - Comparing Compliance vs Security Risks

Security Risks	Compliance	Priority [1,5]
1	1	1
1	3	2
1	5	3
1	7	4
2	1	2
2	3	3
2	5	4
2	7	4
3	1	3
3	3	4
3	5	4
3	7	5

4	1	4
4	3	4
4	8	5
5	1	4
5	3	5
5	8	5
7	1	5
7	3	5
7	5	5
10	1	5
10	3	5
10	5	5

These outcomes highlight the importance that also compliance has for the decision makers.

6. Exploring the Impact of Investment Options by Means of Modelling and Simulation

We used modelling and simulation techniques to make predictions about the impact of possible IAM investment options on the outcomes of interest and map them against decision makers' preferences, to identify suitable investments.

Predictive mathematical approaches are suitable to carry out modelling and simulations. The adopted modelling approach is based on "predictive system modelling", specifically "discrete-event probabilistic modeling" [7,32].

Our approach, the mathematical basis of which is presented in [10,28,32,33,34], views a system as having the following key components:

- **Environment**: it is treated as a source of events that are incident upon the system of interest according to given probability distributions;
- **Location:** The components of a system of interest are distributed around a collection of places, which may correspond to geographical or more abstract notions of location;
- **Resource**: this captures the components of the system that are manipulated by its processes e.g. a system, people, etc.;
- **Process**: this captures the (operational) dynamics of the system. Processes manipulate resources in order to deliver the system's intended services or outcomes.

The adopted approach provides advantages over analytical approaches as it explicitly represents the dynamic dependencies and interactions among the involved entities, processes and decisions. This is of relevance for the IAM scenario where a wide variety of events, business processes, systems and human interactions are involved. We used the GNOSIS modelling toolset [9,30] which implements this framework and supports Monte Carlo-style simulations [8].

As result of the analysis of various enterprise environments and the IAM processes impacting business services, we built a *general model*, re-usable in different enterprise contexts with minor changes and the instantiation of a few parameters. The modelled aspects have been discussed and validated with the security and IAM experts. Figure 8 shows the high-level view of the model.

A copy of the GNOSIS model developed for the IAM case study is available in Appendix A.

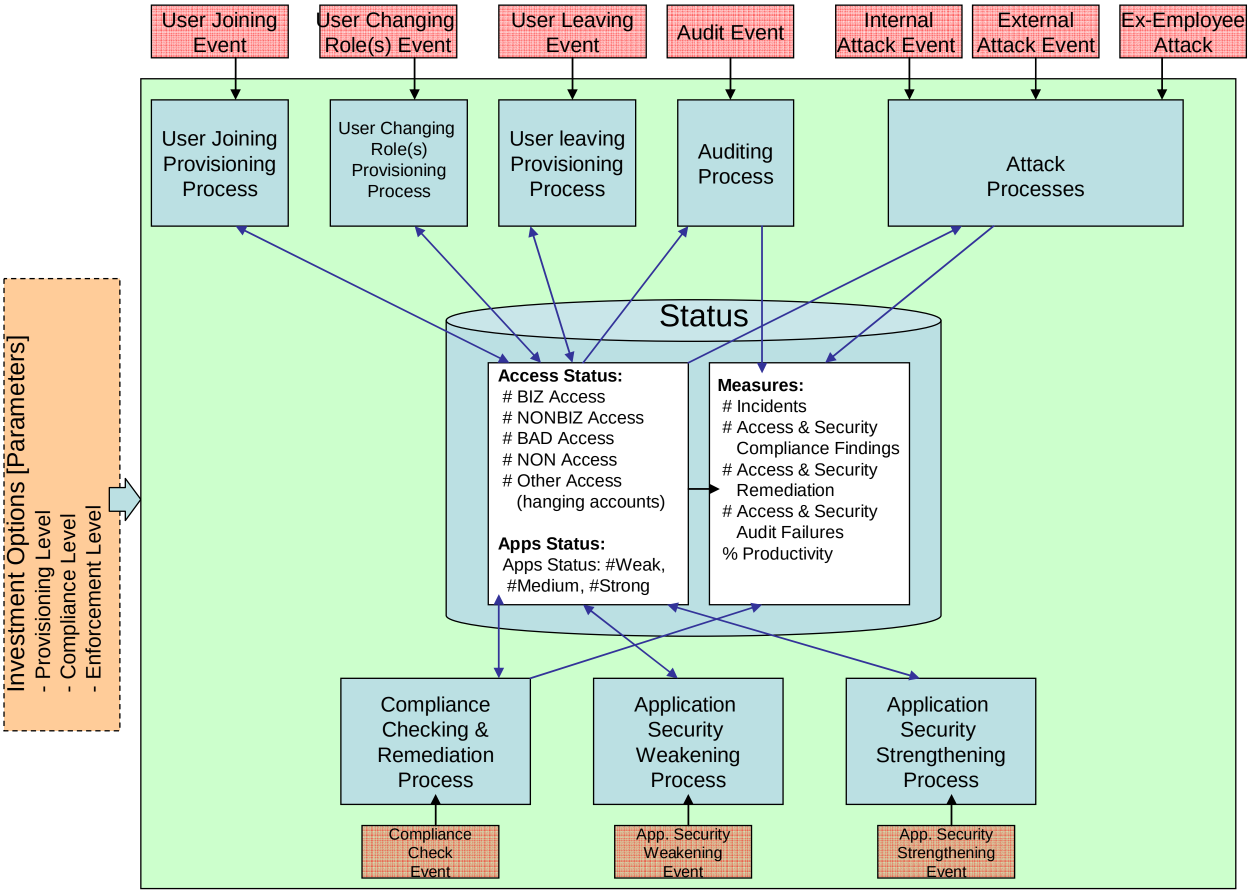

User Joining Event
User Changing Role(s) Event
User Leaving Event
Audit Event
Internal Attack Event
External Attack Event
Ex-Employee Attack
User Joining Provisioning Process
User Changing Role(s) Provisioning Process
User leaving Provisioning Process
Auditing Process
Attack Processes
Investment Options [Parameters]
- Provisioning Level
- Compliance Level
- Enforcement Level
Status
Access Status:
# BIZ Access
# NONBIZ Access
# BAD Access
# NON Access
# Other Access (hanging accounts)
Apps Status:
Apps Status: #Weak, #Medium, #Strong
Measures:
# Incidents
# Access & Security Compliance Findings
# Access & Security Remediation
# Access & Security Audit Failures
% Productivity
Compliance Checking & Remediation Process
Application Security Weakening Process
Application Security Strengthening Process
Compliance Check Event
App. Security Weakening Event
App. Security Strengthening Event

Fig. 8. High-level View of the IAM Model

This model is characterised by the following aspects:

- ***Status*** of the system, including *measures*, number of managed business services/SAP applications, security status of these applications (i.e., weak, medium, strong), number of users, overall status of access rights;
- ***Set of processes*** that can modify the status;
- ***Events*** that trigger processes.

The ***status*** of the model consists of:

- **Status of users' access rights on managed applications**: users' access rights are classified in a few classes and tracked by the model. More details follow;
- **Security status of applications**: the security status of each managed application has been classified as one of the following: *weak, medium or strong*. Application security status can vary over time, based on enforcement investments;
- **Measures:** a few measures have been identified and grounded within modelled processes, related to: *number of incidents deriving from successful attacks, number of access & security compliance checking findings; number of access & security remediation, number access & security audit failures, productivity*. Section 6.2 provides more details about these measures as well as the specific ones that have been used as ***"proxies"*** to estimate the utility function components of relevance to the decision maker.

The *model tracks the users' access rights for the managed SAP applications* to explicitly characterise the *access posture* of the organization and determine the impact on strategic outcomes of interest.

Wrongly provisioned access rights fuel threats & attacks and/or have a negative impact on productivity and compliance (e.g. due to audit failures).

Four categories of access were identified: ***BizAccess*** (legitimate access rights correctly granted), ***NoBizAccess*** (legitimate access rights not granted*)*, ***BadAccess*** (illegitimate access rights, granted) and ***NoAccess*** (illegitimate access rights, not granted). A summary is provided in the following table. ***"Hanging Accounts"***, i.e. those access rights that are still allocated to a user, despite the user has left the organisation or changed role, are also tracked.

User Access Rights	**Actual Situation:** **Access Allowed**	**Actual Situation:** **No Access Allowed**
Expected Situation: **Access Allowed**	**Business Access (BizAccess)**: user provisioned with correct access (as expected) to business applications, as expected	**No Business Access (NoBizAccess):** user has no access to business applications, against what expected
Expected Situation: **No Access Allowed**	**Bad Business Access (BadAccess):** user has access to business applications, against what expected	**No Access (NoAccess)**: user has no access to business applications, as expected

The impact of different *IAM provisioning* and *compliance checking* investments, for investment levels in the [1-5] range, have been factored in the modeled processes by representing the cause-effect relationships that are at the base of failures, mistakes and successes, driven by probability distributions which depend on these investments. As anticipated, the *enforcement* investment level =4.

The IAM model captures the following key processes:

- Provisioning of users' accounts & access rights (user joining, changing roles and leaving);
- Compliance Checking and Remediation activities;
- Auditing activities; Impact of attacks;
- Weakening of SAP applications' security;
- Strengthening of SAP applications' security;
- Threats & attacks.

Processes are triggered by related **events**, some of them exogenous (i.e. not under the control of the IT management teams, such as frequency of attacks, frequency of people joining or leaving the organization, audit checks), some of them endogenous (i.e. that can be affected by the organization, e.g. frequency of compliance checking, security upgrades of applications). These events are characterized by probability distributions.

Two examples of modeled processes are shown in Figures 9 and 10. An overview of the core processes is presented in this section, whilst the full set of modeled processes is presented in section 6.1.

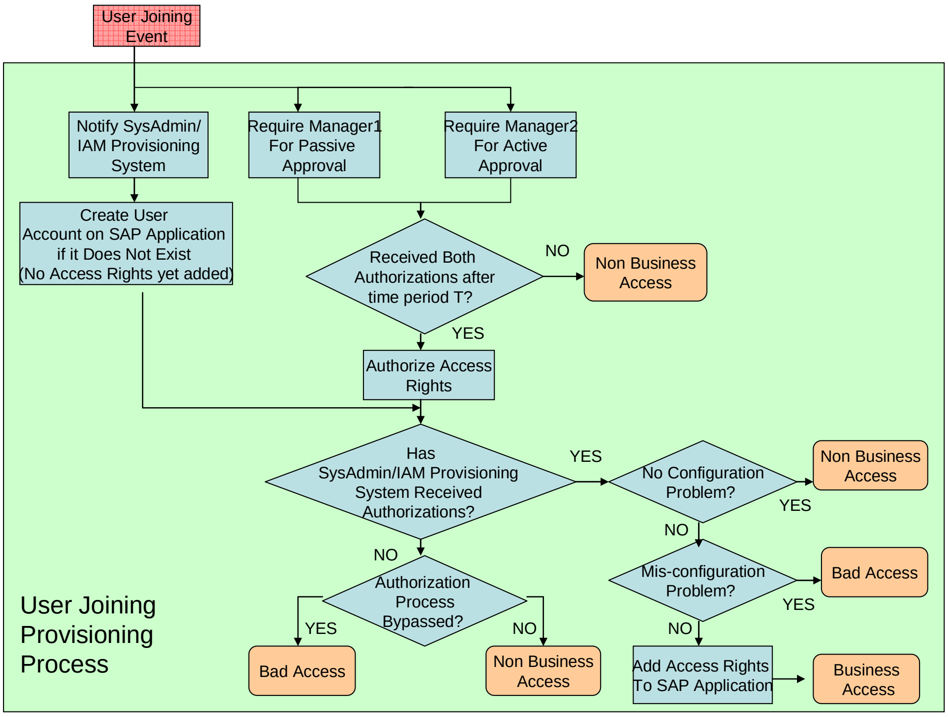

User Joining Event
Notify SysAdmin/ IAM Provisioning System
Require Manager1 For Passive Approval
Require Manager2 For Active Approval
Create User Account on SAP Application if it Does Not Exist (No Access Rights yet added)
Received Both Authorizations after time period T?
NO
Non Business Access
YES
Authorize Access Rights
Has SysAdmin/IAM Provisioning System Received Authorizations?
YES
No Configuration Problem?
Non Business Access
YES
NO
Mis-configuration Problem?
Bad Access
YES
NO
Authorization Process Bypassed?
YES
NO
Bad Access
Non Business Access
NO
Add Access Rights To SAP Application
Business Access
User Joining Provisioning Process

Fig. 9. Modeled User Joining Provisioning Process

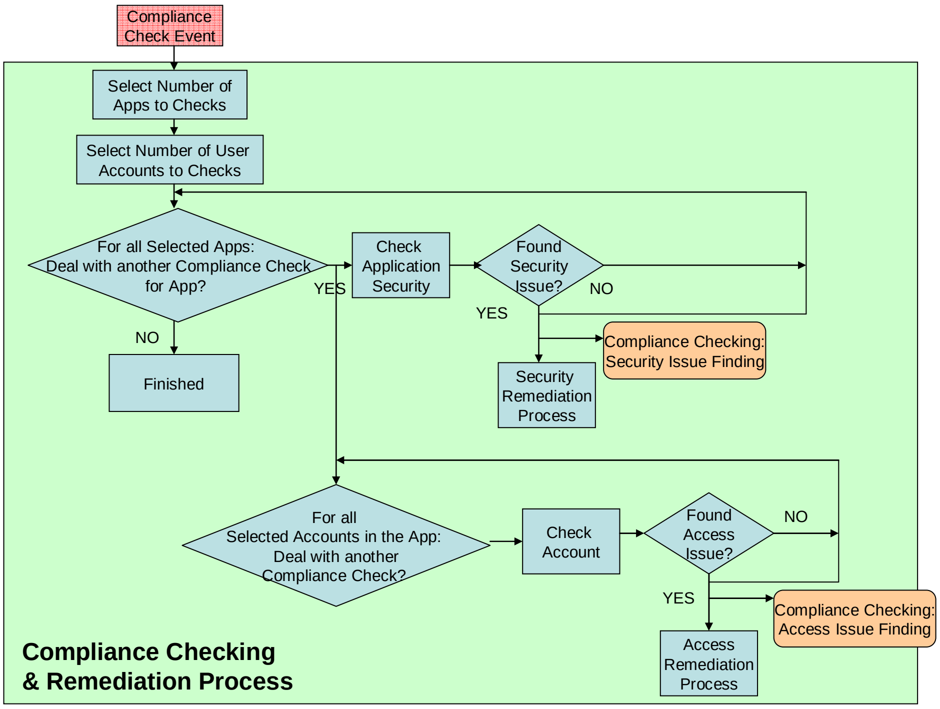

Compliance Check Event
Select Number of Apps to Checks
Select Number of User Accounts to Checks
For all Selected Apps: Deal with another Compliance Check for App?
YES
NO
Finished
Check Application Security
Found Security Issue?
NO
YES
Compliance Checking: Security Issue Finding
Security Remediation Process
For all Selected Accounts in the App: Deal with another Compliance Check?
Check Account
Found Access Issue?
NO
YES
Compliance Checking: Access Issue Finding
Access Remediation Process
Compliance Checking & Remediation Process

Fig. 10. Modeled Compliance Checking and Remediation Process

Figure 9 illustrates the modeled process for *user joining the organizations*. The user provisioning steps of *approval* and *deployment of user accounts* are represented, along with potential failures that can happen, such as misconfiguration, mistakes and attempts to bypass the system, which have impact on access (*BadAccesses* and *NoBizAccesses)*. The higher the provisioning investments the lower is the probability that these mistakes can occur. Similar processes have been modelled for user leaving the company or changing their role.

Figure 10 shows the process for *compliance checking and remediation*. Depending on the level of investment made on compliance, a specific number of SAP applications is checked against their current security level - *modeled as weak, medium, strong* - and the status of user accounts checked to identify bad accesses and hanging account. In case of violation are spotted, remediation activities take place, whose durations depend on these investments. The higher the investment in compliance, the higher the number of violations that can be detected and fixed, hence reducing the security threats and the likelihood of audit failures. Investments in provisioning compete against the ones in compliance, as they reduce the number of potential violations. Compliance investments do not address productivity issues, as compliance checks do not usually detect *NoBizAccess*. The auditing process has been modeled in a similar way, but with the aim of spotting violations that count as failures.

Another example of modeled process (not shown), is about *ex-worker attacks*. In this context skills of employees are taken into account as well as the current intranet protection level and the presence of hanging accounts. These aspects determine the likelihood of successful attacks to the organizations. The number of successful incidents is measured. Assumptions are made on the external threat environment, such as the frequency of attacks and determination of attackers.

The complete list of modelled threats (as processes) follows:

- **Internal threats**: these threats are posed by employees, who might accidentally or deliberately misuse their credentials and access rights to get access to confidential information, create bogus identities, get financial advantages, sell credentials, etc.;
- **External threats**: there threats are posed by external attackers (including ex employees), which might leverage exposed credentials or vulnerable systems;
- **Ex-workers threats**: these are a special type of external threats, posed by ex-workers who might exploit additional knowledge and credentials to attack the organisation, potentially also during the process of leaving the organisation (or soon after doing it).

The likelihood of these threats in succeeding is affected by the various IAM investments.

The overall processes impact the status of the model, by modifying the values of various *measures*, which (as anticipated) include: *number of occurred incidents; number of access & security compliance findings and remediation; number of access and security audit failures; productivity*.

Some of these measures (metrics) are *proxies* of the utility function's components which reflect the priorities and preferences of the decision maker, as discussed in Section 5. Specifically, the *productivity* measure, defined as "ratio/percentage of all user accounts that the organisation would have liked to have been provisioned", is calculated as:

(bizaccess + badaccess)/ (bizaccess + nobizaccess + badaccess)".

The cost element has not been directly represented in the model, as it is mainly a function of the provisioning and compliance investment levels.

The model is driven by a set of parameters which determine and affect the following aspects: *Provisioning, Compliance and Enforcement Investment Levels*; *Status Initialization; Threat Environment; Events; Processes.*

Probability distributions associated to these parameters have been derived from empirical data obtained from audit logs of the organization and discussions with the decision makers and IT teams.

Probabilities related to events have been modeled with *negative exponential* (negexp) distributions. Probabilities such as likelihood of mistakes, faults, etc. vary depending on the investment levels in the [1-5] range.

Section 6.1 provides the detailed overview of the various components involved in the IAM model. Section 6.2 discusses the various parameters and assumptions made in the model. Finally, Section 6.3 discusses the simulations that have been carried out and related experimental results.

6.1 Processes Represented in the IAM Model

Various processes of relevance for the IAM case study have been modelled. As anticipated, we abstracted, parameterised and represented processes that are common to various enterprise environments where IAM solutions are deployed to support business services and deal with security matters.

These processes are triggered by stochastic events i.e. events that depend on probability distributions (e.g. probability that a new user joins or leaves the organisation). Various activities involved in these processes are also driven by probabilistic distributions (e.g. probability of mis-configuration during a provisioning activity, etc.). Probability distributions are determined and/or affected by a variety of factors:

- IAM investment levels (on provisioning, compliance and enforcement areas);
- Parameters;
- Model status, for example in terms of the status of users' access rights and applications.

The complete list of the probability distributions and parameters is provided in Section 6.2. The remaining part of this section focuses on modelled processes.

A first core IAM aspect we modelled is related to ***Provisioning Management***. Three associated processes have been explicitly modelled corresponding to three key events:

- User joining the organisation and requiring access rights to protected applications
- User leaving the organisation
- User changing their role

Figure 11 illustrates the common aspects involved in the provisioning process of a *new user joining the organisation*:

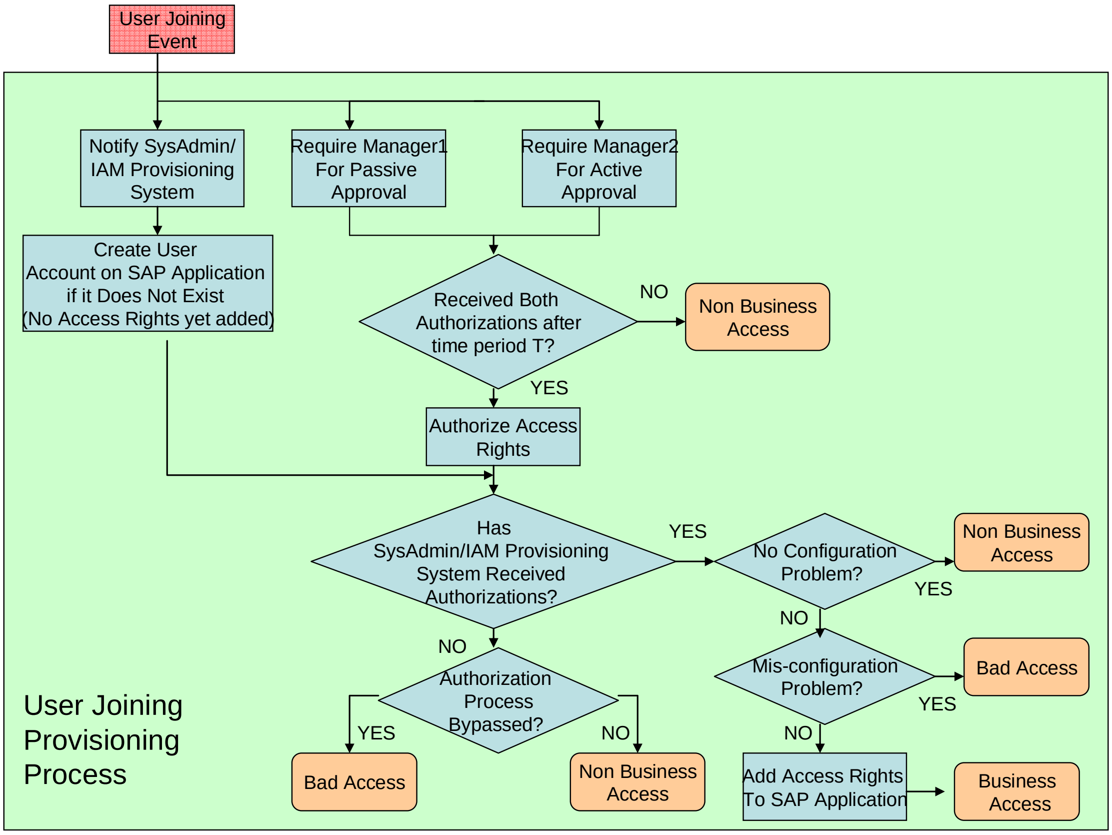

User Joining Event
Notify SysAdmin/ IAM Provisioning System
Require Manager1 For Passive Approval
Require Manager2 For Active Approval
Create User Account on SAP Application if it Does Not Exist (No Access Rights yet added)
Received Both Authorizations after time period T?
NO
Non Business Access
YES
Authorize Access Rights
Has SysAdmin/IAM Provisioning System Received Authorizations?
YES
No Configuration Problem?
Non Business Access
YES
NO
Mis-configuration Problem?
Bad Access
YES
NO
Add Access Rights To SAP Application
Business Access
NO
Authorization Process Bypassed?
YES
Bad Access
NO
Non Business Access
User Joining Provisioning Process

Fig. 11. User Joining - Provisioning Process

The core aspects involved in this process include:

- The user that joins the organisation requires access rights for a set of business services, (underpinned by SAP applications);
- For each application involved in the provisioning process, either a *System Admin* or an *automated IAM provisioning system* (the level of automation available depends on the investments made in the provisioning area) is notified to carry out configuration steps. At the same time *passive and active approval request*s are sent to the user's managers;
- The *system admin* or the *IAM provisioning system* creates a user account for the application without any access rights and waiting for management authorizations;
- Two managers will be required to, respectively, passively and actively approve the granting of users' access rights. It might happen that these authorizations are never received (because of faults or lack of management activities). This prevents the user for accessing the resources. The model keeps into account this access problem, by labelling it as a "non business access". This affects the productivity of the user, as they cannot carry out their jobs;
- In case of successful authorization, the requested access rights might be properly configured for the user. This is accounted in the model as "business access". However, problems might happen during this process. User access rights might never be granted (e.g. because of failures in the system administrator or automated systems when acting on this) or they might be mis-configured (i.e. the granted access rights are not the ones that have been authorised for). This is accounted in the model respectively as a "non business access" and "bad access". Bad access has a negative impact on audits and can potentially enable attacks that leverage and misuse these credentials. Non business access has a negative impact on productivity;
- If no authorization was received, the user might still try to bypass the system and procedures (for example by directly interacting with system administrators). In case of success, the model tracks of this access anomaly as "bad access".

The probability that some activities succeed and/or that problems happen depends on the level of investments made in the *provisioning area*. The higher the investments the lower are the probabilities that mistakes and failures occur.

Figure 12 illustrates common aspects involved in the provisioning process *for a user leaving the organisation*:

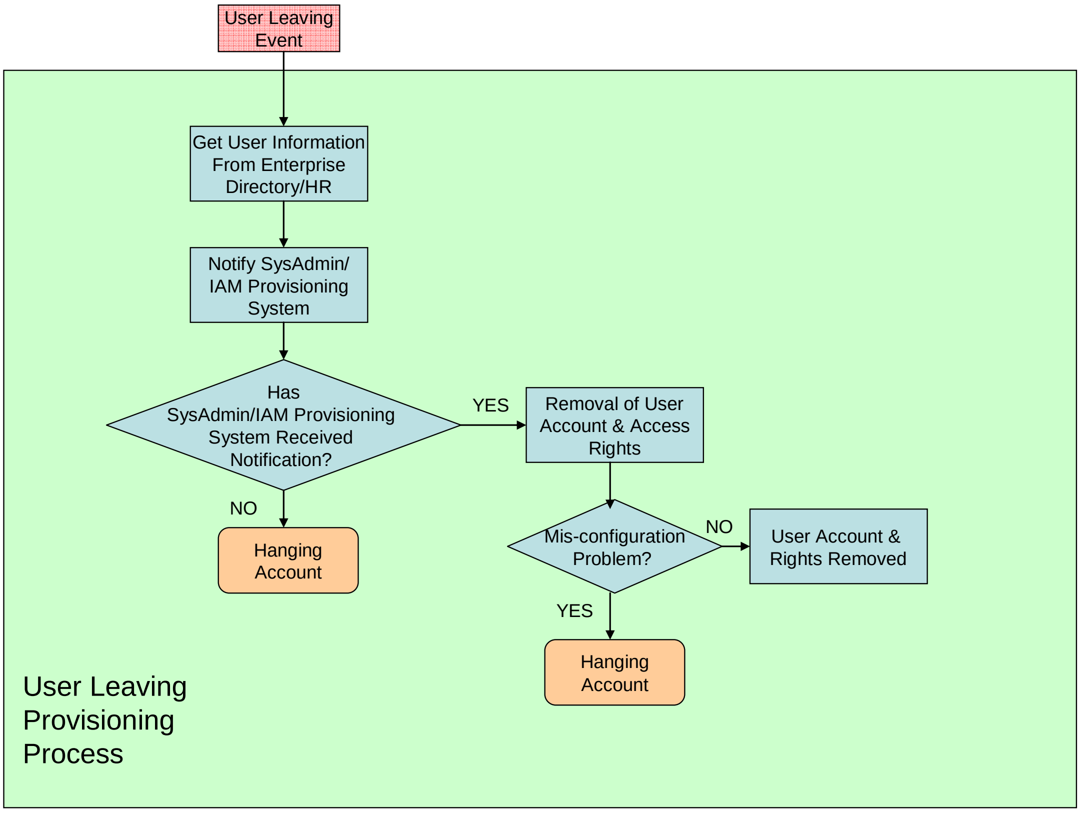

User Leaving Event
Get User Information From Enterprise Directory/HR
Notify SysAdmin/ IAM Provisioning System
Has SysAdmin/IAM Provisioning System Received Notification?
YES
NO
Removal of User Account & Access Rights
Hanging Account
Mis-configuration Problem?
NO
User Account & Rights Removed
YES
Hanging Account
User Leaving Provisioning Process

Fig. 12. User Leaving - Provisioning Process

The core aspects involved in this process include:

- A user leaves the organisation. Their access rights and accounts must be de-provisioned from one or more SAP applications;
- Information about the user and their roles are retrieved from a directory, possibly the enterprise directory (or role definitions, by HR);
- For each application involved in the provisioning process, either a *System Admin* or an *automated IAM provisioning system* (the level of automation available depends on the investments made in the provisioning area) is notified to carry out configuation steps.;
- There might be failures in the notification process. If the system admin or the IAM provisioning system does not receive this notification, the user account and/or their access rights might not be removed. This is accounted as a "hanging account". This has a negative impact on audits and can potentially enable attacks that leverage and misuse these credentials.

Figure 13 illustrates common aspects involved in the provisioning process *for a user changing their roles*:

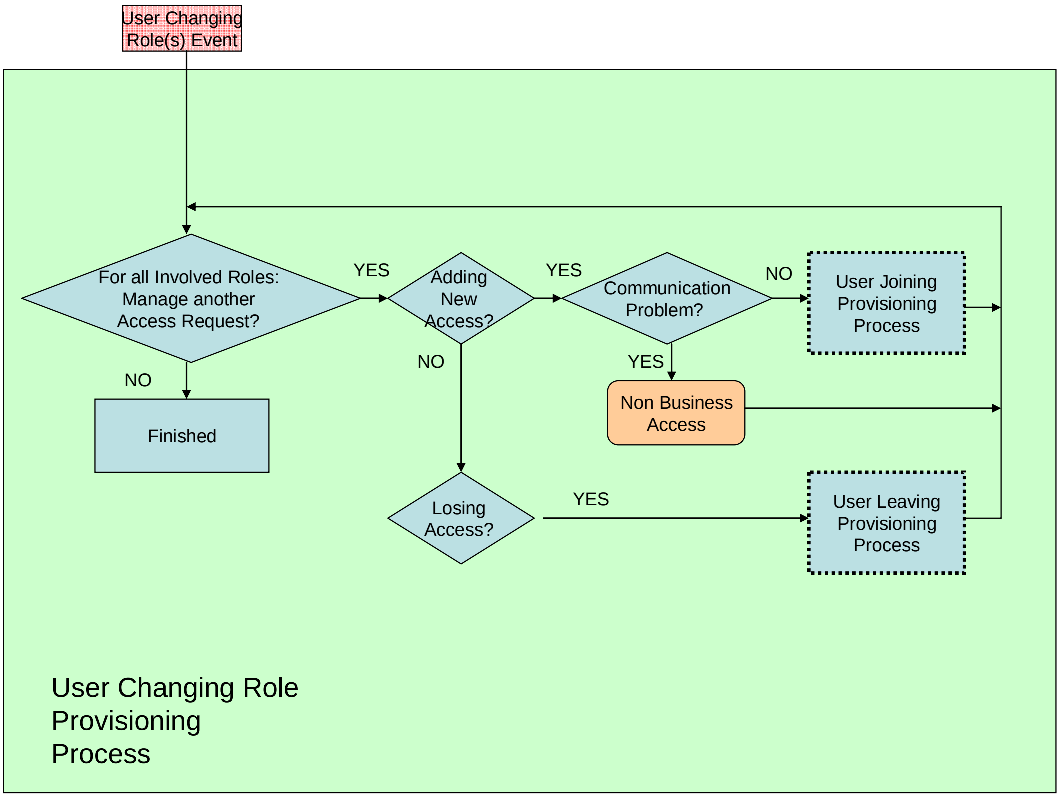

User Changing Role(s) Event
For all Involved Roles: Manage another Access Request?
YES
NO
Finished
Adding New Access?
YES
NO
Communication Problem?
NO
YES
User Joining Provisioning Process
Non Business Access
Losing Access?
YES
User Leaving Provisioning Process
User Changing Role Provisioning Process

Fig. 13. User Changing Role - Provisioning Process

The fact that a user changes their roles has been modelled as it follows:

- The user might gain new access rights for a set of applications. This is modelled similarly to the one for a new user joining the organisation – see Figure 11;
- The user might lose access rights for another set of applications. This is modelled similarly to the one for a user leaving the organisation – see Figure 12.

In this specific context, if a user gains access rights on a set of applications, there might be communication problems that prevent the provisioning process from happening. This is accounted in the model as “non business access”. Again, this will negatively affect the productivity of the user.

Another modelled core aspect is ***Compliance Management***.

Figure 14 illustrates the common aspects involved in IAM compliance checking and remediation activities. Compliance checking involves monitoring and checking for potential issues, both in terms of access control and security. In case of issues are detected, remediation activities are usually carried out, to fix them.

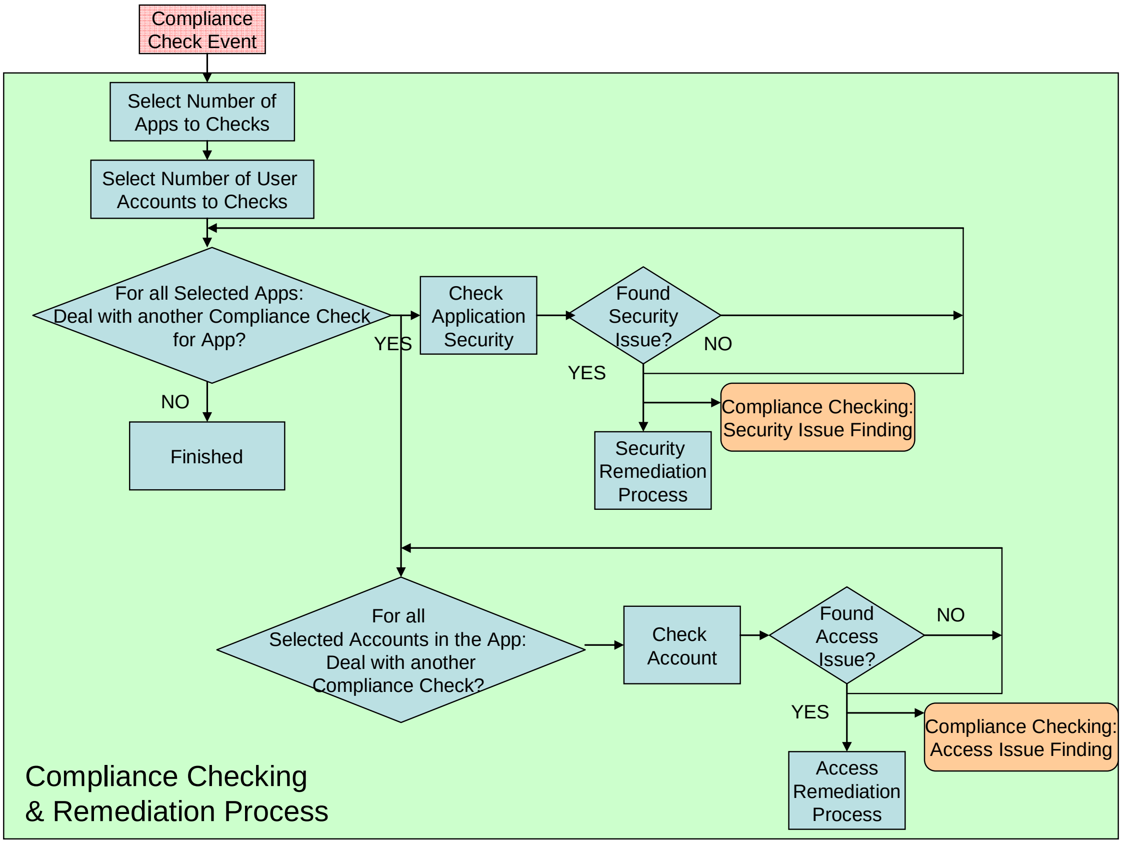

Compliance Check Event
Select Number of Apps to Checks
Select Number of User Accounts to Checks
For all Selected Apps: Deal with another Compliance Check for App?
YES
NO
Finished
Check Application Security
Found Security Issue?
NO
YES
Compliance Checking: Security Issue Finding
Security Remediation Process
For all Selected Accounts in the App: Deal with another Compliance Check?
Check Account
Found Access Issue?
NO
YES
Compliance Checking: Access Issue Finding
Access Remediation Process
Compliance Checking & Remediation Process

Fig. 14. Compliance Checking & Remediation Process

The organisation can affect the compliance checking process based on investments made in the *compliance* space. The higher the compliance investments the higher is the likelihood to spot mistakes, mis-configurations and failures and fix them. This is modelled in terms of: (1) the frequency by which these checks happens over time (dictated by the frequency of the Compliance Check Event) and (2) the number of applications and related users' accounts & rights that are checked every time.

The core aspects involved in this process include:

- Identify the number of SAP applications and the number of user accounts & access rights to be checked. This depends on the level of compliance investments;
- For each selected application, a security check is carried out. As anticipated in this section, applications are classified in three categories, from a security viewpoint: weak, medium and strong. If, the selected application has either weak or medium security, a remediation activity is carried out. This is accounted in the model in terms of security and remediation findings. The remediation time will depend on the level of compliance investments that have been made by the organisation;
- For each selected application, a number of checks are made on user accounts and access rights to identify issues. Specifically, we assumed that compliance checking will look for *"bad accesses"* and "hanging accounts" by cross checking known information about the users (i.e. roles the user is entitled too and/or the fact the user still works for the organisation). *"Non business accesses"* are not easily identifiable by these checks as no user account/access rights will available on the application and it hard to determine the full list of users that, at a point in time, should be entitled to access an application. In case of access issues are spotted a remediation activity is carried out. This is accounted in the model in terms of access and remediation findings.

Organisations often carry out auditing activities (e.g. SOX audits) to identify compliance and governance issues. Specifically, applications are checked against security common practices and user accounts (and associated user rights) are checked to verify if they reflect known organisational changes/events and/or business needs. These auditing activities are usually independent from the IT operations. The way organisations can affect the auditing outcomes is to improve their practices in terms of provisioning of user account, security enforcement and compliance checking. IAM investments play a key role. In general, the higher the investments in these areas, the higher is the likelihood to pass audits.

Figure 15 illustrated the modelled ***auditing process***:

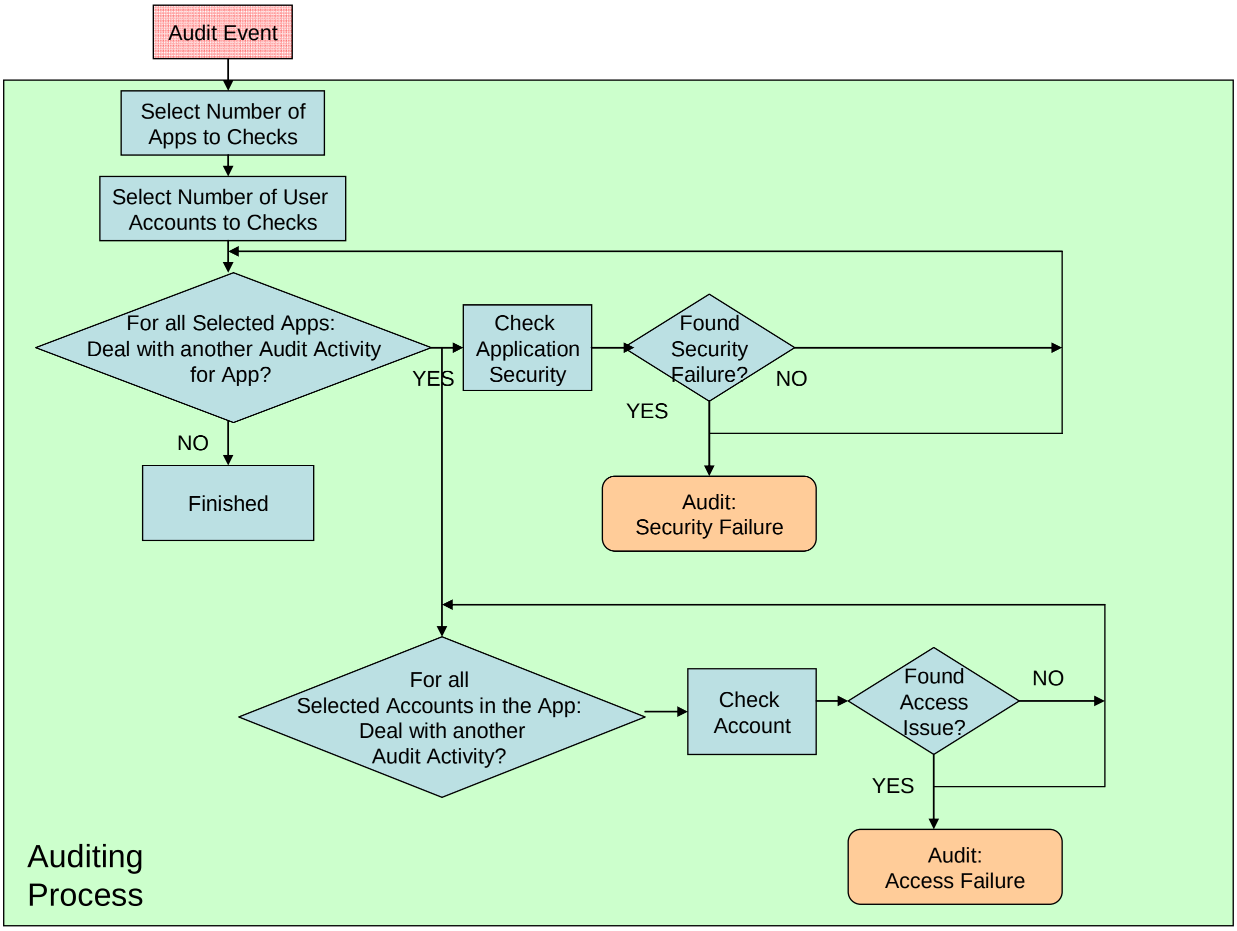

Audit Event
Select Number of Apps to Checks
Select Number of User Accounts to Checks
For all Selected Apps: Deal with another Audit Activity for App?
YES
NO
Finished
Check Application Security
Found Security Failure?
NO
YES
Audit: Security Failure
For all Selected Accounts in the App: Deal with another Audit Activity?
Check Account
Found Access Issue?
NO
YES
Audit: Access Failure
Auditing Process

Fig. 15. Auditing Process

The core aspects involved in this process include:

- Identify the number of applications and the number of user accounts & rights to be checked. This is independent on any investment made by the organisation. Decisions are made by the auditing team (depending on their resources and capabilities);
- For each selected application, an audit check is carried out. If the selected application has either weak or medium security, this is accounted in the model as a security audit failure;
- For each selected application, a number of audit checks are made on user accounts and access rights to identify issues, based on for "bad accesses", "hanging accounts" In case of access issues are spotted, this is accounted in the model as an access audit failure.

The level of security of SAP applications (and the underlying systems hosting them) depends on enforcement investments. As anticipated, security depends on: the correct deployment of control points such as firewalls, anti-virus systems, etc.; carrying on good security practices, such as software updates, patches, etc.; deploying the right IAM solutions for authentication, access control, etc. Continuous enforcement investments are required to ensure that the right level of security is preserved.

This has been modelled by assuming that the level of security of SAP applications can weaken over time, unless the right investments are in place. In the latter case, application security is periodically strengthened. Two processes have been specifically created to deal with the weakening and strengthening of applications.

The process of ***weakening of applications, from a security perspective*** (due to poor patching practices, lack of adoption of anti-viruses, etc.) explicitly models the fact that the security level of (SAP) applications (and the underlying hosting systems) is likely to degrade over time, if no reasonable investments are made in the enforcement area, to keep up with security updates and patches. Figure 16 shows the specific modelled aspects.

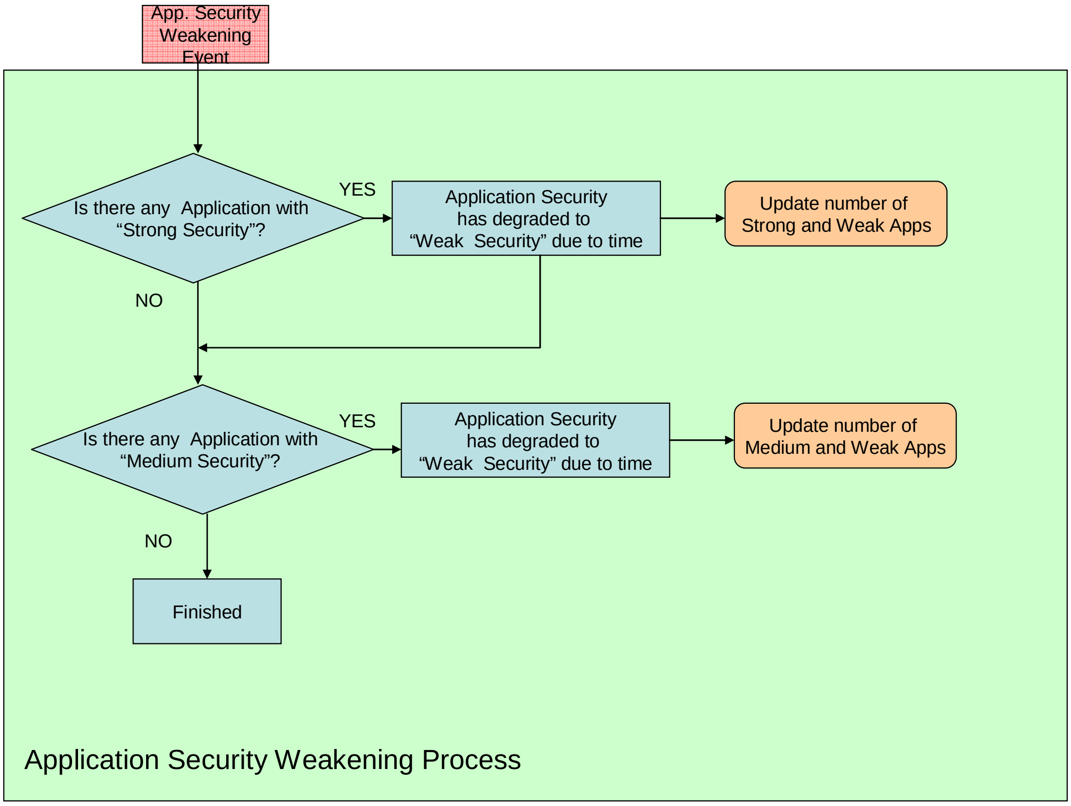

App. Security Weakening Event
Is there any Application with "Strong Security"?
YES
Application Security has degraded to "Weak Security" due to time
Update number of Strong and Weak Apps
NO
Is there any Application with "Medium Security"?
YES
Application Security has degraded to "Weak Security" due to time
Update number of Medium and Weak Apps
NO
Finished
Application Security Weakening Process

Fig. 16. Application Security Weakening Process

The core aspects involved in this process include:

- The frequency by which the security of an application is weakened. This is represented by the "Application Security Weakening event" and depends on the level of investments made in the *enforcement* area;
- The "application security weakening event" trigger the process where the security status of an application (among the overall set of managed SAP applications) is checked;
- If this security status is either *strong or medium*, the new application status will become "weak";
- This change of the application security status is reflected in the overall model status.

The model also captures the process describing the ***strengthening of the security of applications***. Investments made in the enforcement area determine the degrees by which the security level of applications can "increase" over time, by impacting the frequency of patching activities, software updates, adoption of system-level control points, etc. Figure 17 shows the specific modelled aspects.

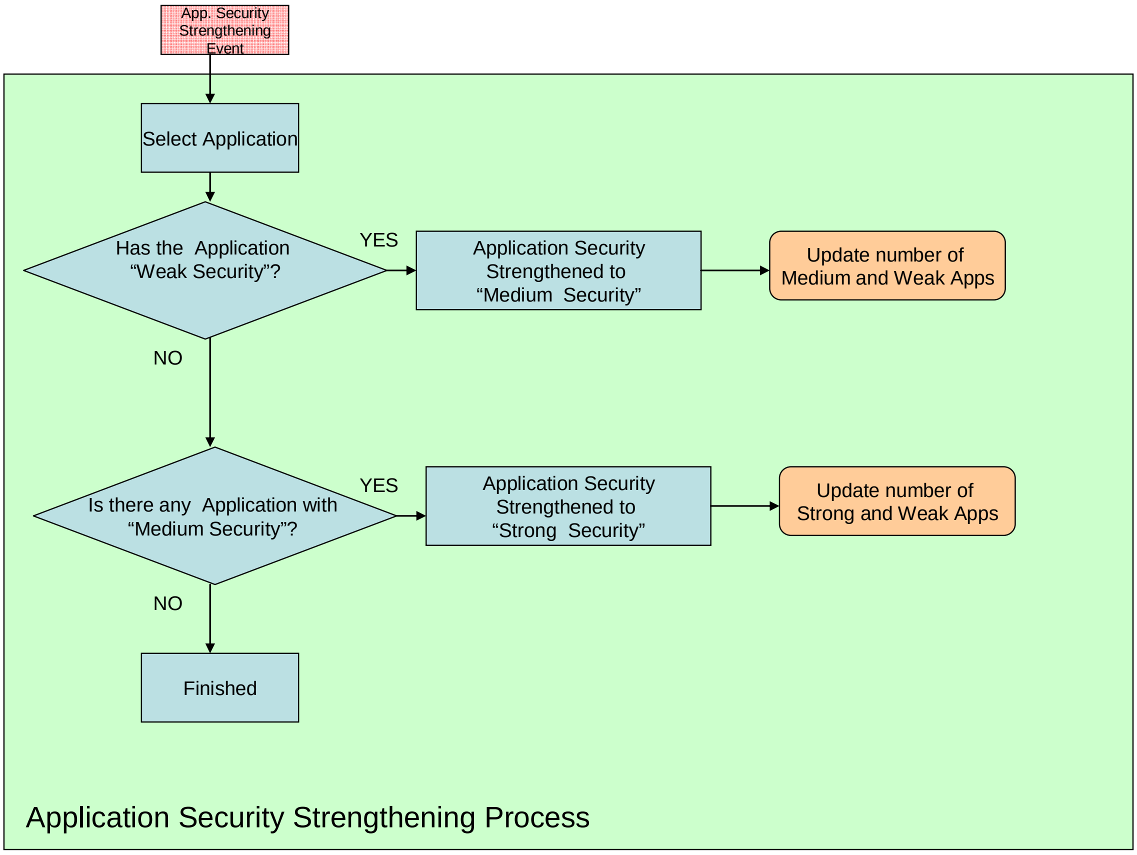

App. Security Strengthening Event
Select Application
Has the Application "Weak Security"?
YES
Application Security Strengthened to "Medium Security"
Update number of Medium and Weak Apps
NO
Is there any Application with "Medium Security"?
YES
Application Security Strengthened to "Strong Security"
Update number of Strong and Weak Apps
NO
Finished
Application Security Strengthening Process

Fig. 17. Application Security Strengthening Process

The core aspects involved in this process include:

- The frequency by which the security of an application can be strengthened. This is represented by the "Application Security Strengthening event" and depends on the level of investments made in the enforcement area;
- The "application security weakening event" triggers the process where the security status of an application (among the overall set of managed SAP applications) is checked;
- If this security status is medium, the new application status will become "strong";
- If this security status is weak, the new application status will become "medium";
- This change of the application security status is reflected in the overall model status.

As anticipated, the model keeps into account the most common types of ***threats*** (and related attacks) that an organisation might have to face: *Internal threats, External threats and Ex-worker Threats*. These threats can materialise into attacks.

The model focuses on attacks that can leverage and exploits some of the following aspects: *access issues (bad accounts, hanging accounts); application security issues (medium and weak applications).* It is important to notice that the likelihood of attacks being successful can be influenced by the organisations by making investments in the three areas of enforcement, provisioning and security. The higher the investments in enforcement the fewer applications are going to have weak or medium security. The higher the investments in provisioning and compliance, the lower are going to be the number of bad accesses and hanging accounts. The model keeps track of the successful number of attacks (incidents) that happen over time.

Various assumptions about the underlying ***threat environment*** are taken into account in the model**:**

- **Internal Threat Level**: this is a number ranging in the [1-5] range, where an higher value means a higher threat level;
- **External Threat Level**: this is a number ranging in the [1-5] range, where an higher value means a higher threat level**;**
- **Ex-worker Threat Level**: this is a number ranging in the [1-5] range, where an higher value means a higher threat level;
- **Average skill level of the attacker** to carry out successful attacks, in a [0-1] range, where 1 means high skills;
- **Intranet Protection level**: it is the level of protection of the organisation Intranet (e.g. in term of network access control, etc.), directly dependent on the investment made in the enforcement space. It is in a [0,1] range, where 1 means high protection;
- **Employee Training level**: his is a number ranging in the [1-5] range, where an higher value means a higher education level;

The model enables the exploration of different threat environments, by acting on the above parameters, for example:

- **Mild Attack Scenario**: users are basically trustworthy; there is some expectancy of fraud attempts as with any employee population; the external attack level is medium-low. People leave the organisation, but not especially with bad feeling;
- **Strong Attack Scenario**: there is a high-rate of redundancies and bad economy. Employees are disgruntled. The external attack level is high.

Figure 18 shows the specific aspects that have been modelled for ***Internal Attacks***.

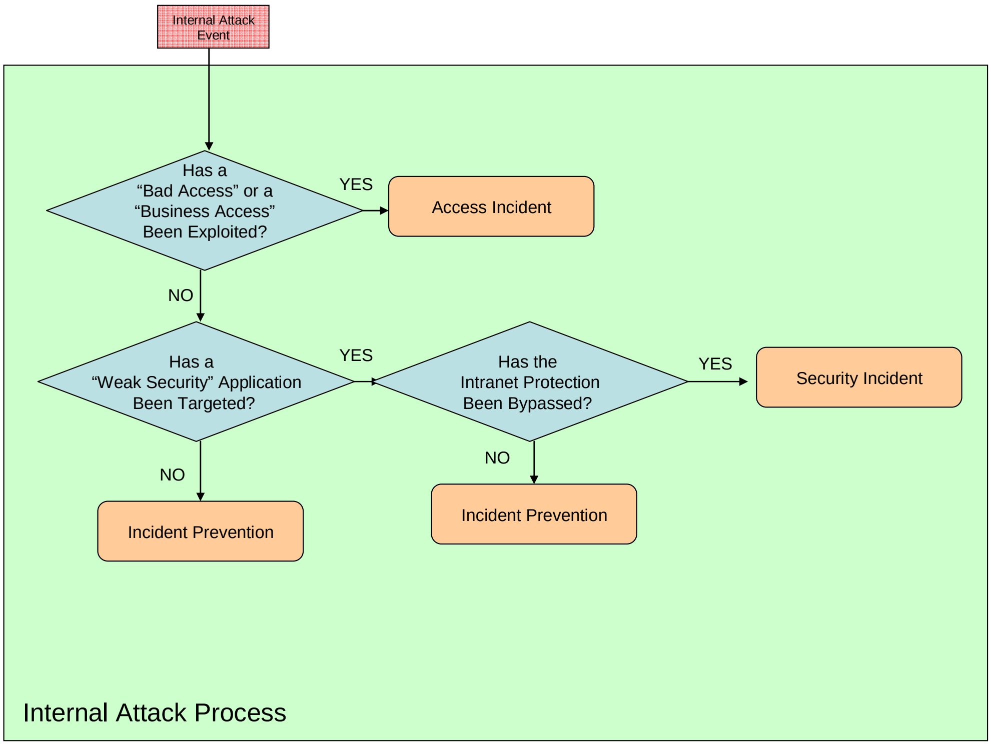

Internal Attack Event
Has a "Bad Access" or a "Business Access" Been Exploited?
YES
Access Incident
NO
Has a "Weak Security" Application Been Targeted?
YES
Has the Intranet Protection Been Bypassed?
YES
Security Incident
NO
Incident Prevention
NO
Incident Prevention
Internal Attack Process

Fig. 18. Internal Attack Process

In the model, the frequency of the "Internal Attack" events is dynamically affected by two factors. Specifically, this frequency is negatively impacted by the number of attacks that have been prevented in the past (this concurs to make the event less frequent). On the other hand, this frequency is positively impacted by the *internal threat level* and the number of s*uccessful attacks/incident*.

The core aspects involved in this process include:

- Checking if any *bad access* or *business access* has been exploited by an internal attacker. This depends on the current access status, that is affected by provisioning and compliance investment levels. In case of successful exploitation, this is accounted in the model as an *(access) incident*;
- In case of failure, the process checks if any weak security application has been targeted by attackers. If so, a check is made if this application has been exploited, due to weak intranet protection. Both aspects directly depend on enforcement investments. If case of successful attack, this is accounted in the model as an *(security) incident*;
- In case of failure of various attack attempts, this is accounted as *incident prevention*.

It is important to notice that a potential path to carry out an Internal Attack comes from exploiting or misusing a *Bad Access* or a *Business Access*. As such we might expect that the higher the provisioning investment level (and, consequently, the higher the number of business access, i.e. correctly provisioned user accounts & access rights) the higher is the number of accounts and access rights that can potentially be exploited or misused. Hence, statistically, we might expect an increase of successful internal attacks by increasing the level of investments in provisioning – all other investments being the same.

The frequency of the *Internal Attack Event* takes into account real patterns that organisations experience in terms of attacks. It increases depending on the number of successful attacks that happened in the past (i.e. the organisation is perceived as being weak, from a security perspective, from the community of attackers) whilst it decreases depending on the number of attacks that have been successfully prevented in the past. More details are available in Appendix A.

Figure 19 shows the specific aspects that have been modelled for ***Ex-workers Attacks***.

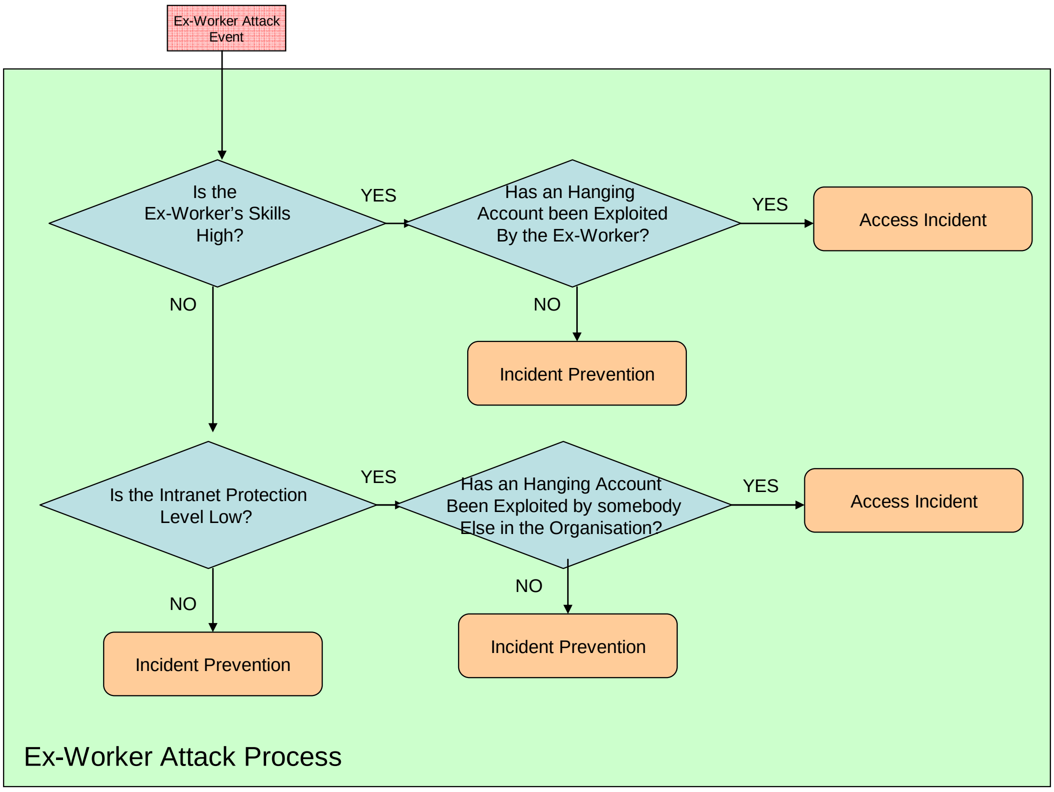

Ex-Worker Attack Event
Is the Ex-Worker's Skills High?
YES
Has an Hanging Account been Exploited By the Ex-Worker?
YES
Access Incident
NO
NO
Incident Prevention
Is the Intranet Protection Level Low?
YES
Has an Hanging Account Been Exploited by somebody Else in the Organisation?
YES
Access Incident
NO
NO
Incident Prevention
Incident Prevention
Ex-Worker Attack Process

Fig. 19. Ex-Worker Attack Process

The core aspects involved in this process include:

- Checking if an ex-worker has reasonable skills to perpetrate an attack. If so, a check is made if any related hanging account has been exploited by this worker. The number of hanging account is affected by investments made in the provisioning area. In case of successful exploitation, this is accounted in the model as an *(access) incident*;
- In case the ex-worker has no sufficient skills, an additional check is made about the level of *intranet protection*. If it is low, a check is made if any *hanging account* has been exploited in the organisation by somebody else (e.g. colleagues, outsiders, etc.). In case of success, this is accounted in the model as an *(access) incident*;
- In case of failure of various attack attempts, this is accounted in the model as *incident prevention*.

Finally, Figure 20 shows the specific modelled aspects for ***External Attacks***.

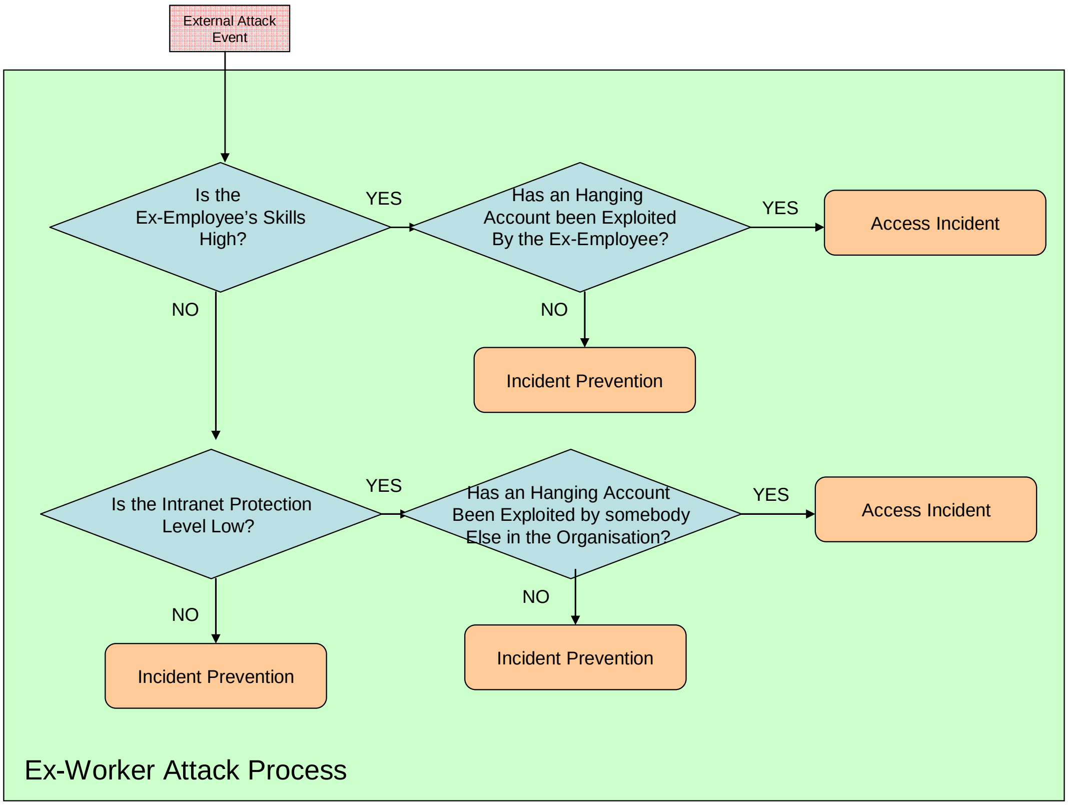

External Attack Event
Is the Ex-Employee's Skills High?
YES
Has an Hanging Account been Exploited By the Ex-Employee?
YES
Access Incident
NO
NO
Incident Prevention
Is the Intranet Protection Level Low?
YES
Has an Hanging Account Been Exploited by somebody Else in the Organisation?
YES
Access Incident
NO
NO
Incident Prevention
Incident Prevention
Ex-Worker Attack Process

Fig. 20. External Attack Process

The core aspects involved in this process include:

- Checking if the intranet protection is weak and can be bypassed. In case it is not, this is accounted in the model as *incident prevention*;
- In case of unauthorised access to the intranet, a check is made if any unauthorised access has been carried out by an ex-employee. In case of success, this is accounted in the model as an *(access) incident;*
- In case of unauthorised access to the intranet, a check is also made if any weak application has been targeted and exploited. In case of success, this is accounted in the model as an *(security) incident*.

The frequency of the *External Attack Event* takes into account real patterns that organisations experience in terms of attacks. It increases depending on the number of successful attacks that happened in the past (i.e. the organisation is perceived as being weak, from a security perspective, from the community of attackers) whilst it decreases depending on the number of attacks that have been successfully prevented in the past. More details are available in Appendix A.

All the above processes are affected by parameters that can be set in to reflect specific assumptions. These processes affect various measures which determine the status of the model.

The values of these measures, obtained from Monte Carlo simulations, eventually define the predicted outcomes of the model. Next sections provide additional information.

6.2 Model Parameters and Measures

This section provides additional details about the various parameters in the model, definition of probability distributions, measures and related proxies.

6.2.1 Parameters

The model is driven by a set of parameters, which reflects specific assumptions and define the initial status and probability distributions used in various processes. The following types of parameters have been taken into account in the model:

- **Status Initialization Parameters**;
- **Threat Environment Parameters**;
- **Event Parameters**;
- **Process Parameters**.

Each of these parameters reflects assumptions that have been made in the model in the specific case study scenario. The probability distributions and values associated to these parameters have been derived from empirical data obtained from audit logs of the organization and discussions with the decision makers and IT teams. They can be modified to reflect different assumptions and contexts.

Some of these parameters depend on probability distributions, such as:

- **Negative Exponential (negexp(x))**: this distribution is used to define the frequency of event arrivals. The parameter x is the average number of days after which an event occur
- **Point Distribution (point[(p1,v1), (p2,v2), …])**: this is a discrete probability distributions characterised by a set of potential outcomes (values Vx) and their correspondent probabilities

More details follow.

a) Status Initialization Parameters

These parameters capture the initial status of the model and reflect core assumptions in terms of IAM investments (provisioning, compliance, enforcement), number of involved SAP applications, security levels of these applications, initial status of access control rights and their classification in various categories (business access, bas access, non business access, non access, hanging account).

The table below illustrates the initial settings that have been used in an instantiation of the model (based on empirical data obtained from discussions with IAM experts and assumptions we made, based on observations).

Status Initialization Parameters	**Definition and Description**
provisioning	It defines the current investment level for provisioning, with value in the [1,5] range. The meaning of these levels has been described in section 4.
compliance	It defines the current investment level for compliance, with value in the [1,5] range. The meaning of these levels has been described in section 4.
enforcement	It defines the current investment level for enforcement, with value in the [1,5] range. The meaning of these levels has been described in section 4. ***In the current case IAM case study this parameter has value 4***
initusers	It defines the initial number of users (tracked by the model) of SAP applications. *In the model it has been set to 10.*
initleavers	It defines the initial number of users that are in the process of leaving the organisations. *In the model it has been set to 0.*
initstrongapp	It defines the initial number of (SAP) applications with "strong security". *It has been set to 15*
initmediumapp	It defines the initial number of (SAP) applications with "medium security". *It has been set to 30*
initweakapp	It defines the initial number of (SAP) applications with "weak security". *It has been set to 15*
inittotalapps	It defines the initial number of (SAP) applications. It is defined as: *initstrongapp + initmediumapp + initweakapp*. In this IAM case study we assumed there were *60 managed SAP applications* and that this number is not going to vary during the observed period of time (1 year).
initbizaccess	It defines the initial number of overall "Business Accesses" that users have on managed SAP applications. *It has been set to 20, assuming that each of the 10 users has an average access to 2 applications.*
initnonbizaccess	It defines the initial number of overall "Non Business Accesses" that users have on managed SAP applications. *It has been set to 0*
initbadaccess	It defines the initial number of overall "bad Accesses" that users have on managed SAP applications. *It has been set to 0*
initnonaccess	It defines the initial number of overall "Non Accesses" that users have on managed SAP applications. *It has been set to 580*
initotheraccess	It defines the initial number of overall "Hanging Accounts" still allocated on SAP applications, despite the owners have left or are in the process to. *It has been set to 0*

intranetprotection	It defines the initial intranet protection level. It depends on the current enforcement investment level. *It is defined as: enforcement/levelRange where levelRange is 5.*

b) Threat Environment Parameters

These parameters capture various assumptions made on the threat environment and aspects qualifying employees within an organisation. The table below illustrates the initial settings that have been used in an instantiation of the model (based on empirical data obtained from discussions with IAM experts and assumptions we made, based on observations).

Threat Environment Parameters	Definition and Description
internalthreat	It defines the current internal threat level, in a [1,5] range. *For a mild threat environment this parameter is set to 2.*
exworkerthreat	It defines the ex-worker threat level, in a [1,5] range. *For a mild threat environment this parameter is set to 2.*
externalthreat	It defines the external threat level, in a [1,5] range. *For a mild threat environment this parameter is set to 2.*
proportionskilled	It defines the proportion of employee that has the required skills to mount an attack. *For a mild threat environment this parameter is set to 2%*
usertraining	It defines the level of education of employees, in a [1,5] range. *For a mild threat environment this parameter is set to 2.*

c) Event Parameters

These parameters qualify the various events that trigger the various modelled processes. The table below illustrates the initial settings that have been used in an instantiation of the model (based on empirical data obtained from discussions with IAM experts and assumptions we made, based on observations).

Event Parameters	Definition and Description
newusertrigger	It defines the frequency of the event of a new user joining the organisation and requiring access rights on 1 or more SAP applications. It has been set to: *negexp(3.5*days)*
leavertrigger	It defines the frequency of the event of a user leaving the organisation; their access rights on 1 or more SAP applications need to be deprovisioned. It has been set to: *negexp(7*days)*
changerightstrigger	It defines the event of a user is changing roles the organisation;

	this has to be reflected on the involved SAP applications that they need to access. It has been set to: *negexp (30*days)*
generalweakeningtrigger	It defines the frequency of the event where the security of an application starts degrading, in absence of any update. It has been set to: *negexp (30*days)*
upgradeapptrigger	It defines the frequency of the event where the security of an application is upgraded. It is dependent on the current enforcement investment level, in the [1,5] range. It is defined as: *upgradeapptrigger = negexp (appUpgradeRate[enforcement level])* where: *appUpgradeRate[1] := 100*days* *appUpgradeRate[2] := 100*days/3* *appUpgradeRate[3] := 100*days/10* *appUpgradeRate[4] := 100*days/40* *appUpgradeRate[5] := 100*days/50*
cCRtrigger	It defines the frequency of the event where a compliance checking & remediation activity is carried out. It depends on the current compliance enforcement level, in the [1,5] range. It is defined as: *negexp (150*days/compliance)*
auditTrigger	It defines the frequency of the event where an audit activity is carried out. It is defined as: *negexp (180*days)*
internalthreattrigger	It defines the basic frequency of the event where an internal threat materialises. It is defined as: *negexp (20*days/internalthreat)* This frequency is affected over time, depending on the number of incidents that occurred and the one that have been prevented
exworkerthreattrigger	It defines the basic frequency of the event where an ex-worker threat materialises. It is defined as: *negexp (100*days/(exworkerthreat * exworkerthreat))*
externalthreattrigger	It defines the basic frequency of the event where an external threat materialises. It is defined as: *negexp (20*days/externalthreat)*

	This frequency changes over time, depending on the number of incidents that occurred and the ones that have been prevented.

d) Process Parameters

These parameters further qualify the processes. The table below illustrates the initial settings that have been used in an instantiation of the model (based on empirical data obtained from discussions with IAM experts and assumptions we made, based on observations).

Process Parameters	**Definition and Description**
numAppNewUser	It defines the probability that a user joining the organisation gets access to a specific number of SAP applications. It is defined as: *point [(0.4,1),(0.3,2),(0.2,3),(0.05,5),(0.04,6),(0.01,7)]* where each pair *(X,Y)* means: - X: probability - Y: number of applications
numAppLeaverUser	It defines the probability that a user leaving the organisation loses access to a specific number of SAP applications. It is defined as: *point [(0.4,1),(0.3,2),(0.2,3),(0.05,5),(0.04,6),(0.01,7)]* where each pair *(X,Y)* means: - X: probability - Y: number of applications The actual type of change (gaining or losing access) is defined by the following point distributions: *point [(0.5,addACCESS), (0.5,loseACCESS)]*
numAppChangeRoleUser	It defines the probability that a user changing roles gains or loses access to a specific number of SAP applications. It is defined as: *point [(0.4,1),(0.3,2),(0.2,3),(0.05,5),(0.04,6),(0.01,7)]* where each pair *(X,Y)* means: - X: probability - Y: number of applications
passiveManagerApprovalRate	It defines the probability of a successful passive manager approval, for the “User Joining Provisioning” process. It is dependent on the current provisioning investment level, in the [1,5] range. It is defined as: *passiveManagerApprovalRate[1] := 60/100* *passiveManagerApprovalRate[2] := 65/100* *passiveManagerApprovalRate[3] := 78/100* *passiveManagerApprovalRate[4] := 98/100* *passiveManagerApprovalRate[5] := 9999/10000*
activeManagerApprovalRate	It defines the probability of a successful active manager

	approval, for the "User Joining Provisioning" process. It is dependent on the current provisioning investment level, in the [1,5] range. It is defined as: *activeManagerApprovalRate[1] := 50/100* *activeManagerApprovalRate[2] := 55/100* *activeManagerApprovalRate[3] := 85/100* *activeManagerApprovalRate[4] := 99/100* *activeManagerApprovalRate[5] := 9999/10000*
sysAdminFailureRate	It defines the probability of a system admin (or IAM system used in case of automation) failure, for the "User Joining Provisioning", "User Leaving Provisioning" and "User Changing Role Provisioning" processes. It is dependent on the current provisioning investment level, in the [1,5] range. It is defined as: *sysAdminFailureRate[1] := 1/50* *sysAdminFailureRate[2] := 1/150* *sysAdminFailureRate[3] := 1/250* *sysAdminFailureRate[4] := 1/800* *sysAdminFailureRate[5] := 1/1000*
sysAdminNoConfigRate	It defines the probability of a system admin (or IAM system used in case of automation) not carrying out the user account configuration – to grant access rights, for the "User Joining Provisioning" and "User Changing Role Provisioning" processes. It is dependent on the current provisioning investment level, in the [1,5] range. It is defined as: *sysAdminNoConfigRate[1] := 1/70* *sysAdminNoConfigRate[2] := 1/180* *sysAdminNoConfigRate[3] := 1/300* *sysAdminNoConfigRate[4] := 1/900* *sysAdminNoConfigRate[5] := 1/1100*
bypassProvisioningApprovalRate	It defines the probability of a user bypassing the approval process (in case of delays or issues), for the "User Joining Provisioning" and "User Changing Role Provisioning" processes. It is dependent on the current provisioning investment level, in the [1,5] range. It is defined as: *bypassProvisioningApprovalRate[1] := 1/50* *bypassProvisioningApprovalRate[2] := 1/100* *bypassProvisioningApprovalRate[3] := 1/500* *bypassProvisioningApprovalRate[4] := 1/1000* *bypassProvisioningApprovalRate[5] := 1/1200*
sysAdminCommunicationFailureRate	It defines the probability of a system admin (or IAM system used in case of automation) of not receiving any communication to remove a user's access rights, for the "User Leaving Provisioning" and "User Changing Role

	Provisioning" processes. It is dependent on the current provisioning investment level, in the [1,5] range. It is defined as: *sysAdminCommunicationFailureRate[1] := 1/50* *sysAdminCommunicationFailureRate[2] := 1/120* *sysAdminCommunicationFailureRate[3] := 1/350* *sysAdminCommunicationFailureRate[4] := 1/900* *sysAdminCommunicationFailureRate[5] := 1/1000*
communicationFailureRate	It defines the probability of a generic communication problem to remove a user's access rights, for the "User Changing Role Provisioning" process. This is due to possible faults in sending approval requests to the involved managers. It is dependent on the current provisioning investment level, in the [1,5] range. It is defined as: *communicationFailureRate[1] := 1/75* *communicationFailureRate[2] := 1/180* *communicationFailureRate[3] := 1/750* *communicationFailureRate[4] := 1/1200* *communicationFailureRate[5] := 1/1500*
appSamplingRatio	It defines the ratio of number of applications that are checked during a compliance checking and remediation activity. It is dependent on the current compliance investment level, in the [1,5] range. It is defined as: *1/(1+ inittotalapps - ((inittotalapps / highLevelValue)*compliance))* where *highLevelValue = 5*
numUserAccountsChecksPerApp	It defines the number of user accounts that are checked (per application) during a compliance checking and remediation activity. It is dependent on the current compliance investment level, in the [1,5] range. It is defined as: *1/(1+(levelRange-compliance)^2)* where *levelValue = 5*
applicationSamplingNumberAUDIT	It defines the number of applications that are checked during an audit activity. It is defined as: *round(inittotalapps/10)*
numAccountChecksPerAppAUDIT	It defines the ratio of user accounts that are checked (per application) during an audit activity. It is defined as: *1/10*

6.2.2 Measures and Proxies

The model keeps track of a few measures which can be modified overtime by the involved processes and affect their behaviours. The following table describes a few core ones:

Measures	Definition and Description
bizaccess	It is the number of overall "Business Accesses" that users have on managed SAP applications.
nonbizaccess	It is the number of overall "Non Business Accesses" that users have on managed SAP applications.
badaccess	It is the number of overall "bad Accesses" that users have on managed SAP applications.
nonaccess	It is the number of overall "Non Accesses" that users have on managed SAP applications.
otheraccess	It is the number of overall "Hanging Accounts" still allocated on SAP applications, despite the owners have left or are in the process to.
Productivity (PROXY)	It is the overall productivity, in terms of the "ratio/percentage of all user accounts that the organisation would have liked to have been provisioned": *(bizaccess + badaccess)/ (bizaccess+nonbizaccess+badaccess)* It is important to notice that "Bad Access" potentially enhances productivity (as long as the required access rights are granted) as well as it can fuel threats.
Totalincidentcount (PROXY)	It is the overall number of incidents that materialise, as an effect of Internal, Ex-worker and External threats.
Totalincidentprevention	It is the overall number of incidents that have been prevented, as an effect of Internal, Ex-worker and External threats.
auditComplianceViolationAccess (PROXY)	It is the overall number of compliance failures, due to access issues, during auditing sessions
auditComplianceViolationSecurity	It is the overall number of compliance failures, due to application security issues, during auditing sessions

A few measures in the model have been used as ***proxies*** (estimators) for utility function components, i.e. for strategic aspects of relevance for decision makers. The following table provide additional information:

Utility Function Component – Strategic Aspect of Relevance for Decision Maker	Proxy
Productivity	**Productivity**

Security Risks	**TotalIncidentCount**
Compliance	**auditComplianceViolationAccess**

Values of these measures are determined by means of Monte Carlo simulations and subsequently mapped against the strategic preferences of decision makers, to identify the most suitable investment options. Section 6.3 discusses the results obtained from various experiments and simulations. Section 7 discusses the mapping process.

6.3 Simulations and Experimental Results

Monte Carlo simulations have been carried out for a simulated timeframe of 1 year.

All the potential combinations of IAM investment options in the space of ***provisioning*** and ***compliance*** (with a constant ***enforcement*** investment level = 4) have been explored. As the investment levels in these two areas could vary in the [1-5] range, this has identified 25 different options**.** For each of these combinations, the model has been run 100 times to get statistically relevant results.

The model has been initialised with a population of 60 SAP applications and a minimal set of existing users (10) and related access rights. This is meant to specifically explore the impact (in terms of security risks, productivity and compliance) of dealing with new users, users changing roles and users leaving the organisation.

Average values have been generated for all the measures. Figures 21, 22 and 23 illustrate how the average values of the *proxy measures* for *productivity, security risks* (i.e., total security incidents) *and compliance* (i.e., audit access failures) vary, depending of the different investment choices. Details follow.

In terms of **Productivity**, the simulation outcomes have been summarised in the following table:

Productivity	Provisioning Investment Level				
Compliance Investment Level	1	2	3	4	5
1	0.324411541	0.370473059	0.667380209	0.96893351	0.999111122
2	0.318294925	0.371447009	0.674128802	0.97417639	0.998537065
3	0.310063746	0.365708694	0.669115194	0.968770634	0.999019907
4	0.305131458	0.366758737	0.665784294	0.970957411	0.998715791
5	0.307169272	0.371907063	0.663422515	0.97152686	0.998568125

Figure 21 provides the graphical rendering of the above table:

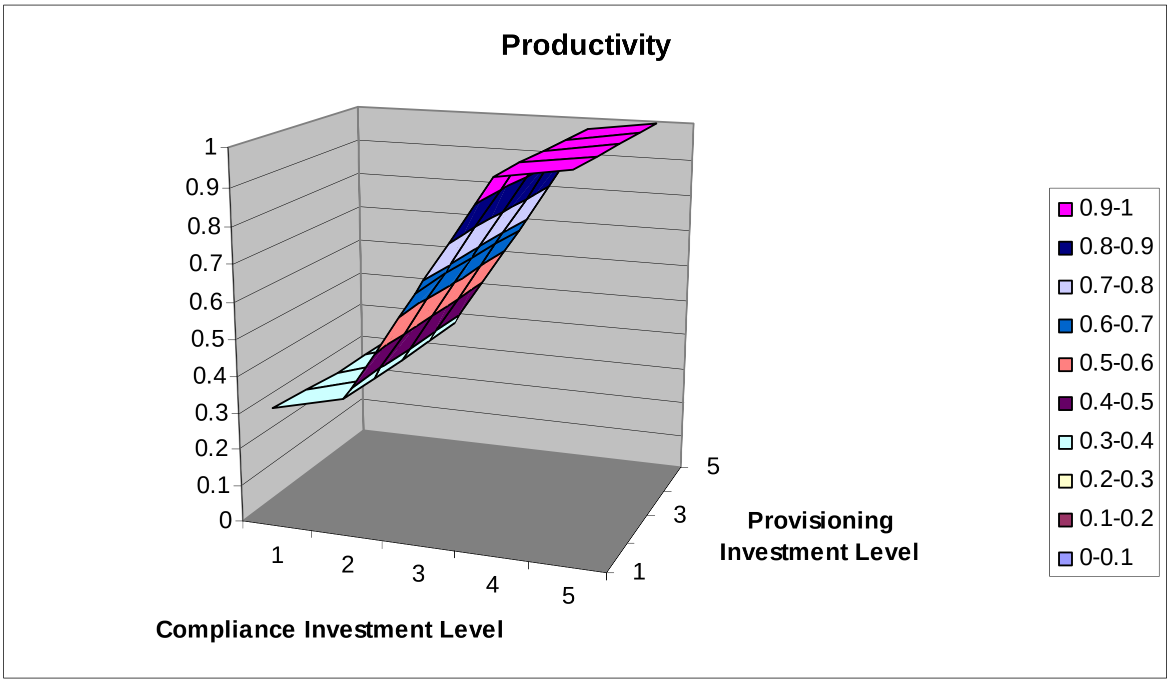


Fig. 21. Productivity outcomes for all combinations of provisioning and compliance investments – observed over 1 year period time

As described in Section 6.2, *productivity* is defined as "ratio/percentage of all user accounts that the organisation would have liked to have been provisioned" and it is calculated in the model as:

$$\mathit{Productivity} = (\mathit{bizaccess} + \mathit{badaccess}) / (\mathit{bizaccess}+\mathit{nonbizaccess}+\mathit{badaccess})$$

These results shows that *productivity* increases almost 30% for each *provisioning* investment level in the [2-4] range and saturates to almost 100% with the *provisioning investment level = 5*. This reflects the fact that the number of *"NoBizAccesses"* substantially drops with the increase of this investment.

Compliance investments have little impact on productivity as they do not affect this factor.

In terms of **Audit Access Failures**, the simulation outcomes have been summarised in the following table:

Audit Access Failures (auditComplianceViolationAccess)	Provisioning Investment Level				
Compliance Investment Level	1	2	3	4	5
1	5.96	2.11	0.64	0.21	0.09
2	4.44	1.81	0.54	0.07	0.2
3	2.79	1.81	0.39	0.1	0.101010101
4	1.909090909	0.48	0.11	0.05	0.04
5	2.09	0.48	0.1	0.05	0.04

Figure 22 provides the graphical rendering of the above table:

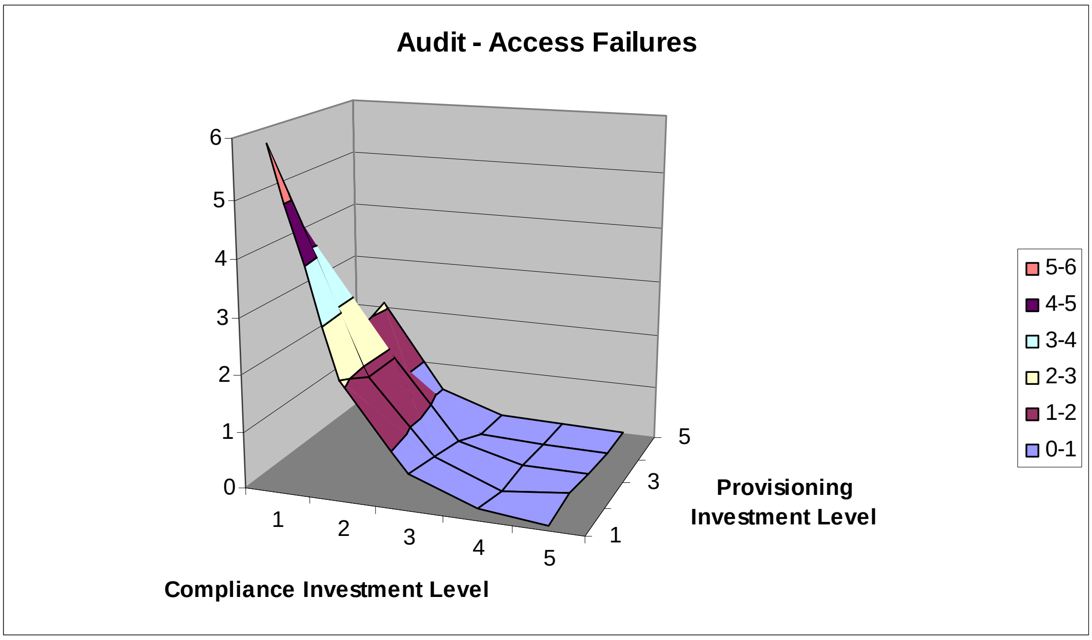


Fig. 22. Total Audit Access Failure outcomes for all combinations of provisioning and compliance investments – observed over 1 year period time

By increasing the investments in compliance or provisioning the number of *audit failures* (due to identifying access issues) decreases.

Specifically, by increasing the investments in *provisioning*, the numbers of *bad accesses* and *hanging account* are reduced, because of better practices and automation and, as a consequence, the number of *audit failures* is reduced; by increasing the investments in compliance, audit failures are reduced too, because of the increased effort in compliance checking and remediation. So, multiple investment trade-offs are potentially possible to deal with *audit failures*, depending on the decision maker's preferences in this space.

In terms of **Total Security Incidents**, the simulation outcomes have been summarised in the following table:

Total Security Incidents (totalIncidentscount)	Provisioning Investment Level				
Compliance Investment Level	1	2	3	4	5
1	2.85	2.17	1.45	1.29	1.44
2	2.49	1.98	1.2	1.19	1.36
3	2.28	1.67	1.49	1.51	1.282828283
4	1.808080808	1.31	1	1.29	1.39
5	1.39	0.92	0.75	0.91	0.97

Figure 23 provides the graphical rendering of the above table:

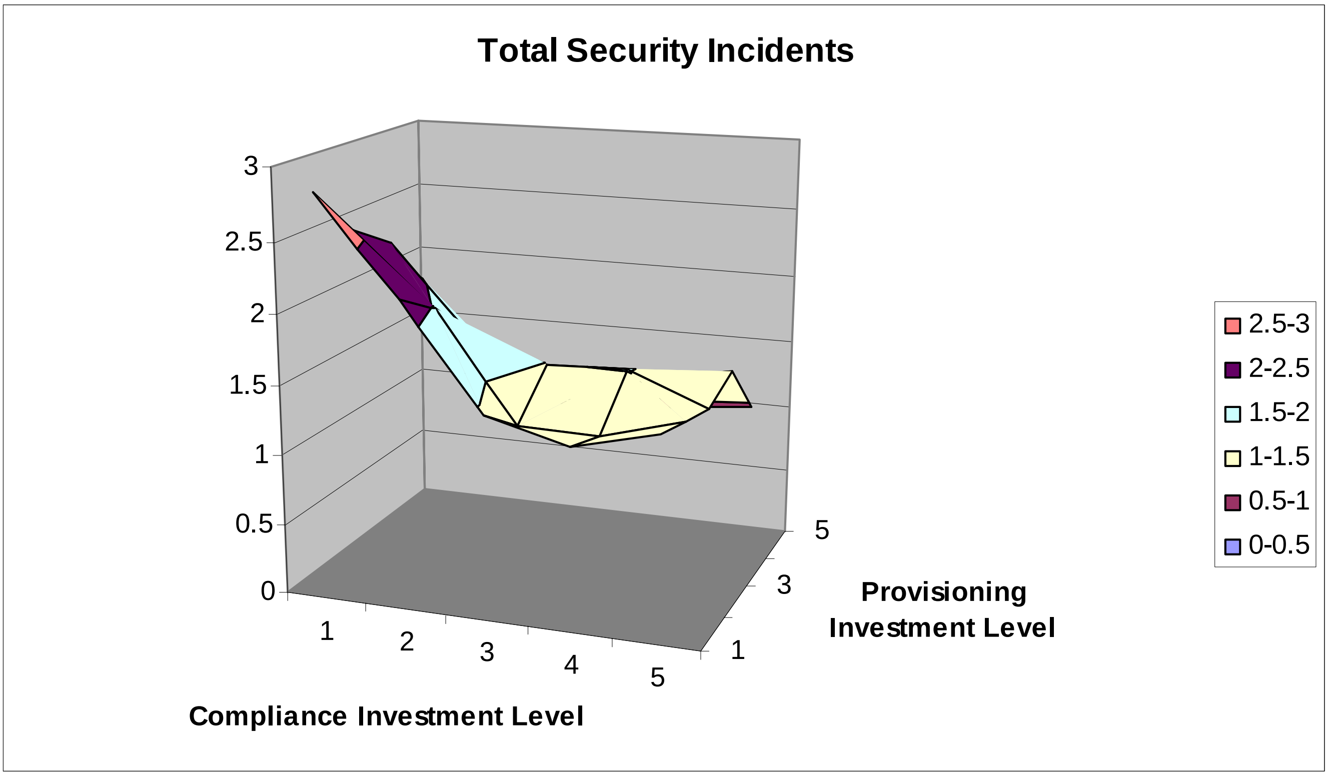


Fig. 23. Total Security Incident outcomes for all combinations of provisioning and compliance investments – observed over 1 year period time

This figure shows a relatively low number of yearly security incidents: this reflects the fact that the enforcement investment level is 4. Additional investments in *provisioning* and *compliance* have, in general, a positive effect in further reducing the number of these incidents.

The model that produced these outcomes is the results of various refinement steps driven by reality checks and discussions with the decision maker and the other involved security & IAM experts. The predictions we obtained have been validated as feasible and realistic.

The next section, illustrates how these predicted outcomes have been compared against the preferences elicited from the decision maker, to identify suitable investment choices.

7. Mapping Predicted Outcomes against Decision Makers' Preferences

This step aims at identifying the most suitable IAM investment options - that is, the most suitable *provisioning and compliance* investment levels - by mapping the predicted outcomes against the decision maker's preferences.

The data (predicted outcomes) shown in Figures 21, 22 and 23 (and in the associated tables) can be rearranged and displayed in the same way as for the preference elicitation results, shown in Figures 5, 6 and 7, to enable comparisons.

Specifically, the following table and Figure 24 show how the predicted average values of *Security Risks* and *Productivity* vary, for each combination of compliance and provisioning investment levels:

Compliance Investment Level	Provisioning Investment Level	Security Risks (totalIncidentCount)	Productivity (productivity)
1	1	2.85	0.324412
2	1	2.49	0.318295
3	1	2.28	0.310064
4	1	1.808081	0.305131
5	1	1.39	0.307169
1	2	2.17	0.370473
2	2	1.98	0.371447
3	2	1.67	0.365709
4	2	1.31	0.366759
5	2	0.92	0.371907
1	3	1.45	0.66738
2	3	1.2	0.674129
3	3	1.49	0.669115
4	3	1	0.665784
5	3	0.75	0.663423
1	4	1.29	0.968934
2	4	1.19	0.974176
3	4	1.51	0.968771
4	4	1.29	0.970957
5	4	0.91	0.971527
1	5	1.44	0.999111
2	5	1.36	0.998537
3	5	1.282828	0.99902
4	5	1.39	0.998716
5	5	0.97	0.998568

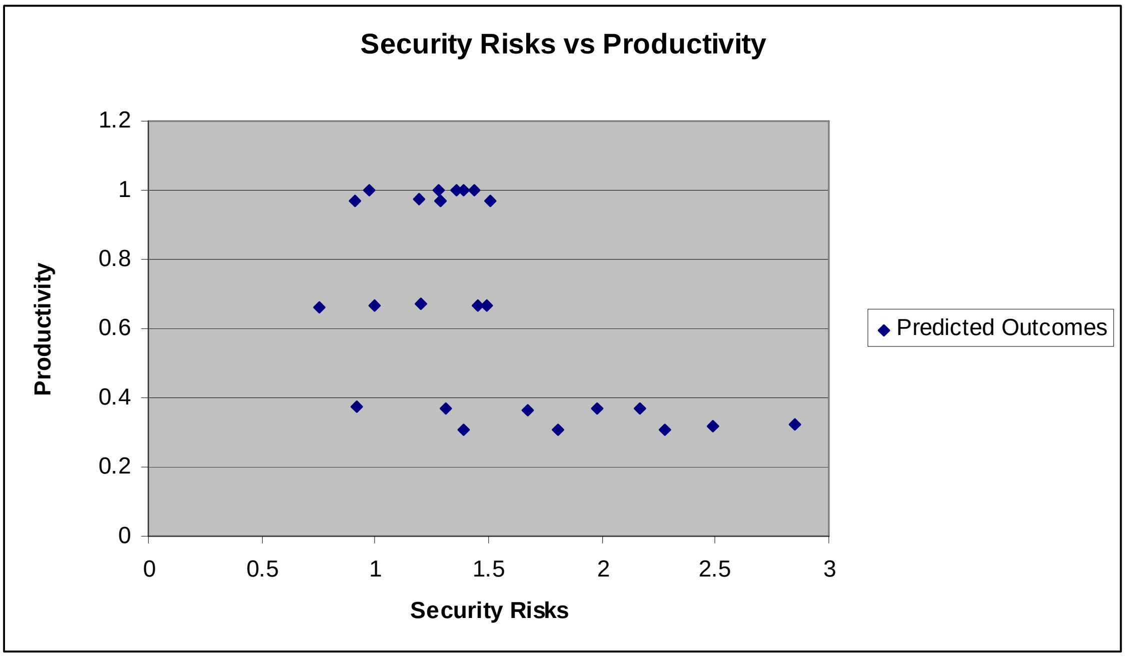


Fig. 24. Predicted Outcomes – Security Risks vs Productivity for all combinations of investment levels

The following table and Figure 25 show how the predicted average values of *Productivity* and *Compliance* vary, for each combination of compliance and provisioning investment levels:

Compliance Investment Level	Provisioning Investment Level	Productivity (productivity)	Compliance (auditComplianceViolationAccess)
1	1	0.324412	5.96
2	1	0.318295	4.44
3	1	0.310064	2.79
4	1	0.305131	1.909091
5	1	0.307169	2.09
1	2	0.370473	2.11
2	2	0.371447	1.81
3	2	0.365709	1.81
4	2	0.366759	0.48
5	2	0.371907	0.48
1	3	0.66738	0.64
2	3	0.674129	0.54
3	3	0.669115	0.39
4	3	0.665784	0.11
5	3	0.663423	0.1
1	4	0.968934	0.21
2	4	0.974176	0.07
3	4	0.968771	0.1
4	4	0.970957	0.05
5	4	0.971527	0.05
1	5	0.999111	0.09
2	5	0.998537	0.2
3	5	0.99902	0.10101
4	5	0.998716	0.04
5	5	0.998568	0.04

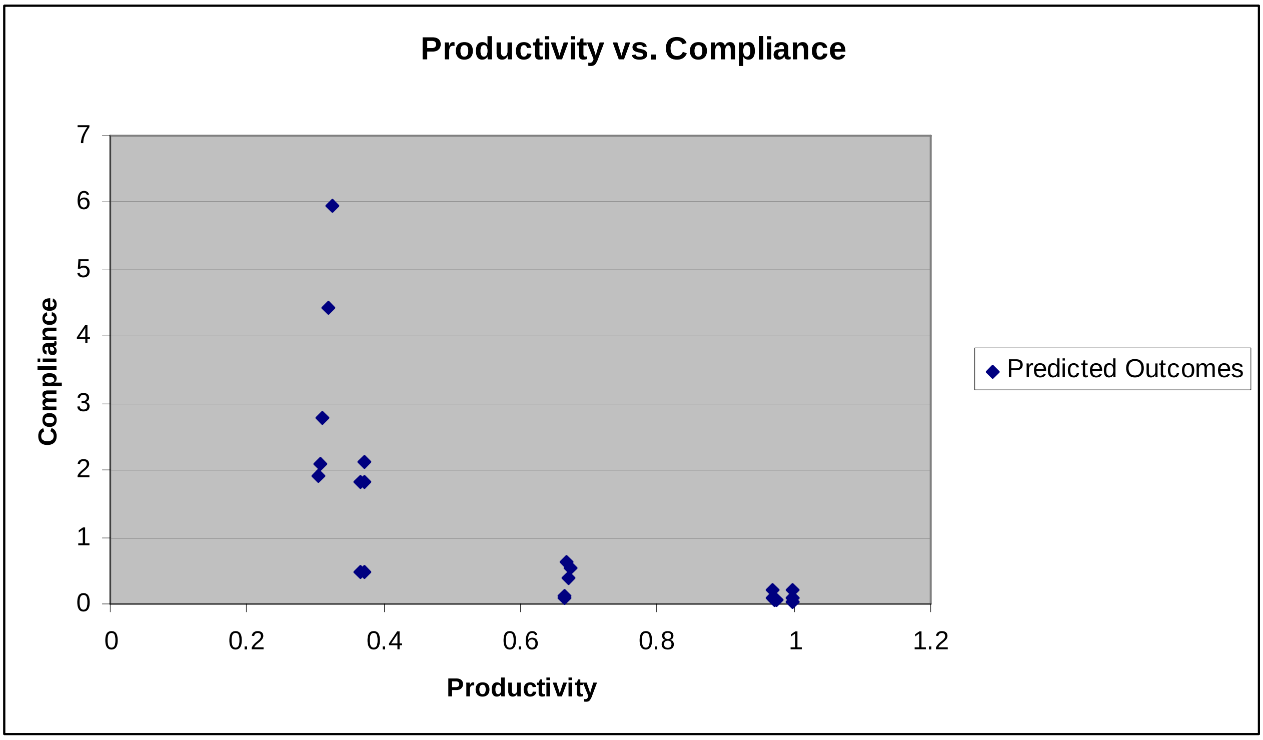


Fig. 25. Predicted Outcomes –Productivity vs Compliance (violations) for all combinations of investment levels

The following table and Figure 26 show how the predicted average values of *Security Risks* and *Compliance* vary, for each combination of compliance and provisioning investment levels:

Compliance Investment Level	Provisioning Investment Level	Security Risks (totalIncidentCount)	Compliance (auditComplianceViolationAccess)
1	1	2.85	5.96
2	1	2.49	4.44
3	1	2.28	2.79
4	1	1.808081	1.909091
5	1	1.39	2.09
1	2	2.17	2.11
2	2	1.98	1.81
3	2	1.67	1.81
4	2	1.31	0.48
5	2	0.92	0.48
1	3	1.45	0.64
2	3	1.2	0.54
3	3	1.49	0.39
4	3	1	0.11
5	3	0.75	0.1
1	4	1.29	0.21
2	4	1.19	0.07
3	4	1.51	0.1

4	4	1.29	0.05
5	4	0.91	0.05
1	5	1.44	0.09
2	5	1.36	0.2
3	5	1.282828	0.10101
4	5	1.39	0.04
5	5	0.97	0.04

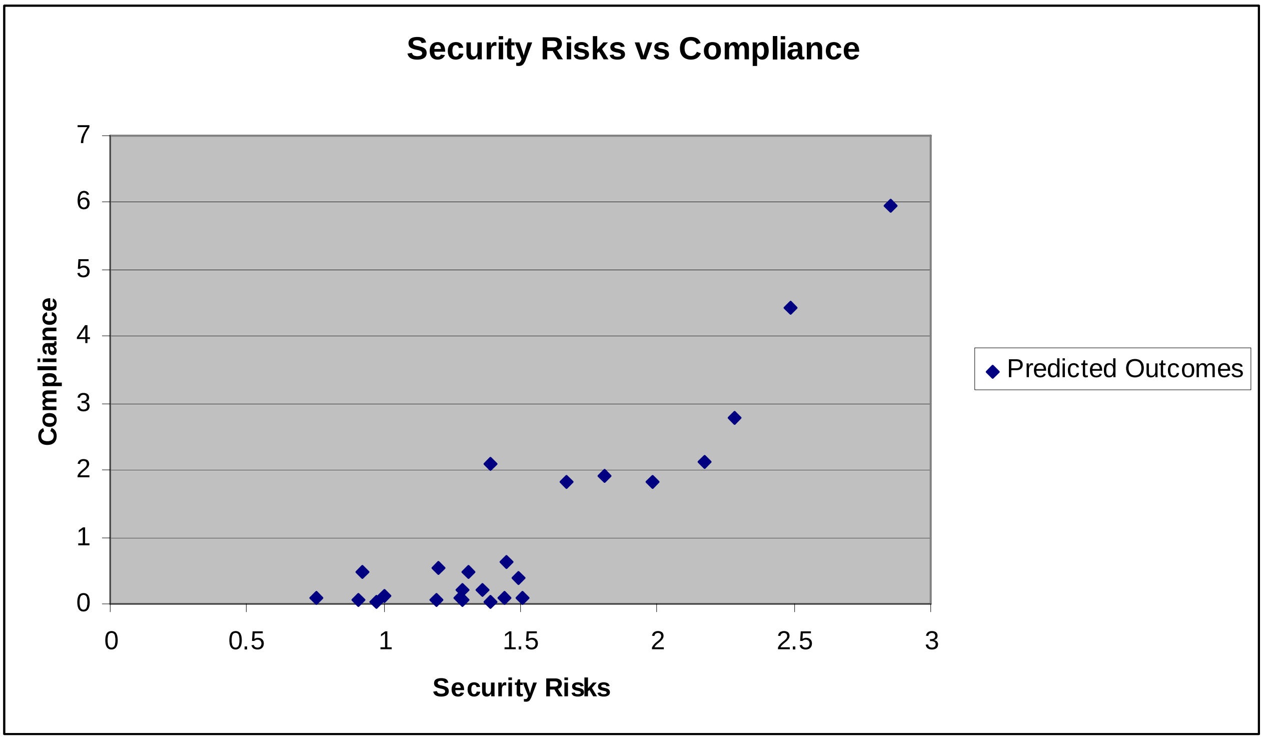


Fig. 26. Predicted Outcomes –Security Risks vs Compliance (violations) for all combinations of investment levels

It is important to notice that each point (pair of outcome values) shown in Figures 24, 25 and 26 is determined (and can be labelled with) by the *compliance and provisioning* investment levels necessary to achieve the associated values.

The predicted outcomes shown in Figures 24, 25 and 26 can now be directly mapped against the strategic preferences elicited from the decision maker shown in Figures 5, 6 and 7 to identify which investments are required to ensure that the decision maker obtains their preferred choices.

Figures 27, 28 and 29 provide a high-level mapping of this information: predicted outcomes are compared against the elicited preferences – which are classified according to decision makers' priorities.

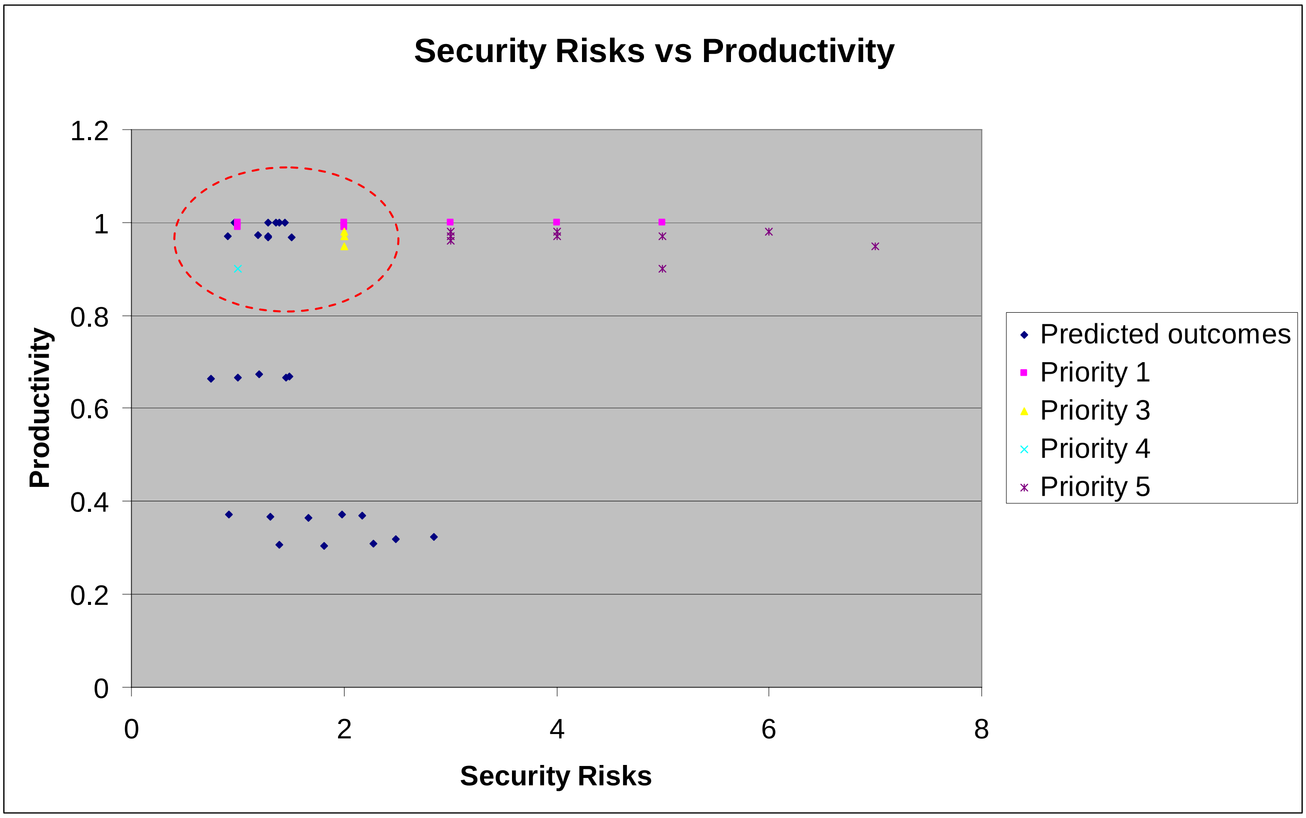


Fig. 27. Comparing Predicted Outcomes against Strategic Preferences (ordered by Priorities) – Security Risks vs Productivity

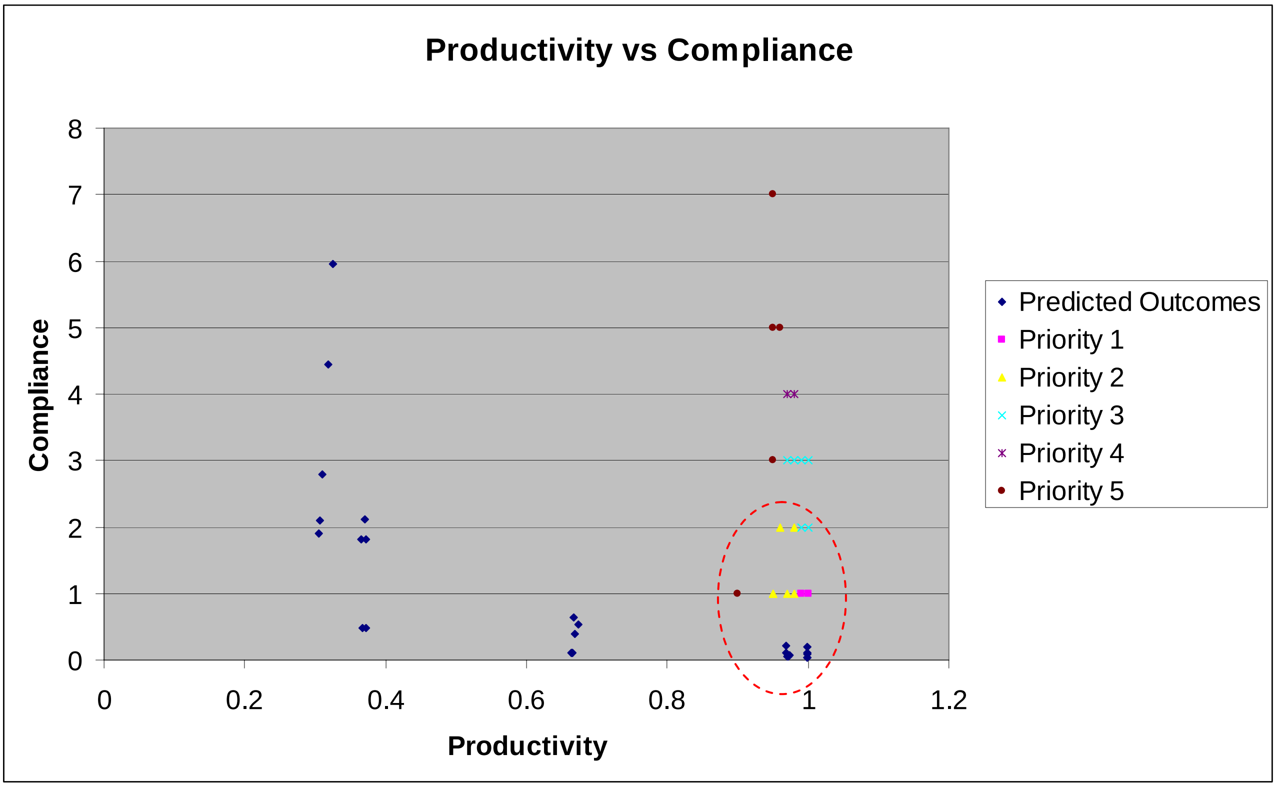


Fig. 28. Comparing Predicted Outcomes against Strategic Preferences (ordered by Priorities) – Productivity vs Compliance

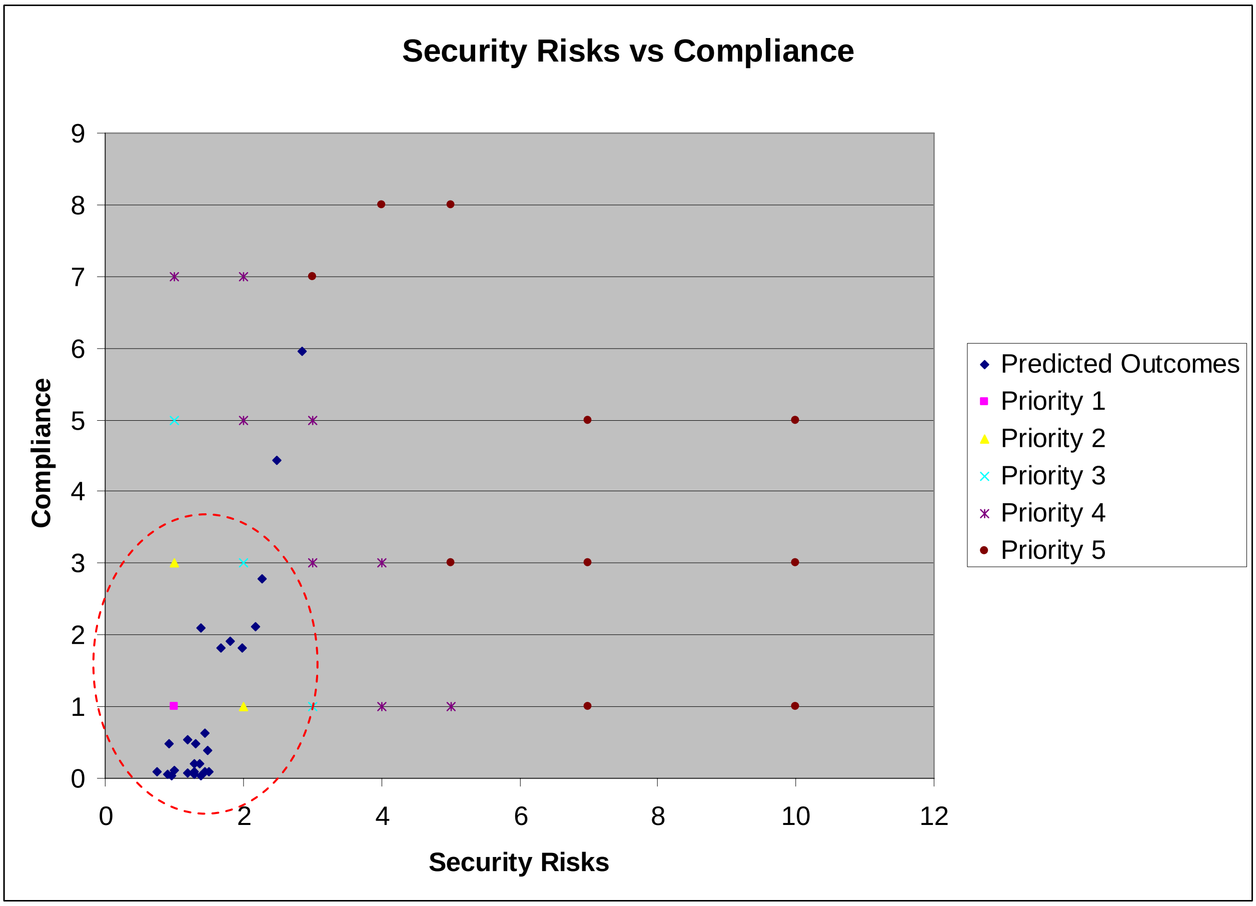


Fig. 29. Comparing Predicted Outcomes against Strategic Preferences (ordered by Priorities) – Compliance vs Security Risks

Figures 27, 28 and 29 highlight where the most significant predicted outcomes lay i.e. the ones matching the top priority preferences expressed by decision makers.

By zooming on these highlighted areas, Figures 30, 31 and 32 show the result of mapping the predicted outcomes against *the* <u>*decision makers' top priority preferences*</u> *(i.e. priorities 1, 2/3)*. Each point that represents a pair of predicted outcomes has been labeled with the associated compliance and provisioning levels.

Specifically, Figure 30 zooms on the highlighted area in Figure 27:

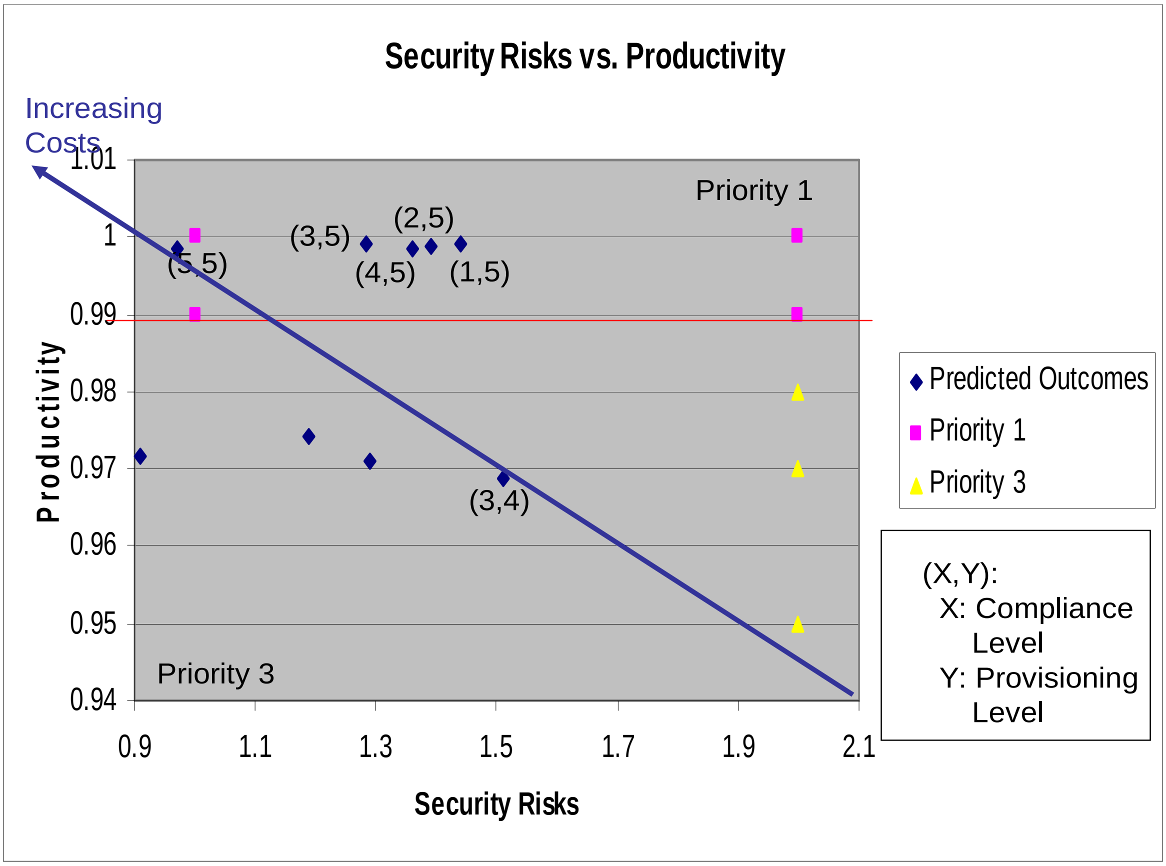


Fig.30. Zooming - Comparing Predicted Outcomes against Strategic Preferences (ordered by Priorities) – Security Risks vs Productivity

This figure shows that, in order to achieve the decision makers' Priority 1 preferences, it is necessary to have a *Provisioning Investment Level* = 5.

In this context, any *Compliance Investment Level*, in the [1-5] range is suitable, to achieve these results. Instead, the most likely combination of investments to achieve the decision makers' preferences labelled as Priority 3, is the following: *Provisioning Investment Level* = 4 and *Compliance Investment Level* = 3.

Figure 31 zooms on the highlighted area in Figure 28:

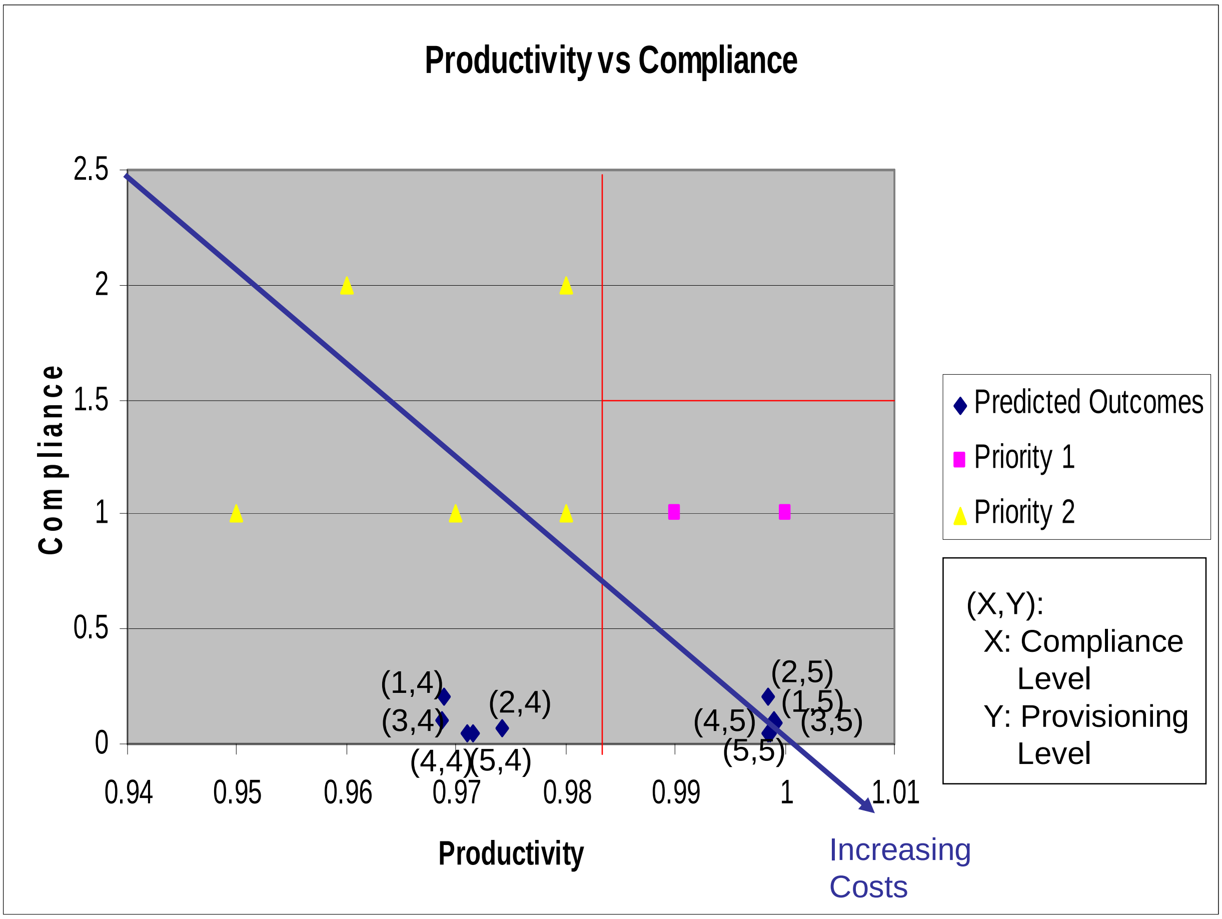


Fig. 31. Zooming - Comparing Predicted Outcomes against Strategic Preferences (ordered by Priorities) – Compliance vs Productivity

This figure shows that to achieve Priority 1's preferences, it is required to have a *Provisioning Investment Level* = 5.

Also in this context, very little difference makes the compliance investment level because the high level of provisioning investment already minimise the occurrence of potential failures and faults.

Again, this is achieved with high investment costs. Instead, Priority 2's preferences can be achieved with a *Provisioning Investment Level = 4.*

Figure 32 zooms on the highlighted area of in Figure 29:

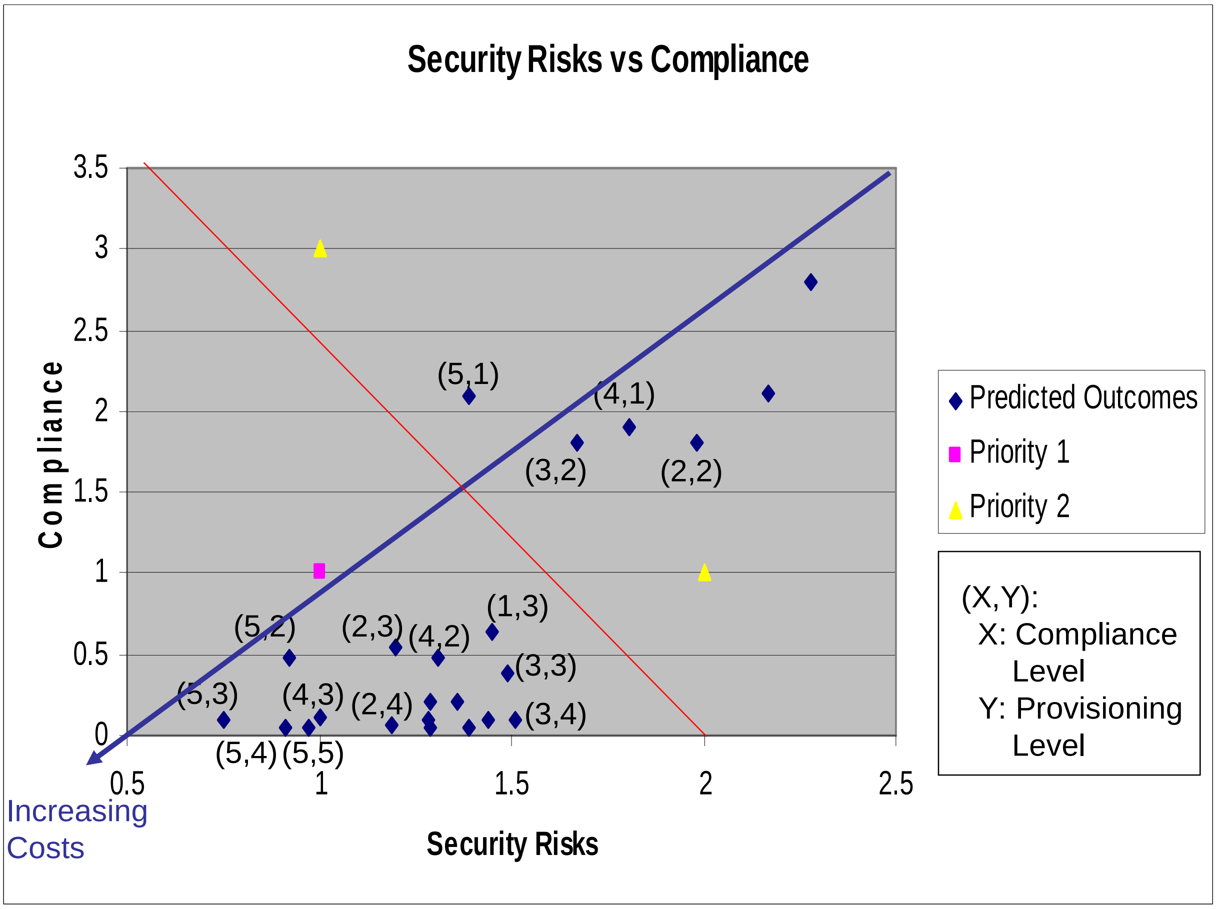


Fig. 32. Zooming - Comparing Predicted Outcomes against Strategic Preferences (ordered by Priorities) – Compliance vs Security Risks

This figure shows that Priority 1's preferences can be achieved with a wide range of investment possibilities: the *Provisioning Investment Level* can be any value in the [2-5] range; the *Compliance Investment Level* can be any value in the [4-5] range. Priority 2's preferences can be achieved with even a wider range of investment possibilities.

To conclude, by keeping into account these outcomes and various constraints shown in Figure 30, 31 and 32, in order to achieve the decision makers' *Priority 1* preferences, the required investments are:

- ***Provisioning Investment Level = 5;***
- ***Compliance Investment Level = 4.***

This result did not come as a surprise. The decision maker was biased towards achieving high productivity: the predicted outcomes indicate that this can happen only with the highest provisioning investment level and reasonably high compliance investment level, at high costs.

This conclusion has been presented to the decision maker to illustrate the consequences of their preferences. These predictions and conclusions have been validated as feasible and realistic. This enabled the decision maker to reassess their preferences & priorities and explore other options. A follow-up refinement process is currently in place. We believe this is an encouraging result as it provided the decision maker with new ground for analysis and decisions at the business level to act on.

8. Discussion and Related Work

In this case study, the decision maker had an initial clear idea of their priorities and a large IAM budget.

In general this is not so straightforward, as decision makers' priorities might not be obvious, the budget might be much more limited and more stringent trade-offs might need to be taken into account.

In addition, different decision makers within the organization are usually involved in the decision making process: they might have different focuses (e.g. on compliance or on security) and priorities, reflected by different preferences. In this context, our approach can be used to explore these viewpoints, starting from common assumptions, and provide help to decision makers to explore trade-offs and reach compromises.

Additional work is required to refine our approach, in particular to instantiate the decision makers' utility functions. At the moment our work only provides an empirical estimate. Ideally, the targets (preferences) identified by the decision makers and the selected predicted outcomes could also be used to mathematically instantiate these utility functions and fully represent the space of preferences of the decision maker. This is work in progress.

We are not aware of a similar approach to the Economics of IAM, aiming at providing strategic decision support capabilities in the space of Identity and Access Management by coupling economic and system modelling.

As anticipated, the methodology and approach discussed in this paper is the result of recent work by the current authors and others, e.g. [10,11,25,27,28,30,31]. The work presented in this paper further refines this approach, in particular from the preference elicitation front.

Initial work in the IAM Economics space, aiming at providing strategic decision support to decision makers has been discussed in [25] by the current authors: however, that paper does not explicitly discuss the elicitation of strategic preferences; the analysis of IAM investments focuses only on enforcement and provisioning, without considering the role of compliance investments.

Related work on how to use mathematical modeling to affect decisions and provide decision support, is presented in the Management Science Journal [12] as well as in papers focusing on areas such as hydrology, land usage and environmental contexts [13,14,15] or social science [16]. In contrast this work focuses on IT and security aspects. Our challenge is to help strategic decision makers to gain consensus, shared understanding and decision support by effectively involving them in the overall process, from the preference gathering phase to the review of outcomes and any subsequent refinement.

Modelling and simulation have already been used in specific contexts of IAM, to explore the impact of technical choices on policies, such as password policies [17,18], identity phishing [19] and security polices for network access control [20]. This is important related work. However, it does address the problem of how to effectively provide support to (different) decision makers during the decision making process by factoring in economic and strategic aspects. Initial work in this space has been carried out by the authors of this paper [21], but by focusing primarily on modelling and simulation aspects.

In general, we are not aware of current research or commercial solutions that aim at modelling and simulating the overall complexity of identity management – from a strategic angle and providing related decision support capabilities. Standards such as ISO 27001 [22], CoBit [23], ITIL [24] describe best practices and methodologies respectively in terms of information security management, IT governance and service management. Decision makers still need to understand, interpret and instantiate them in their specific operational environments. We can use these standards as drivers and references but our work adds the value of grounding the reasoning to specific environments, related policies and the underlying IT infrastructures (possibly along with human and social behaviours).

9. Conclusions

This paper presented an approach to support decision makers in defining their Identity and Access Management (IAM) strategy.

We illustrated a methodology that helps decision makers work through this complex problem by explicitly exploring their preferences between different strategic outcomes; using system modeling and simulation to predict and analyse the consequences (likely outcomes) associated with different IAM investment choices, for a number of assumed future threats and business scenarios; mapping these predicted outcomes against preferences, to identify the most suitable investment options. We showed how this methodology has been applied in an IAM case study involving enterprise business services underpinned by SAP applications.

Our results have been validated by a senior security and IAM expert acting as a CIO/CISO decision maker, on behalf of a major customer. This enabled discussions and further reassessment of preferences. This work is in progress: we plan to do further research in this space.

Acknowledgments

We would like to thank Adam Mcleroy, Mike Wonham and Francisco Montes for their valuable input, feedback and discussions that helped us to shape our work, directions and the IAM case study.

References

[1] SAP, SAP business solutions, http://www.sap.com/solutions/business-suite/index.epx, 2009

[2] Oracle, Identity Management solutions, http://www.oracle.com/us/products/middleware/identity-management/index.html, 2009

[3] SAP, SAP Netweaver Identity Management, http://www.sdn.sap.com/irj/sdn/nw-identitymanagement, 2009

[4] SAP, SAP VIRSA, http://www.sap.com/uk/solutions/solutionextensions/virsa/index.epx, 2009

[5] APPROVA, APPROVA Access Manager, http://www.approva.net/products/accessmanager/, 2009

[6] Baldwin, A., Casassa Mont, M., Shiu, S., Using Modelling and Simulation for Policy Decision Support in Identity Management, IEEE 10th Symposium on Policies for Distributed Systems and Networks, IEEE Policy 2009 Symposium, 20-22 July, London, 2009

[7] Fishman, G.S., Discrete-Event Simulation: Modelling, Programming and Analysis, Springer-Verlag, 2001

[8] Wikipedia, Monte Carlo method, http://en.wikipedia.org/wiki/Monte_Carlo_method, 2009

[9] HP Labs, Core Gnosis, http://www.hpl.hp.com/research/systems_security/gnosis.html, 2009

[10] Collinson, M., Monahan, B., Pym, D., A discipline of mathematical systems modelling, Forthcoming monograph, College Publications, London, 2010.

[11] Beres, Y, Pym, D. and Shiu, S., Decision support for systems security investment. Manuscript, HP Labs, submitted to BDIM 2010, 2009.

[12] Management Science, Management Science Journal, http://mansci.journal.informs.org/, 2009

[13] Becu, N., Neef, A., Schreinemachers, P., Sankapitux, C., Participatory computer simulation to support collective decision making: Potential and limits of stakeholder involvement, ScienceDirect, Elsevier, 2007

[14] Adams, P.W., Hairston, A.B., Using Scientific Input in Policy and Decision Making, Oregon State University, 1995

[15] Khoo, H.H., Spedding, T.A., Tobin, L., Taplin, D., Integrated Simulation and Modelling Approach to Decision Making and Environmental Protection, Kluwer Academic Publisher, 2001

[16] Kennedy, C., Theodoropoulos, G., Towards Intelligent Data-Driven Simulation for Policy Decision Support in the Social Sciences, School of Computer Science, University of Birmingham, UK, 2005

[17] Shay, R., Bhargav-Spantzel, A., Bertino, B., Password policy simulation and analysis, DIM 2007, 2007

[18] A. Adams and M.A. Sasse, "Users are not the enemies", Communications of the ACM, 1999

[19] Moore, T., Clayton, R., The Consequence of Non-Cooperation in the Fight Against Phishing, 3rd APWG eCrime Res. Summit, 2008

[20] Koh, J.Y., Yi, M., Cho, T., Kim, H., Knowledge-Based Modeling and Simulation of Network Access Control Mechanisms Representing Security Policies, Springer, Information and Communications Security LNCS book, 2002

[21] Baldwin, A., Casassa Mont, M., Shiu, S., Using Modelling and Simulation for Policy Decision Support in Identity Management, HP Labs Technical Report, HPL-2009-56, 2009

[22] ISO, ISO 27001, Information Security Management, 2005

[23] ISACA, Cobit, IT Governance, http://www.isaca.org/, 2008

[24] ITIL, ITIL IT Infrastructure Library for Service Management, http://www.itil-officialsite.com/home/home.asp, 2008

[25] Baldwin, A., Casassa Mont, M., Monahan, B., Pym D., Shiu, S., System Modelling to Support Economic Analysis of Security Investments: A case Study in Identity and Access Management, Trust Economics Workshop and HPL Technical Report HPL-2009-173, 2009

[26] Anderson, R., Why information security is hard — an economic perspective. 17th ACSAC, 358–365, New Orleans: IEEE, 2001.

[27] Beautement, A., Coles, R., Griffin, J., Ioannidis, C., Monahan, B., Pym, D., Sasse, A., Wonham, M., Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security. In Managing Information Risk and the Economics of Security. M. Eric Johnson (editor), Springer, 2009: 141-163.

[28] Beres, Y., Griffin, J., Shiu, S., Heitman, M., Markle, D., Ventura, P., Analysing the Performance of Security Solutions to Reduce Vulnerability Exposure Windows, ACSAC, 33–42, CA, IEEE, 2008.

[29] Gordon, L., Loeb, M., Managing Cybersecurity Resources. McGraw Hill, 2006.

[30] Yearworth, M., Monahan, B., Pym, D., Predictive Modelling for Security Operations Economics. Workshop on the Economics of Securing the Information Infrastructure (WESII), 23—24 October, 2006, Washington DC, HP Labs TR HPL-2006-125.

[31] Ioannidis, C., Pym, D., Williams, J., Investments and trade-offs in the economics of information security. To appear, Proc. Financial Cryptography and Data Security, Dingledine, R. and Golle, P. (editors), LNCS, Springer, 2009.

[32] Collinson, M., Monahan, B, Pym, D., Semantics for Structured Systems Modelling and Simulation. To appear, *Proc. Simutools 2010*, ACM.

[33] Collinson, M., Monahan, B., Pym, D., A Logical and Computational Theory of Located Resource. To appear, Journal of Logic and Computation, 2009. Advance Access published on 22 July, 2009. doi:10.1093/logcom/exp021.

[34] Collinson, M., Pym, D., Algebra and logic for resource-based systems modelling. *Mathematical Structures in Computer Science* 19:959-1027, 2009. doi:10.1017/S0960129509990077.

[35] Casassa Mont, M, Beres, Y., Pym, D., Shiu, S., Economics of Identity and Access Management: Providing Decision Support for Investments, HPL Technical Report HPL-2010-11, 2010

Appendix A: IAM Model

This section contains the complete IAM model that has been developed to carry out our simulations. It has been developed by using the HP Labs GNOSIS modelling and simulation tools [9].

```
-- Title     : iam_economics-model.gn - Model about IAM economics for business services underpinned by SAP applications
-- Author    : Simon Shiu & Marco Casassa Mont & Yolanta Beres (simon.shiu@hp.com, marco.casassa-mont@hp.com, yolanta.bers@hp.com)
-- Date/Time : 31 Decembr 2009
-- Version   : v.09-o
-- Copyright : Hewlett-Packard 2009

-- output : on
-- Trace Level = 1

-- spawnlimit : 10000000
-- livenesslimit : 10000000
-- seed      : 8769886775889

  // Time parameters - by default time is measured in days
  //-----------------------------------------------------------

  param days       = 1
  param weeks       = 7 * days
  param years       = 365 * days

 // Simulation Parameters
  //----------------------

  param runTime = 1*years   // simulation runtime
  param coin = uniform (0,1) // generic uniform distribution
```

```
// Investment Levers: increasing these numbers increases investment
//-------------------------------------------------------------------

param provisioning = 1  // options in [1,5] range
param enforcement = 4   // options in [1,5] range
param compliance = 1    // options in [1-5] range  - this is about investments in IAM compliance checking, reporting and remediation tools

// Lever Ranges
param lowLeverValue = 1;
param highLeverValue = 5;
param leverRange = (highLeverValue - lowLeverValue) +1;


// Initialisation of General Parameters
//-------------------------------------

// Users

param initusers = 10
param initleavers = 0

// Applications (Classified by Security Configuration/Enforcement: Strong, Medium, Weak)

param initstrongapp = 15
param initmediumapp = 30
param initweakapp = 15
param inittotalapps = initstrongapp + initmediumapp + initweakapp

// User Accounts (Classified in terms of various access types)

param initbizaccess = 20
param initnonbizaccess = 0
param initbadaccess = 0
param initnonaccess = 580
param initotheraccess = 0
```

```
 // Audit Process Properties

 param numAccountChecksPerAppAUDIT =    1/10                  // External factor. Independent from investments
 param applicationSamplingNumberAUDIT = round(inittotalapps/10) // External factor. Independent from investments

 // Compliance Checking Process Properties

 param numUserAccountsChecksPerApp = 1/(1+(leverRange-compliance)^2)  // number of checked user accounts per app - dependency on compliance
lever
 param appSamplingRatio = 1/(1+ inittotalapps-((inittotalapps/highLeverValue)*compliance)) // number of audited apps - dependency on compliance
lever

 // Provisioning Process Properties

   // Managing passive and active approval: dependency on investment in provisioning
   // failure depending on misconfiguration of managers/no manager


           // passiveManagerApprovalRate[provisioning] := probability
           array passiveManagerApprovalRate[int] : num = {0}

           passiveManagerApprovalRate[1] := 60/100
           passiveManagerApprovalRate[2] := 65/100
           passiveManagerApprovalRate[3] := 78/100
           passiveManagerApprovalRate[4] := 98/100
           passiveManagerApprovalRate[5] := 9999/10000

           // activeManagerApprovalRate[provisioning] := probability
           array activeManagerApprovalRate[int] : num = {0}

           activeManagerApprovalRate[1] := 50/100
           activeManagerApprovalRate[2] := 55/100
           activeManagerApprovalRate[3] := 85/100
           activeManagerApprovalRate[4] := 99/100
```

```
        activeManagerApprovalRate[5] := 9999/10000

        param testPassiveApproval = bernoulli(passiveManagerApprovalRate[provisioning])
        param testActiveApproval = bernoulli(activeManagerApprovalRate[provisioning])

// Managing SysAdmin failures
        //----------------------------

        // sysAdminFailureRate[provisioning] := probability
array sysAdminFailureRate[int] : num = {0}

sysAdminFailureRate[1]    := 1/50
sysAdminFailureRate[2]    := 1/150
sysAdminFailureRate[3]    := 1/250
sysAdminFailureRate[4]    := 1/800
sysAdminFailureRate[5]    := 1/1000

// sysAdminNoConfigRate[provisioning] := probability
array sysAdminNoConfigRate[int] : num = {0}

sysAdminNoConfigRate[1] := 1/70
sysAdminNoConfigRate[2] := 1/180
sysAdminNoConfigRate[3] := 1/300
sysAdminNoConfigRate[4] := 1/900
sysAdminNoConfigRate[5] := 1/1100


        param sysAdminFailureConfig = bernoulli(sysAdminFailureRate[provisioning])
        param sysAdminNoConfig = bernoulli(sysAdminNoConfigRate[provisioning])


// Likelihood to bypass provisioning approval
        //-------------------------------------------

        // bypassProvisioningApprovalRate[provisioning] := probability
        array bypassProvisioningApprovalRate[int] : num = {0}

        bypassProvisioningApprovalRate[1] := 1/50
        bypassProvisioningApprovalRate[2] := 1/100
        bypassProvisioningApprovalRate[3] := 1/500
        bypassProvisioningApprovalRate[4] := 1/1000
        bypassProvisioningApprovalRate[5] := 1/1200

        param bypassProvisioningApproval = bernoulli(bypassProvisioningApprovalRate[provisioning])

// Communication failure with sysadmin
        //---------------------------------------

        // sysAdminCommunicationFailureRate[provisioning] := probability
        array sysAdminCommunicationFailureRate[int] : num = {0}

        sysAdminCommunicationFailureRate[1] := 1/50
        sysAdminCommunicationFailureRate[2] := 1/120
        sysAdminCommunicationFailureRate[3] := 1/350
        sysAdminCommunicationFailureRate[4] := 1/900
        sysAdminCommunicationFailureRate[5] := 1/1000


        param sysAdminCommunicationFailure = bernoulli(sysAdminCommunicationFailureRate[provisioning])


        // Communication of changes to management
//---------------------------------------


        // communicationFailureRate[provisioning] := probability
        array communicationFailureRate[int] : num = {0}

        communicationFailureRate[1] := 1/75
communicationFailureRate[2] := 1/180
```

```
  communicationFailureRate[3] := 1/750
  communicationFailureRate[4] := 1/1200
  communicationFailureRate[5] := 1/1500


  param testCommunicationFailure = bernoulli(communicationFailureRate[provisioning])



// Threat Scenario Settings
//-------------------------

param high = 10
param low = 1

(*
	scenario 1

	Basically a trustworthy internal group, there is some expectancy of fraud ayttempts as with any population.
	People are leaving, but not especially with bad feeling.
*)
param internalthreat = 2 // range 1-5
param exworkerthreat = 2 // range 1-5
param externalthreat = 2 // range 1-5
param proportionskilled = 0.02  // range [0,1]
param usertraining = 2 // higher means less likely to make mistakes
param coolofftimeforleaver = 15 * exworkerthreat
var skill = low

(*
	scenario 2
	Major redundancy and bad economy imply disgruntled effect
*)

(*
        param internalthreat = 3 // range 1-5
        param exworkerthreat = 5 // range 1-5
        param externalthreat = 4 // range 1-5
        param proportionskilled = 0.1 // range [0,1]
        param usertraining = 2 // higher means less likely to make mistakes
        param coolofftimeforleaver = 15 * exworkerthreat
        var skill = low
*)


// Environmental and Threat parameters
// ------------------------------------


// User Events - New, Leaving and Chainging Users

param newusertrigger    = negexp(3.5*days)
param leavertrigger = negexp(7*days)
param changerightstrigger = negexp (30*days)

// Application Events

// appUpgrateRate[enforcement] := probability
         array appUpgradeRate[int] : num = {0}

         appUpgradeRate[1] := 100*days
  appUpgradeRate[2] := 100*days/3
  appUpgradeRate[3] := 100*days/10
  appUpgradeRate[4] := 100*days/40
  appUpgradeRate[5] := 100*days/50

param upgradeapptrigger = negexp (appUpgradeRate[enforcement])
param generalweakeningtrigger = negexp (30*days)

// Number of Applications affected by users joining, leaving and changing role
```

```
param numAppNewUser = point [(0.4,1),(0.3,2),(0.2,3),(0.05,5),(0.04,6),(0.01,7)]
param numAppLeaverUser = point [(0.4,1),(0.3,2),(0.2,3),(0.05,5),(0.04,6),(0.01,7)]
param numAppChangeRoleUser = point [(0.4,1),(0.3,2),(0.2,3),(0.05,5),(0.04,6),(0.01,7)]

// Ratio of adding or losing roles/access for User Changing Role

param addACCESS = 1
param loseACCESS = 2
param typeAccessChange = point [(0.5,addACCESS), (0.5,loseACCESS)]


// Compliance Events

param cCRtrigger = negexp (150*days/compliance)  // CCR activities determined by level of compliance investments
param accessRemediationTime = normal (8*days,3)  // average time taken for access remediation
param weakAppRemediationTime = normal (15*days,3)  // average time taken for remediation for weak app --> medium app
param mediumAppRemediationTime = normal (10*days,3)  // average time taken for remediation for medium app --> strong app

param auditTrigger = negexp (180*days) // Exogenous event. Triggered by external auditing factor

// Threat Events and settings

param internalthreattrigger = negexp (20*days/internalthreat)
param exworkerthreattrigger = negexp (100*days/(exworkerthreat * exworkerthreat))
param externalthreattrigger = negexp (20*days/externalthreat)
param threattrigger = negexp (10*days)

param badaccessweight = 3 // Bad access is considered three times as bad (as likely to help fraud) as biz access
param otheraccessweight = 5 // Other access (i.e. hanging account) is considered as very bad
param weakprotection = 0.5
param mediumprotection = 0.75
param strongprotection = 0.9

param intranetprotection = enforcement/leverRange
```

```
(*
  The State
  all the ones representing the configuration (user to resource mapping)
  - bizaccess, nonbizaccess, badaccess and nonaccess
  and the ones representing the state of the strength of enforcement
  and the ones representing the compliance checking and auditing processes
*)


        var users = initusers
        var leavers = initleavers

        var newuserAcccount = 0
        var leaverAcccount = 0
        var changeuserAcccount = 0

  var strongapp = initstrongapp
  var mediumapp = initmediumapp
  var weakapp = initweakapp
  var totalapps = inittotalapps

        var bizaccess = initbizaccess
  var nonbizaccess = initnonbizaccess
  var badaccess = initbadaccess
  var nonaccess = initnonaccess

  // we also need to count accounts for people who've left
  var otheraccess = initotheraccess


  var sanitydistance = 0
        var badleaver = 0
        // and what we use to count the loss
  var incidentacount = 0
  var incidenthcount = 0
  var incidentwcount = 0
  var incidentecount = 0
  var incidentescount = 0
  var incidenteacount = 0
  var incidenteawcount = 0
  var incidentprevention = 0
  var incidenteprevention = 0
  var incidenteaprevention = 0

 // Compliance CCR variables

  var complianceCCRactivities = 0
  var accessIssuesFinding = 0
  var securityIssuesFinding = 0
  var accessRemediationActivities = 0
  var securityRemediationActivities = 0

  var weakAppRemediationActivities = 0
  var mediumAppRemediationActivities = 0

// Audit variables

  var auditActivities = 0


// Aggregated Metrics

  var productivityMetric = 0
  var totalincidentcount = 0
  var totalincidentprevention = 0
  var auditComplianceViolationAccess = 0
var auditComplianceViolationSecurity = 0

//-------------------------------------------------------------------
// The Process/Structure Model
//  Processes that represent day to day IAM business
//  comings and goings of users: newuser, leaver, changerights
//  and apps security management
//-------------------------------------------------------------------

//-------------------------------------------------
// Process dealing with the Management of New Users
//-------------------------------------------------
process newuser = {
launch newuser after newusertrigger

var numApp = numAppNewUser
var counter = 1
var totalapps = strongapp + mediumapp + weakapp

// lets assume these are generally well handled

users := users + 1

 // We only care about the access affecting involved applications
 // For all other applications users will have no access

 nonaccess := nonaccess + (totalapps - numApp)

 newuserAcccount := newuserAcccount + numApp

 counter := 1
 while [counter <= numApp]
   {
             trace ("NEW USER PROVISIONING %v (OF %v)", counter, numApp)
             call newuserProvisioning()
```

```
            counter := counter +1
   }
}

// Routine - Provisioning Process of New Users

routine newuserProvisioning () = {

        // Provisioning lever: 1-5 range

        var approvalSuccess = 0

        if [(testPassiveApproval == 1)]
          {  // case where correct passive approval has been given
            approvalSuccess := approvalSuccess + 1

            // TBD: adding waiting time --> productivity impact
    }

         if [(testActiveApproval ==1)]
          {  // case where correct active approval has been given
            approvalSuccess := approvalSuccess + 1

            // TBD: adding waiting time --> productivity impact
   }

  // full approval has been given by management
  if [(approvalSuccess == 2)]
    {
              if [(sysAdminFailureConfig == 1)]
               {   // sysadmin configuration went wrong
                        badaccess := badaccess + 1
               }
              or [(sysAdminNoConfig == 1)]
               {
```

```
                        // sysadmin carried out no configuration
                        nonbizaccess := nonbizaccess + 1
                }
               or else
                {
                       // user account has been properly configured
                       bizaccess := bizaccess + 1
                }
     }
    or else
    {
           //case where initial approval process has failed

           if [(bypassProvisioningApproval ==1)]
             { // process is bypassed to get unauthorised access
              badaccess := badaccess + 1

             }
      or else
        {
              nonbizaccess := nonbizaccess + 1
        }
    }
  }

//------------------------------------------------
// Process Dealing with the Management of Leavers
//------------------------------------------------

 process leaver = {
   launch leaver after leavertrigger



 var numApp = numAppLeaverUser
 var counter = 1
```

```
  var totalapps = strongapp + mediumapp + weakapp



  users := users - 1
  leavers := leavers + 1

  leaverAcccount := leaverAcccount + numApp

    // most of applications are already not accessible to the user ...
    if [(nonaccess - totalapps + numApp)>0]
     {
        nonaccess := nonaccess - totalapps + numApp
     }
    or else
     {
                nonaccess := 0
     }

  counter := 1

   while [counter <= numApp]
     {
                 trace ("USER LEAVER - DE-PROVISIONING %v (OF %v)", counter, numApp)
                 call userLeaverDeProvisioning()
                 counter := counter +1
     }
     launch  leaverCoolOffTime after 0.0
}

process leaverCoolOffTime =
  {
          hold (coolofftimeforleaver)
    leavers := leavers - 1
  }
```

```
// Routine - De-Provisioning Process for Leaving Users

routine userLeaverDeProvisioning()= {

        // add delay time to deprovisioning (depending on provisoning leaver)

        if [(sysAdminCommunicationFailure ==1)]
        {
                // Communication failure with SysAdmin - no deprovisioning of current access
                // the user retains his current access rights despite not being anymore entitled
                otheraccess := otheraccess +1  //hanging account
 }
 or [(sysAdminFailureConfig ==1)]
 {
          //Failure in configuration. User retain access
          otheraccess := otheraccess +1  //hanging account
 }
        or else
 {
          // proper De-Provisioning process - user loses their access rights

          var totalNumAcc = bizaccess + badaccess + nonbizaccess
          var cointoss = uniform (0,totalNumAcc)

          // Checking what is affected
          //
          if [(cointoss<bizaccess)]
           {
                  bizaccess := bizaccess -1          // traditional deprovisioning of business access
           }
          or [(cointoss<(bizaccess + badaccess))]  // user actually had no biz access. They might had badaccess or nonbizaccess ...
           {
                  badaccess := badaccess - 1
          }
```

```
                or else                                         // case where the user had nobizaccess. Handling it at deprovisioning ...
                {
                          if [nonbizaccess>0]
                            {
                              nonbizaccess := nonbizaccess-1
                      }
                }
      }
}
 //-----------------------------------------------------------------
 // Process dealing with User changing roles (adding/losing roles)
 //-----------------------------------------------------------------

 process changerights = {
   (*
     This should really change access amounts in a volume correlated
     with the number of apps/resources.
     But that gets pretty messy for not much gain at this stage
   *)
   launch changerights after changerightstrigger

   var numApp = numAppChangeRoleUser
   var counter = 1
   var totalapps = strongapp + mediumapp + weakapp

    counter := 1

    changeuserAcccount := changeuserAcccount + numApp

    while [counter <= numApp]
      {
                  //  Decision on which type of change is involved: adding or losing role
                  if [(typeAccessChange == loseACCESS)]  // LOSE ACCESS TO APP
                   {
                     trace ("USER LOSING ROLE/ACCESS TO APP - DE-PROVISIONING %v (OF %v)", counter, numApp)
      // Failure of communication is already taken into account in the routine
          call userLoseAccessDeProvisioning()
    }
        or else //GET ACCESS TO APP
        {
            // there might be a failure in communicating the need to add access rights
         if [(testCommunicationFailure==1)]
         {
              // Case of non biz access
              nonbizaccess := nonbizaccess + 1
              nonaccess := nonaccess - 1
         }
         or else
         {
             trace ("USER GETTING ROLE/ACCESS TO APP - PROVISIONING %v (OF %v)", counter, numApp)
          nonaccess := nonaccess - 1
             call newuserProvisioning()
         }
        }
        counter := counter +1
  }
}


 // Routine - De-Provisioning Process for Users Losing Access

 routine userLoseAccessDeProvisioning()= {

     // add delay time to deprovisioning (depending on provisoning leaver)

     if [(sysAdminCommunicationFailure ==1)]
     {
          // Communication failure with SysAdmin - no deprovisioning of current access
```

```
            // the user retains his current access rights despite not being anymore entitled
                          bizaccess := bizaccess - 1
                 badaccess := badaccess + 1

}
or [(sysAdminFailureConfig ==1)]
{
      //Failure in configuration. User retain access
                   bizaccess := bizaccess - 1
                 badaccess := badaccess + 1

}
    or else
{
      // proper De-Provisioning process - user loses their access rights

      // Checking what is affected
      //
      nonaccess := nonaccess + 1

      var totalNumAcc = bizaccess + badaccess + nonbizaccess
      var cointoss = uniform (0,totalNumAcc)

      if [(cointoss<bizaccess)]              // traditional deprovisioning of business access
       {
             bizaccess := bizaccess -1
       }
      or [(cointoss<(bizaccess + badaccess))]  // user actually had no biz access. They might had badaccess or nonbizaccess ...
       {
             badaccess := badaccess - 1
      }
      or else                             // case where the user had nobizaccess. Handling it at deprovisioning ...
      {
            if [nonbizaccess>0]
            {
                    nonbizaccess := nonbizaccess-1
              }
            }
    }
}

//--------------------------------------------------
// General process shifting the balance of weak apps.
// We reflect the fact that application security erode and threats increase
// It has to keep investing to preserve the current state
// of protection
//--------------------------------------------------

  // the weakening of applications is a function of time
  // assuming the applications have some degree of enforcement/security
  process generalweakening = {
          launch generalweakening after generalweakeningtrigger

          if [strongapp > 0] {
                  strongapp := strongapp - 1
                  weakapp := weakapp + 1
          }
          if [mediumapp > 0] {
                  mediumapp := mediumapp - 1
                  weakapp := weakapp + 1
          }
  }

  // The process and frequency of upgrading applications depends on the investment efforts made on enforcement

  process upgradeapp = {
    launch upgradeapp after upgradeapptrigger
    // toss a coin and use thresholds to determine the protection strength of app to be upgraded
    // NB we assume it can't be strong, as there would be nothing to do
    var totalapps = mediumapp + weakapp
  var upgradeappcointoss = uniform (0, totalapps)
  if [upgradeappcointoss < weakapp] { // were upgrading a weak app
    weakapp := weakapp - 1
    mediumapp := mediumapp + 1
  }
  or [upgradeappcointoss < weakapp + mediumapp ] { // were upgrading a medium app
    mediumapp := mediumapp - 1
    strongapp := strongapp + 1
  }

}

//---------------------------------------------------------------------------------
//  The Threat Environment
//  We assume attacks of different types can happen, with some frequency - depending on the threat environment
//  Depending on its type and the state we check if it succeeds or not
//------------------------------------------------------------------------------------

//----------------------
// Internal Attacks
//----------------------

process internalattack = {
                // Attack frequency modelled as a negative exponential
                // Prevention of previous attacks might reduce the frequency, whilst the number of successful
                // previous attack can incentivate furhter attacks
                        var temp = negexp (((incidentprevention+1) * 30 * days)/((incidentacount+1) * internalthreat)^2)
                        var trigger = 1*days max temp
             launch internalattack after trigger

                        // Create state/context for this attack

                        var accessthreat = ((badaccessweight * badaccess) + bizaccess) / nonaccess
                        // Check it the attacked application is a weak or a strong one
                        var appthreat = 1
var totalapps = strongapp + mediumapp + weakapp
var cointoss = uniform (0,totalapps)

if [cointoss < weakapp] { // the attacker has attacked a weak app, so has good chance of success
    appthreat := weakprotection
}
or [cointoss < (weakapp + mediumapp) ] { // the attacker has attacked a medium app
    appthreat := mediumprotection
     }
or else { // the attacker has attacked a strong app
    appthreat := strongprotection
     }
     // check how much skill the attacker has
     var coin = uniform (0,1)
     if [coin < proportionskilled] {
             skill := high
     }
     or else {
             skill := low
     }

     // The state is determined, checking if the attack succeeds
     coin := uniform (0,1)

     // Attack exploiting access threat
     if [coin < accessthreat] {
             incidentacount := incidentacount + 1
     }
     // Attack exploiting skills
       //or [skill == high] {
            // incidenthcount := incidenthcount + 1
       //}
     // Attack exploiting level of protection of targeted application
     or [appthreat == weakprotection] {
             coin := uniform (0,1)
            // Keeping into account the level of Intranet protection
            if [coin > intranetprotection] {
                incidentwcount := incidentwcount + 1
            }
            or else {
                 incidenteprevention := incidenteprevention + 1
            }
        }
        or else {
            incidentprevention := incidentprevention + 1
        }
    }

var intranet = high

//----------------------
// Ex Workers Attacks
//----------------------

process exworkerattack = {
    launch exworkerattack after exworkerthreattrigger

    // Create the state/context for this attack
     var totalaccess = badaccess + bizaccess + otheraccess
  var hangingthreat = 0

  //trace("totalaccess: %v", totalaccess)

   if [totalaccess>0] {
        hangingthreat := leavers * otheraccess * otheraccessweight / totalaccess
   }

    var coin = uniform (0,1)
    // Checking state of intranet security protection
    if [coin > intranetprotection] {
          intranet := low
    }
    or else {
          intranet := high
    }
    // Checking skills of attackers
    coin := uniform (0,1)
    if [coin < proportionskilled] {
          skill := high
    }
    or else {
          skill := low
    }

    // Now we have the state. Checking if the attack succeeds

    if [skill == high] {
      coin := uniform (0,1)

      // Attack might succeed because of attacker's skills and the "hanging account" threat

      if [coin < hangingthreat] {
            incidentescount := incidentescount + 1
        }
      or else {
            incideteprevention := incidenteprevention + 1
      }
}

      // Attack might succeed because of the intranet state and the "hanging account" threat

or [intranet == low] {
      coin := uniform (0,1)
      if [coin < hangingthreat] {
            incidentecount := incidentecount + 1
```

```
     }
     or else {
         incidenteprevention := incidenteprevention + 1
     }
 }
 or else {
     incidenteprevention := incidenteprevention + 1
 }
}

//----------------------------
// External Attacks
// External threat is all about attempts to abuse user accounts (e.g. to steal or embarass)
// rather than deploy bots etc...
// so success is tied to availability of credentials, and strength of protection of apps and intranet
//----------------------------

process externalattack = {
    var temp = negexp (((incidenteaprevention+1)/(incidenteawcount+1))^2 * 20 * days/externalthreat)
    var trigger = temp

    launch externalattack after trigger //externalthreattrigger
    var intranet = high
    var coin = uniform (0,1)

    // Checking for protection level of intranet
    if [coin > intranetprotection] {

        var coin1 = uniform (0,1)


        // Attack based on current threat profile (internal and ex-worker threats)

        if [ coin1 < (internalthreat * exworkerthreat)/25 ] {
            incidenteacount := incidenteacount + 1
```

```
                    }
            var totalapps = strongapp + mediumapp + weakapp
            var cointoss = uniform (0,totalapps)

            // Attack on weak application

            if [cointoss < weakapp] { // the attacker has attacked a weak app, so has good chance of success
                incidenteawcount := incidenteawcount + 1
          }
          or else {
                  incidenteaprevention := incidenteaprevention + 1
          }
          }
     or else {
                incidenteaprevention := incidenteaprevention + 1
     }
}

//---------------------------------------------------------------
// COMPLIANCE MANAGEMENT
//
// Process in charge of dealing with periodic IAM compliance checks and reporting
// Dependency on investments made on compliance
// Remediation activities are generated on reactive basis
//------------------------------------------------------------

 process complianceCheckAndRemediation = {
          launch complianceCheckAndRemediation after cCRtrigger

          var probAccessIssues = 0
          var numapp = weakapp + mediumapp + strongapp

          var appSamplingNumber = 0

          var numAccountChecksPerApp = round (users * numUserAccountsChecksPerApp)
```

```
    var numA = 1
    var numU = 1
    var pTest = 0
var numAccessFindings = 0
    var appFactor = 0
var badCount = 0

    complianceCCRactivities := complianceCCRactivities + 1

    appSamplingNumber := round(numapp * appSamplingRatio)


    // Check for non compliance in terms of access rights
    // Initial assumption - probability of discovery of compliance issues depends on:
    //   - frequency of checks (modeleled by frequency of running this process - based on investment in compliance
    //   - actual number of bad accesses, other accesses (hanging accounts)
    // QUESTION: should we consider nonbiz accesses? Are they relevant as a matter of compliance? - at the moment we don't


// ACCESS ISSUE
    // Probability of finding something wrong about access rights - average value for all managed applications
    // An assumption of uniformity of distribution is made here

    probAccessIssues := (badaccess + otheraccess)/(bizaccess + badaccess + otheraccess)

    //trace("Probability Discovery access issues = %v",  probAccessIssues)

    numAccessFindings := 0
    badCount := badaccess + otheraccess

    // For each sampled application
    for numA=1 to appSamplingNumber
    {
    // For each tested user account
```

```
        for numU=1 to numAccountChecksPerApp
         {
               // testing if an access issues has been found
               // keep into account bad findings
               pTest := coin

          if [ (pTest < probAccessIssues) && (badCount > 0)]
           {
                 accessIssuesFinding := accessIssuesFinding + 1
                 numAccessFindings := numAccessFindings + 1
                 badCount := badCount - 1
           }
           or else {}
    }
        }

       // Carry out remediation activity on access
  launch CCRaccessRemediation (numAccessFindings) after 0.0

  // Check for application compliance, based on current security settings
  // Assumption aiming at improving security status
  // weak --> medium
  // medium --> strong
  // TO BE DONE: understand testing criteria for "discovering" an application is either weak or medium
  //var checkAppCoin = uniform (0, numapp)

       for numA=1 to appSamplingNumber
       {
    launch checkCCRappfindings after 0.0
  }
}

process checkCCRappfindings  = {
        if [(coin *(weakapp + mediumapp + strongapp)) < weakapp] { // found a weak application
          securityIssuesFinding := securityIssuesFinding +1
          launch CCRweakAppRemediation  after 0.0
         }
        or [coin *(weakapp + mediumapp + strongapp) < (weakapp + mediumapp) ] { // found a medium protected application
          securityIssuesFinding := securityIssuesFinding +1
          launch CCRmediumAppRemediation  after 0.0
         }
        or else {   // application is ok
               }
}



  // Access control - CCR remediation activities
  // Reaction to CCR reports

  process CCRaccessRemediation (numberAFinding:num) = {

           var flag = 0
           var nFixes = numberAFinding
           var i = 0
           var ht = accessRemediationTime

           // waiting time to fix the access configuration problem
    while [ ht < 0] { ht := accessRemediationTime }

    hold(ht)

           for i = 1 to nFixes
             {

                          if [(badaccess>0) && (otheraccess>0)]
                           {

                                // case if both badaccesses and otheraccesses are present
```

```
              // checking the type of wrong access to be fixed
              if [coin * (badaccess + otheraccess) < badaccess]
               {
               // case of fixing a bad access (of an existing user)
               badaccess := badaccess -1
               nonaccess := nonaccess +1
            }
              or else
               {
                  // case of fixing other access (hanging account of a user that has left)
                 otheraccess := otheraccess -1
                 badaccess := badaccess-1     // ASSUMPTION: this also fixes a bad access, due to previous misconfiguration
               }
             accessRemediationActivities := accessRemediationActivities +1
           }
          or [badaccess > 0]
           {
              // case of bad access
               badaccess := badaccess -1
               nonaccess := nonaccess +1
               accessRemediationActivities := accessRemediationActivities +1
           }
          or [otheraccess > 0]
           {
               // case of other access
               otheraccess := otheraccess -1
               //nonaccess := nonaccess +1
               accessRemediationActivities := accessRemediationActivities +1
           }
          or else
           {
               trace("This might not actually ever happen - case where there is no bad access or other access");
           }
  }
}
```

```
// Weak Application - CCR remediation activities
// Reaction to CCR reports


process CCRweakAppRemediation  = {

        var ht = weakAppRemediationTime

// average time taken for remediation for weak app --> medium app

  while [ ht < 0 ] {ht := weakAppRemediationTime}

  hold(ht)

         if [weakapp>0]
          {
                weakapp := weakapp - 1
                mediumapp := mediumapp + 1
           weakAppRemediationActivities := weakAppRemediationActivities + 1
           securityRemediationActivities := securityRemediationActivities + 1
    }
   or else { }
}

 // Medium Application - CCR remediation activities
// Reaction to CCR reports


process CCRmediumAppRemediation  = {
  var ht = mediumAppRemediationTime
  // average time taken for remediation for medium app --> strong app
        while [ht<0] { ht :=  mediumAppRemediationTime}
   hold(ht)

            if [mediumapp>0]
             {
                    mediumapp := mediumapp - 1
                    strongapp := strongapp + 1
              mediumAppRemediationActivities := mediumAppRemediationActivities + 1
              securityRemediationActivities := securityRemediationActivities + 1
     }
    or else { }
}

// Auditing Activity
// Driven by External factors. Checking for Compliance Violations

process auditActivity = {
           launch auditActivity after auditTrigger

             var probAccessIssues = 0
             var numapp = weakapp + mediumapp + strongapp


             var numA = 1
             var numU = 1
             var pTest = 0
             var auditedAccounts = 0


             auditActivities := auditActivities + 1

             // Check for non compliance in terms of access rights in user accounts
             // Probability of finding something wrong about access rights - for applications
             // An assumption of uniformity of distribution is made here

             probAccessIssues := (badaccess + otheraccess)/(bizaccess + badaccess + otheraccess)
```

```
         trace("AUDIT - Probability Discovery access issues = %v",  probAccessIssues)

         auditedAccounts := round(numAccountChecksPerAppAUDIT * users)

         // For each sampled application
         for numA=1 to applicationSamplingNumberAUDIT
         {
                 // Check for application compliance, based on current security settings
     if [(coin *(weakapp + mediumapp + strongapp)) < weakapp] { // found a weak application
        auditComplianceViolationSecurity := auditComplianceViolationSecurity + 1
       }
     or [(coin*(weakapp + mediumapp + strongapp) )< (weakapp + mediumapp) ] { // found a medium protected application
        auditComplianceViolationSecurity := auditComplianceViolationSecurity + 1
        }
     or else {   // application is ok
        }


         // For each tested user account
         for numU=1 to auditedAccounts
          {
                  pTest := coin

                  // testing if an access issues has been found
                  // keep into account bad findings
            if [ pTest < probAccessIssues]
             {
                    auditComplianceViolationAccess := auditComplianceViolationAccess + 1
             }
     }
    }
}
```

```
  launch newuser after 1.0 * days
  launch leaver after 1.3 * days
  launch changerights after 1.6 * days

  launch upgradeapp after 1.95 * days
        launch generalweakening after 2.3 * days

  launch internalattack after internalthreattrigger
        launch exworkerattack after exworkerthreattrigger
        launch externalattack after externalthreattrigger

        launch complianceCheckAndRemediation after 10.0 * days
  launch auditActivity after auditTrigger

  hold (runTime)

        totalincidentcount := incidentecount + incidentescount + incidentacount + incidenthcount + incidentwcount + incidenteacount + incidenteawcount
        totalincidentprevention := incidentprevention + incidenteprevention + incidenteaprevention

        totalapps := strongapp + mediumapp + weakapp // In this model the number of applications does not change

        if [(bizaccess+nonbizaccess+badaccess)>0] {
          productivityMetric := (bizaccess + badaccess)/(bizaccess+nonbizaccess+badaccess)
   }
  or else {
          productivityMetric :=0
}

  dump ()

  close
```