



## **Economics of Identity and Access Management: Providing Decision Support for Investments**

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

HP Laboratories  
HPL-2010-11

### **Keyword(s):**

Economics, Decision Support, IAM, Modeling, Simulation, Security

### **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.



# Economics of Identity and Access Management: Providing Decision Support for Investments

M. Casassa Mont, Y. Beres, D. Pym, S. Shiu

**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.**

**Index Terms—Economics, Decision Support, IAM, Modeling, Simulation, Security**

## I. 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.

M. Casassa Mont is with Hewlett-Packard Labs, Systems Security Lab, Bristol, UK (phone: +44-117-3128794; fax: +44-117-3129250; e-mail: marco.casassa-mont@hp.com).

Y. Beres is with Hewlett-Packard Labs, Systems Security Lab, Bristol, UK (e-mail: yolanta.beres@hp.com).

D. Pym is with Hewlett-Packard Labs, Systems Security Lab, Bristol, UK (e-mail: david.pym@hp.com).

S. Shiu is with Hewlett-Packard Labs, Systems Security Lab, Bristol, UK (e-mail: simon.shiu@hp.com).

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. [1,2,3,4,5,6], 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, CoBit, 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.

## II. ECONOMICS OF IDENTITY AND ACCESS MANAGEMENT

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 ease 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:

$$U = \omega_1 f_1(T_1 - \overline{T_1}) + \omega_2 f_2(T_2 - \overline{T_2}) + \dots + \omega_n f_n(T_n - \overline{T_n})$$

where  $T_i$  ( $1 \leq i \leq n$ ) represent the outcomes of interest - for example, *security risks*, *productivity*, *compliance and costs*;  $\overline{T_i}$  ( $1 \leq i \leq n$ ) represent the decision maker's targets for these outcomes. The functions  $f_i$  ( $1 \leq i \leq n$ ) represent the decision

maker's tolerance for variance from the targets. Finally, the weights  $\omega_i$  ( $1 \leq i \leq n$ ) 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  $f_i$  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:  $f(x) = (e^{\alpha x} - 1)/\alpha^2$ . 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  $\omega_i$  and that (b) is equally tolerant for going over or under target for each outcome. A related utility function could be the following:

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

## III. 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. [2,3, 7,8,9,10,11] has started to develop a methodology that integrates these two approaches and demonstrates its feasibility. Figure 1 provides an overview of the methodology.

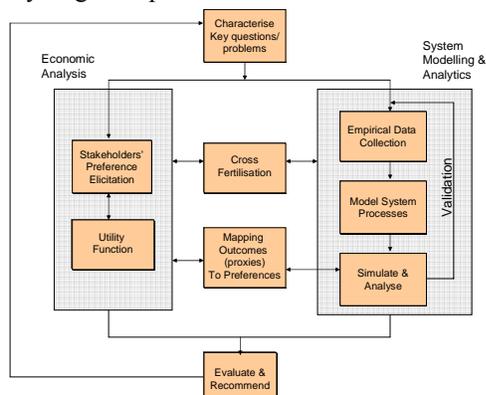


Fig. 1. Overview of the Methodology

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.

#### IV. 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. Due to the space limitations we can only provide an overview of the findings of this case study. The details are going to be provided in [17].

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, Supply Chain Management, Human Resources, Product Lifecycle Management and Supplier Relationship Management.

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 II, 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* [4,10]. 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*.

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 V, VI and VII describe how the methodology has been applied to provide decision support.

## V. ELICITATION OF STRATEGIC 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 II, 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, see Table 1.

TABLE 1: DEFINITION OF OUTCOMES OF RELEVANCE & METRICS

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

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 in Table 2.

TABLE 2: PREFERENCE TRADE-OFFS FOR STRATEGIC OUTCOMES

<b>Security Risks vs. Productivity</b>	Exploring how much the decision maker is willing to compromise security in order to improve productivity (or the way around)
<b>Productivity vs. Compliance</b>	Lack of compliance can sometime be acceptable to increase productivity and the way around (due to stronger controls and bureaucratic processes)
<b>Productivity vs. Costs</b>	Exploring how much the decision maker is willing to compromise in terms of productivity, based on the involved costs
<b>Security Risks vs. Compliance</b>	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

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 2 shows the results.

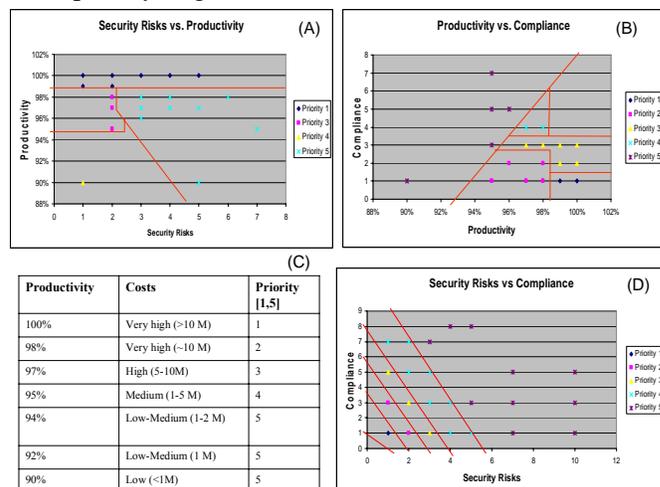


Fig. 2. Results of Elicitation of Decision Maker's Relative Preferences

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 2-(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 2 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 2, 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.

## VI. EXPLORING THE IMPACT OF IAM INVESTMENT OPTIONS BY MEANS OF MODELING 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” [13,15]. Our approach, the mathematical basis of which is presented in [3, 7,14,15,16], 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] which implements this framework and supports Monte Carlo-style simulations.

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 3 shows the high-level view of the 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.

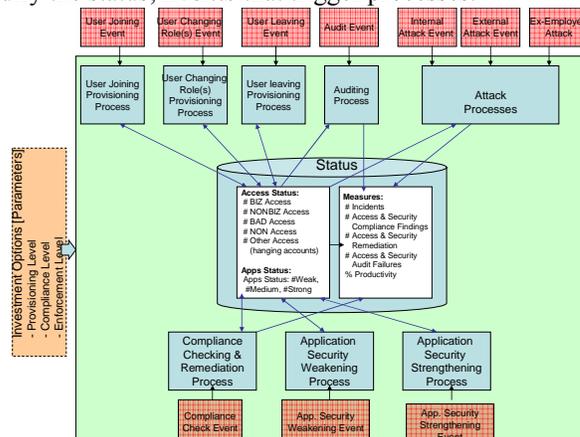


Fig. 3. High-level View of the IAM Model

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). “**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.

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 these 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.

It is beyond the scope of this paper (due to space limits) to provide the details of all the modeled processes and probability distributions. This will be available in [17]. Two examples of modeled processes are shown in Figures 4 and 5.

Figure 4 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.

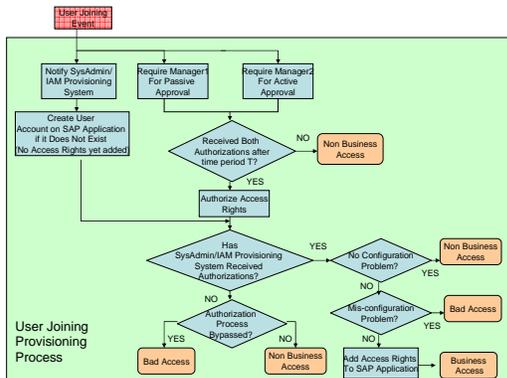


Fig. 4. Modeled User Joining Provisioning Process

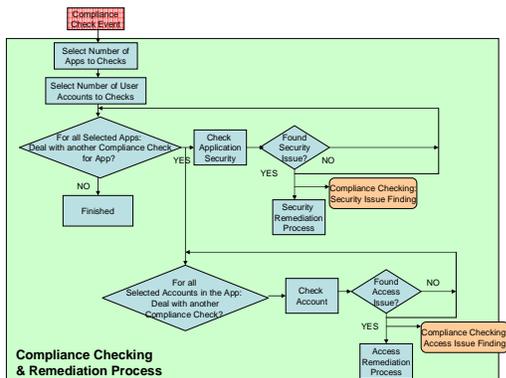


Fig. 5. Modeled Compliance Checking and Remediation Process

Figure 5 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 overall processes impact the status of model, by modifying the values of various *measures*, which 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 V, Table I. 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.

#### A. Assumptions and Parameters

The model is driven by a set of parameters which determine 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. Table 3 shows examples of these parameters. Full details will be available in [17].

TABLE 3: EXAMPLES OF PARAMETERS

<b>User Events - Frequency</b>	<b>New user:</b> negexp (3.5 days), <b>Leaving user:</b> negexp(7 days), <b>User change:</b> negexp(30 days)
<b>Attack Events - Frequency</b>	<b>Internal attack:</b> negexp (10days), <b>External attack:</b> negexp (10days), <b>Ex-worker attack:</b> negexp (25days)
<b>Provisioning Process</b>	<b>sysAdminFailureRate</b> [1,5]=[1/50,1/150,1/250,1/800,1/1000] <b>bypassProvisioningApprovalRate</b> [1,5]=[1/50,1/100,1/500,1/1000,1/1200]
<b>Audit Freq.</b>	<b>Audit activity:</b> negexp (180*days)

We considered a population of 60 SAP applications. The model was initialized with a small set of users, 10 (and related access rights) to explicitly explore the impact of handling new users, users changing roles or leaving the organisation.

#### B. Predicting the Impact of Investment Choices

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.

Average values have been generated for all the *measures*.

Figures 6 and 7 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.

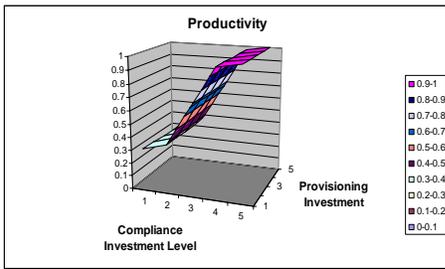


Fig. 6. Simulation - Outcomes for Productivity

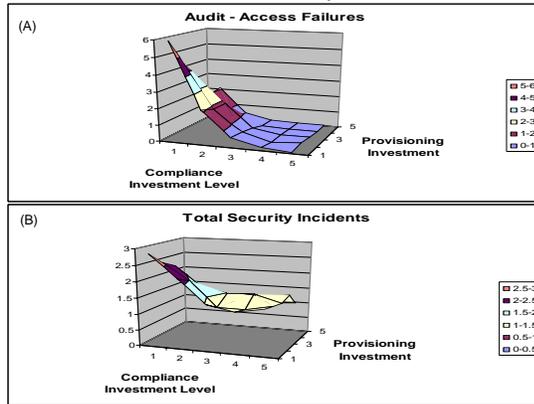


Fig. 7. Simulation - Outcomes for Audit Access Failures and Total Security Incidents

Figure 6 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.

Figure 7 - (A) shows that by increasing the investments in compliance or provisioning the number of *audit failures* (due to access issues) decreases. By increasing the investments in *provisioning*, the number of *bad accesses* and *hanging account* are reduced, because of better practices and automation; by increasing the investments in compliance, audit failures are reduced too, because of the increased effort in compliance checking. So, multiple investment trade-offs are potentially possible to deal with *audit failures*, depending on the decision maker’s preferences in this space. Figure 7 - (B) shows a relatively low number of yearly security incidents: this reflect the fact 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.

## VII. 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 6 and 7 can be displayed in the same way as for the preference elicitation results, shown in Figure 2. Figures 8 and 9 show the result of mapping these predicted outcomes against *the decision makers’ top priority preferences* (i.e. *priorities 1, 2/3*) in Figure 2. Each point that represents a predicted outcome has been labeled with the associated compliance and provisioning levels.

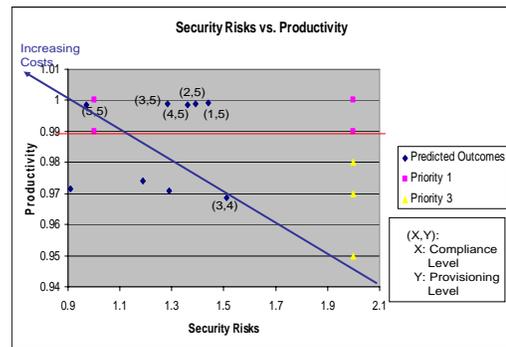


Fig. 8. Mapping of Outcomes against Top Priority Decision Makers’ Preferences – Security Risks vs Productivity

Figure 8 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.

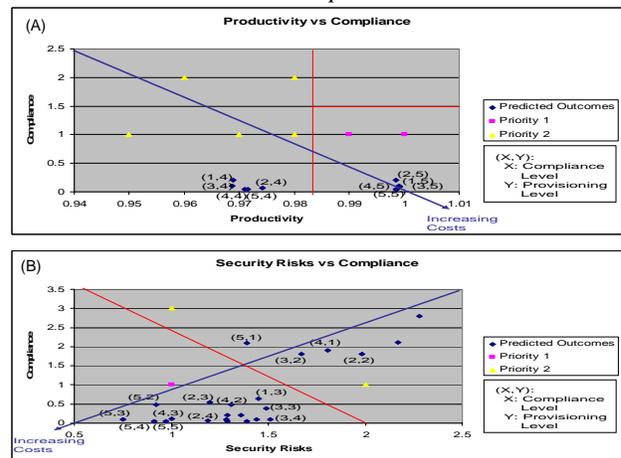


Fig. 9. Mapping of Outcomes against Top Priority Decision Makers’ Preferences – Productivity vs Compliance and Security Risks vs. Compliance

Figure 9 — graph (A) 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. Finally Figure 9 — graph (B) 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.

By keeping into account these outcomes and various constraints, 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.

## VIII. DISCUSSION

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.

## IX. 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.

## REFERENCES

- [1] Anderson, R., Why information security is hard — an economic perspective. 17<sup>th</sup> ACSAC, 358–365, New Orleans: IEEE, 2001.
- [2] Beauteant, 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.
- [3] 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.
- [4] Baldwin, A., Casassa Mont, M., Shiu, S., Using Modelling and Simulation for Policy Decision Support in Identity Management, IEEE Policy 2009 Symposium, 20-22 July, London, 2009
- [5] Gordon, L., Loeb, M., *Managing Cybersecurity Resources*. McGraw Hill, 2006.
- [6] 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, Washington DC, 2006
- [7] Collinson, M., Monahan, B., Pym, D., A Discipline of Mathematical Systems Modelling. Forthcoming monograph, College Publications, London, 2009.
- [8] Ioannidis, C., Pym, D., Williams, J., Investments and trade-offs in the economics of information security. To appear, Proc. Financial Cryptography and Data Security, Dingleline, R. and Golle, P. (editors), LNCS, Springer, 2009.
- [9] Yearworth, M., Monahan, B., Pym, D., Predictive Modelling for Security Operations Economics, HP Labs TR HPL-2006-125, 2006
- [10] 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 TR HPL-2009-173, 2009
- [11] Beres, Y., Pym, D. and Shiu, S., Decision support for systems security investment. Manuscript, HP Labs, submitted to BDIM 2010, 2009.
- [12] SAP, SAP business solutions, <http://www.sap.com/>, 2009
- [13] Fishman, G.S., *Discrete-Event Simulation: Modelling, Programming and Analysis*, Springer-Verlag, 2001
- [14] 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.
- [15] Collinson, M., Monahan, B., Pym, D., Semantics for Structured Systems Modelling and Simulation. To appear, *Proc. Simutools 2010*, ACM.
- [16] 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.
- [17] Casassa Mont, M., Beres, Y., Pym, D., and Shiu, D., Economics of Identity and Access Management: A Case Study on Enterprise Business Services, HPL Technical Report HPL-2010-12, 2010