The Design of an Identity and Access Management Assurance Dashboard Model

Ferdinand Damon, Marijke Coetzee

▶ **To cite this version:**

Ferdinand Damon, Marijke Coetzee. The Design of an Identity and Access Management Assurance Dashboard Model. 12th International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS), Sep 2018, Poznan, Poland. pp.123-133, 10.1007/978-3-319-99040-8_10 . hal-01963057

HAL Id: hal-01963057
https://inria.hal.science/hal-01963057

Submitted on 21 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

The design of an identity and access management assurance dashboard model

Ferdinand Damon, Marijke Coetzee

Academy for Computer Science and Software Engineering,
University of Johannesburg, South Africa
marijkec@uj.ac.za, ferdida@za.ibm.com

Abstract. Executives overseeing Identity and Access Management (IAM) solutions of enterprise information systems have to manage problematic issues at business, technology and governance levels and their related trade-offs. They are required to make informed investment decisions about technology in a complex, ever changing world. The IAM assurance dashboard model proposed by this research provides a comprehensive view of identity and access management components at an executive level. By revealing the current status of the IAM environment within an enterprise, strategic identity and access decisions are possible based on compliance with IAM requirements. The IAM assurance dashboard model gives the current state of an enterprise's IAM status, based on evaluation criteria such as hot spots, maturity, technology gaps and compliance. The SABSA model supports the design of the IAM assurance dashboard which is business requirements driven, to address the needs of executives.

Keywords: Identity management, access management, assurance, SABSA, dashboard, executive view

1 Introduction

In enterprise information systems, security begins with identity management, which is vital to ensure the integrity of identities used to access potentially sensitive resources [1]. As business units do not have an enterprise-wide view of their environment, they may implement silo identity stores and access policies, making a unified strategy for IAM (Identity and Access Management) [2] [3] difficult. Such challenges lead to increasing administrative costs and ineffective controls. From a governance perspective, the implementation of IAM solutions can lead to challenges due to a lack of business focus, where executives overlook the significant impact of IAM on business decisions and compliance [4]. There may also be a lack of funding for IAM projects as the focus is on resolving business problems and customer enhancements [5]. Compliance requirements with laws and regulations forces enterprises to invest more in IAM solutions as they may otherwise incur severe penalties. More importantly, there is to date no executive view of how well IAM functions. To be able to effectively manage IAM problems, a need exists to define a view of IAM for executives to highlight critical issues that

have not been sufficiently addressed [6] [7]. These IAM challenges are primarily focused on business requirements, and less on technology. The main contribution of this research is to extend previous research of the authors on an IAM assurance model [12] by presenting the design of an IAM assurance dashboard model to address these concerns.

To achieve this, the next section defines identity and access management. Nine IAM requirements drive the design of the IAM assurance dashboard model. IAM academic and vendor frameworks all support three core IAM layers that forms the model foundation. IAM assurance components that the dashboard constitutes of are identified by mapping the nine IAM requirements to SABSA (Sherwood Applied Business Security Architecture) layers. The design of the IAM assurance dashboard model is presented, and finally, the paper is concluded.

2 Identity and Access Management (IAM)

Identity and access management (IAM) is a security management approach that aims to enable authorised users to access to specific resources [2]. The objective of IAM solutions is to address challenging compliance requirements progressively. The benefits of implementing an IAM solution are reduced management costs and more flexible support of business activities. The management of identities can be either manual or automated with processes defined over a life-cycle.

Access management, also referred to as access control or entitlement management, supports the provision of user authentication and access control services [1]. An entitlement is a group of attributes that are responsible for representing user privileges and access rights. A role represents a logical association of entitlements. A typical access management flow requires the identification of an identity, followed by authentication [2]. Various technologies and processes support the core elements of an IAM, as identified by security requirements and strategy.

3 IAM assurance dashboard model design

Information security regulations dictate that enterprises define and implement administrative, operational, and technical controls that demonstrate ‘‘reasonable assurance’’ that IAM risks are managed to an acceptable level [8]. The need for assurance requires a general approach that shows compliance with security policies, procedures, and technologies. For this research, IAM assurance refers to the degree of confidence that IAM requirements are satisfied. Figure 1 presents the design approach that details the development of the IAM assurance dashboard model. Figure 1 identifies that the design approach commences with the identification of nine IAM requirements shown in Figure 1(a). Next, the design proceeds clockwise from Figure 1(b) to Figure 1(h), as discussed next.

Identify IAM requirements: In order to identify the components of an IAM assurance dashboard model, IAM requirements were previously identified as drivers for this process [9], [10], [11], [12] as follows:

- *Law and Regulatory* compliance determine that enterprises need to adhere to rules such as those found in the Sarbanes–Oxley (SOX) Act [13].
- Information *access anywhere* requires that employees should be able to access systems from any location using any device.
- *Access protection/accountability* necessitates that identities are entitled to access information and that such actions are audited to protect against increased risk.
- *Single view of an identity* ensures that all attributes of an identity are combined into a single authoritative view.
- *Operational efficiency* ensures that processes such as employee hiring and employee retirement are efficient.
- *Cross enterprise integration* enables the granting of access to external users who are not managed by the enterprise.
- *Cost reduction* identifies that the numbers of employees managing access and compliance needs to be limited.
- *Risk management* expects that IAM risks need be identified and mitigated.
- *End-user experience* links many of the IAM requirements listed as users prefer to be authenticated once and be granted the right levels of access to resources based on their current context.

Next, to ensure that IAM requirements are presented to executives as enablers of business improvements in conjunction with security, their mapping within a security architecture is defined by firstly identifying SABSA as an architecture of choice.

SABSA for IAM assurance: The choice of a security architecture is key to align security functions with the organization's business functions. SABSA (Sherwood Applied Business Security Architecture) [14] is an enterprise security architecture model used by many global enterprises. A guiding principle of SABSA is that it should meet the business requirements of an enterprise and be sufficiently flexible to incorporate global standards, best practices, or legislative acts such as ISO 27001 and CobIT [15]. For executives who require that information security should enable and improve new business opportunities, the SABSA model is thus well-suited, as it is driven by the analysis of business requirements.

The SABSA model is a six layered model, partly shown in Figure 1(b). First, the contextual layer addresses the business requirements definition stage. At each next lower layer a new level of abstraction and detail is developed. From the description of the conceptual architecture, the logical services architecture, the physical infrastructure architecture, and the component architecture (where technologies and products are selected) are defined. Finally, the service management layer ensures operations are managed across all layers. SABSA further defines six vertical dimensions that are refined horizontally by asking six questions namely *what, why, how, who, where* and *when.* Note that figures 1(b) and 1(c) do not give the complete SABSA architecture, but only shows the six architectural layers and the one People (*who*) vertical dimension, shown in Figure 1(c). For this research, the *who* dimension is used to refine IAM assurance as

this layer focuses on people and organisational aspects of security to provide a top down analysis from IAM business requirements to technology concerns and governance [12]. The People (*who*) dimension provides a combined view of the access and identity management domains concepts with elements such as identities and roles in the component architecture layer relating to identity management. Examples of access control include access control lists and access, found in the component and security management architecture layers. Next, the IAM requirements are mapped to identified SABSA layers.

Map IAM requirements to SABSA layers: The mapping of the nine core IAM requirements to the SABSA model is represented in Figure 1(b) and 1(d), resulting in particular IAM domains to be identified. The contextual architecture layer supports (1) law and regulatory compliance, (2) risk management, and (3) access protection and accountability. The conceptual layer supports (4) single view of identity, (5) information access anywhere, and (6) cross enterprise integration. The logical layer supports (7) end user experience. This mapping highlights that the contextual, conceptual and logical architecture layers play a major role in addressing IAM requirements. The contextual architecture level further supports the fact that the representation of IAM information for strategic IAM business driven decisions is important to address. Finally, (8) cost reduction and (9) operational efficiency requirements are supported by the security service management layer. The physical and component security architectures are not mapped to any IAM requirements, indicating that these layers may be enablers of the other layers. For example, directory servers are used as enablers for identity stores.

These nine technology agnostic requirements, mapped to SABSA layers identify that the continuous improvement of processes is needed for operational efficiency. As the SABSA framework is complex to understand, executives need to be presented with a more structured view of IAM. In this regard, a reference framework can assist an enterprise to understand how to identify the components of an IAM assurance dashboard by identifying core layers.

IAM assurance core layers: A large number of IAM frameworks have been proposed and applied by academia and vendors such as the new identity management architecture [16], the generic and complete three level identity management model [17], IBM [18] and Oracle Systems [19]. A review of frameworks reveal that three core layers need to be included in the IAM assurance dashboard as follows:

- *Processes, Procedures and Policies* need to be defined before technology components so that legal and regulatory requirements of an enterprise can be complied to.
- *Technology Frameworks* are used to implement processes procedures and policies by, e.g. Public Key Infrastructure (PKI) or a federation framework.
- *Governance and Monitoring* ensure continuous improvement and review of processes as technology advances and new threats emerge.

These core layers are shown to the right by Figure 1(e). To be able to define an IAM assurance dashboard, these three layers are refined in more detail by using the SABSA framework [12].

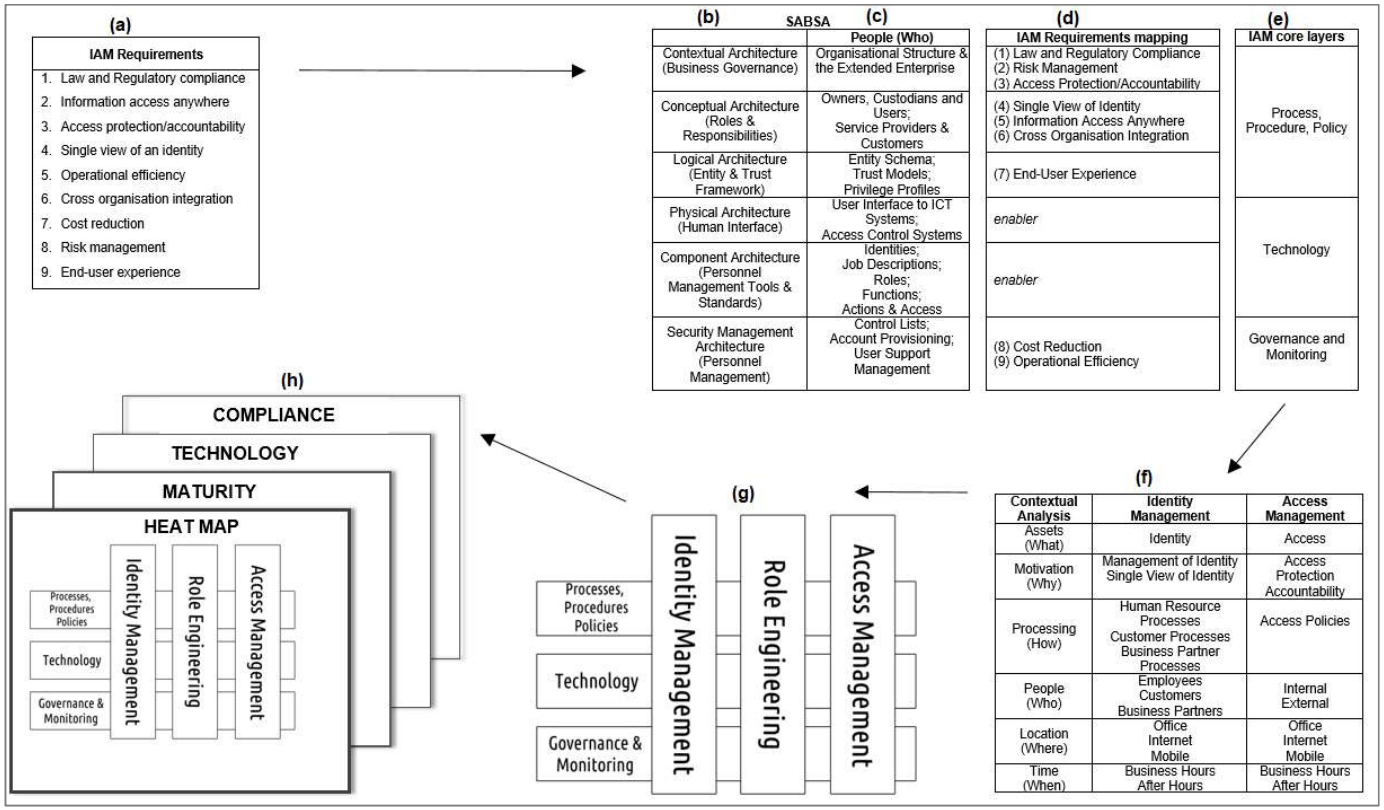

Fig. 1. IAM assurance dashboard component identification

The next steps aim to identify the components of the IAM assurance dashboard. First, SABSA layers and their related IAM requirements are organized according to the core layers; then the SABSA contextual layer is viewed in more detail as it focuses specifically on business requirements.

***Mapping IAM core layers to SABSA*:** Figure 1(e) shows how the layers of the SABSA model maps to the three core IAM layers. The *contextual, conceptual,* and *logical,* security architecture layers of the SABSA model map to the *processes, procedures and policies* IAM core layer as they all focus on general, business design activities. The selection of security products and the deployment environment is defined by the *component* and *physical* security architecture layers of SABSA and maps to the *technology* core IAM layer. Finally, the *security service management* architecture layer maps to the *governance and monitoring* layer. Key features of this layer are system operations and service management which must be considered when defining processes, procedures and policies or selecting technology components [14]. The resulting layers are shown horizontally in Figure 1(g) as the foundation for the IAM assurance dashboard model, containing the nine IAM requirements

SABSA contextual layer supporting IAM requirements: To complete the analysis of the SABSA model to identify IAM assurance dashboard components, the contextual security architecture layer shown first in Figure 1(b), is now viewed horizontally in more detail as its specific focus is to assist with the refinement of business requirements. To gain an understanding of IAM requirements from a business view for both identity management and access management, the six *what, why, how, who, where* and *when* questions are shown in Figure 1(f). Identity management describes the life-cycle of an identity (what), by considering the sources from which an identity is defined to be able to validate the identity (why). The identity is managed by stakeholders such as human resources divisions and business partners (how) and can be customers or employees (who). Identity may be accessed at the office or from distant locations (where) and at different times (when). Similarly, access management business requirements focus on the resources (what) an identity (who) want to access. Authorisation defines the level to which an identity has access (who). Lastly different mechanisms of authentication can be presented to users such as user name and password or biometric authentication (how).

IAM assurance dashboard initial design: An initial high-level design of the IAM assurance dashboard model is shown in Figure 1(g). Horizontally, the three core layers are shown where the *processes, procedures and policies* layer is defined by business owners. The *technology frameworks* layer is designed by system designers and *governance and monitoring* is designed by audit and operations owners to ensure that the implemented frameworks and processes, procedures and policies function as specified. Within each of these layers lie the nine IAM requirements to enable executive to use the IAM assurance dashboard to determine whether business requirements are being met.

Extrapolated vertically over the core layers are three domains, derived from Figure 1(f). *Identity Management* defines both standard, federated, and cross enterprise identity management. *Access Management* supports both standard mechanisms, and fine grained access control mechanisms that enforce more specific access control rules. Finally, *Role Engineering* is introduced to ensure that identity and access management data are associated via the analysis of enterprise structures, resulting in the definition of roles for access assignment. Each of these three horizontal domains are realised by a variety of components found across the IAM core layers. For example, technology components such as directory services and token infrastructure realise processes, procedures and policies components such as identity management processes, which in turn can be monitored by components such as audit and logging to ensure governance and compliance.

Next, the final phase of the development of the IAM assurance dashboard model is presented.

IAM assurance dashboard component dimensions: To provide a more detailed view of a component, the IAM assurance dashboard model is further refined by considering four evaluation dimensions as shown in Figure 1(h). The first dimension that is of primary interest to executives is the *heat map* that supports a self-assessment by the enterprise to determine its IAM health and hotspots for investment and focus. The *maturity* dimension measures the enterprise against best practices to rate its level of compliance so that areas can be identified to improve. The *technology portfolio* dimension provides a view of the technology supporting the IAM environment. Finally, the *compliance coverage* dimension provides information on the current status of compliance with regulations, based on audit requirements. Areas are highlighted that may result in penalties to the enterprise.

4 IAM assurance dashboard implementation

An implementation of the *heat map* dimension of the IAM assurance dashboard model is shown in Figure 2, as it would be displayed on a mobile device such as a tablet. The components that define the IAM assurance dashboard model are found at the intersection of three domains (vertical) and three layers (horizontal) as shown in Figure 2. The dashboard provides a consolidated view of evaluations performed for each component. The design of the IAM assurance dashboard model is complex and both the visual design requirements as well as the presentation of evaluation components needs to be carefully considered.

The visual design requirements of the IAM assurance dashboard is supported by the six principles of world-class information technology balanced scorecards requirements defined by DeLooze [20] A simple presentation is required with an overall view of IAM assurance on a single page that is aligned with enterprises' IAM implementation strategies and goals. The focus of the dashboard is on the executive level, displaying relevant assumptions and metrics for their evaluation. Evaluation metrics must be well

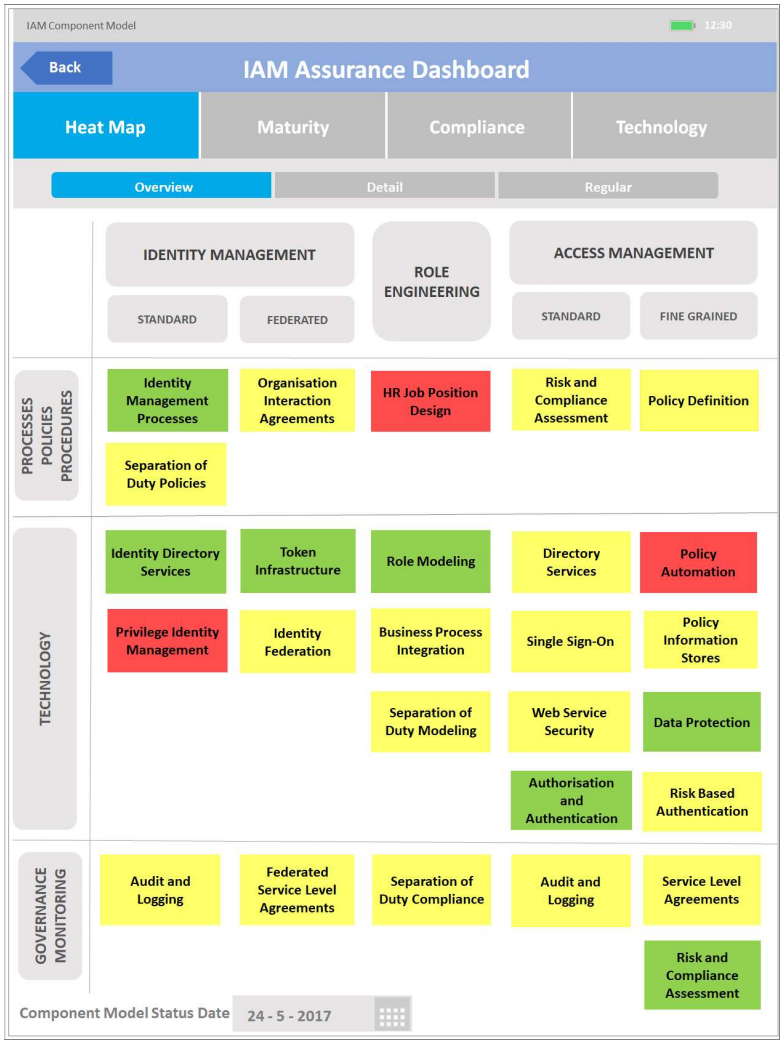

Fig. 2. IAM assurance dashboard heat map

defined and measurable supporting continuous feedback and review. Drill-down capabilities are needed to view the underlying metrics that provided the evaluation result, and ownership and results must be linked to the IAM leadership team.

The presentation of each evaluation component such as *Identity Management Processes* is addressed by considering a general classification of models described by Sharma [21] that provides a reference that can be applied when defining component attributes. In general, components should have a *purpose* such as showing alternative strategies or actions, giving a view on alternatives based on input criteria, or providing an evaluation

is based on best practices. The *degree of certainty of results* can be either deterministic where all properties can be determined or probabilistic where results are based on prediction and experience. A *time reference* provides either static results for a specific point in time or dynamic results that are created continuously. Some results may have to be presented with a degree of generality to stakeholders such as executives or to experts. Finally, *results can be presented* either qualitatively as written text or quantitatively as statistical, heuristic or simulation results.

For example, Figure 3 provides a view of how a specific component such as the as *Identity Management Processes* is presented in detail when executives drill down into it. The detail view of the *Identity Management Processes* component presents the results based on an evaluation of the enterprise's current status against the best practices baseline. The degree of certainty is deterministic, as all properties of the component are known and can be evaluated. Although the evaluation of the IAM assurance dashboard model is continuous, the result time reference is static, a point in time snapshot that can be used as input to decision making. Detailed information is presented for analysis. Finally, the results are quantitative in nature, as a heuristic approach is used for evaluation.

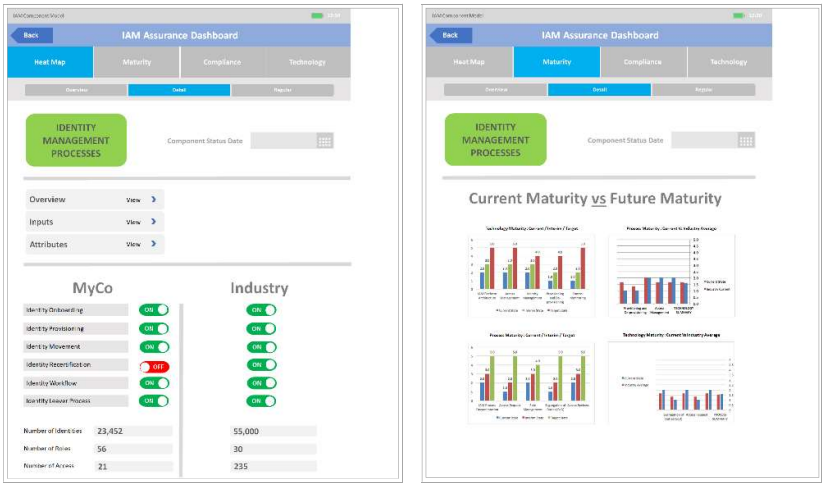

Fig. 3. IAM assurance dashboard detail and maturity

As seen in Figure 2, there are many independent components with potentially overlapping functions. For example, Privileged identity management and directory services are two components, shown to the bottom left of the heat map in Figure 2, within the technology layer. Both components can measure an integrated directory service. Although directory services may be evaluated as not sufficient, the directory services element of privileged identity management can comply with the evaluation criteria, making the duplication this evaluation relevant.

5 Conclusion

The purpose of the IAM assurance dashboard model aids decision makers in meeting the nine IAM requirements. In this regard, the *compliance dimension* of the IAM assurance dashboard model shows executives where the enterprise is not complying with the law and regulatory requirements. Specific actions can be put in place and monitored via the dashboard to ensure effort is made to gain compliance status. Compliance reviews assist with risk management whereby components with a non-compliant status can provide input into risk mitigation plans and resolution actions.

The information access boundary is expanding beyond the enterprises traditional delimitations, allowing enterprises to provide information access anywhere. The *heat map dimension*, and specifically the federation sub-domain as part of the identity management domain provide insights in the readiness and capability to provide service to both internal and external entities for cross enterprise integration. Increased cyber-attacks are forcing enterprises to protect and monitor access to information technology resources. More and more regulations require enterprises to proof that measures are in place to protect user information as well as who accessed user information when. The governance layer components on both the *heat map dimension* as well as the *technology dimension* provides insights into the capability of the enterprise to ensure access protection/accountability.

The identity management directory services component specifically provides a view to the goal of having a single view of an identity requirement. The maturity dimension provides a mechanism to evaluate the level maturity of this requirement with a mature level indicating a true single view of the identity.

The *technology dimension* of the IAM assurance dashboard provides a platform for operations teams to present hot spots where issues are experienced as well as motivate investment cases to implement processes and technologies to solve burning issues. The dashboard can assist with the business case to increase operational efficiency as it would show problem areas on the heat map, compliance requirements, current and future maturity state and lastly the technology that supports the component. These views also lend itself to limiting unnecessary spending and ensuring cost reduction as proposals for technology purchases can be evaluated based on the views presented.

The goal of the IAM assurance dashboard is to continuously improve components in the domains. The result leads to visible compliance results, motivation and business case development, and ultimately a streamlined end-user experience. Future research aims to define the sources that determine each component and how they are evaluated, to be able to implement a proof of concept prototype.

6 References

1. Osmanoglu. E. (2014). Identity and Access Management: Business Performance Through Connected Intelligence. Syngress
2. Bertino E and Takahashi K, (2011) Identity management:concepts, technologies, and systems, Artech House

3. Ng, A C K. (2018), Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities, IGI Global, ISBN13: 9781522548287
4. Moeller R. (2011) COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance, Second Edition. John Wiley & Sons
5. Scheidel J. (2010) Designing an IAM Framework with Oracle Identity and Access Management Suite, Oracle Press
6. Ritchot, B., (2013) An Enterprise Security Program and Architecture to Support Business Drivers. Technology Innovation Management Review, 3(8)
7. Scully, T., (2014). The cyber security threat stops in the boardroom. Journal of business continuity & emergency planning, 7(2), pp.138-148
8. Spears, J.L., Barki, H. and Barton, R. R.,(2013) Theorizing the concept and role of assurance in information systems security. Information & management, 50(7), p.598-605
9. Macehiter N. (2006) A Confusing Array of Identity Management Pressures and Initiatives. What Drives Identity Management Requirements? Macehiter Ward-Dutton Limited
10. Sharman R, Smith S and Gupta M, (2012) Digital Identity and Access Management: Technologies and Frameworks. IGI Global
11. Tipton H, and Krause M. (2007) Information Security Management Handbook, Sixth Edition, Volume 1, Auerbach Publications
12. Damon, F. and Coetzee, M., (2013), Towards a generic Identity and Access Assurance model by component analysis-A conceptual review. In Enterprise Systems Conference (ES), 2013 (pp. 1-11). IEEE
13. Sarbanes, P., (2002) Sarbanes-Oxley Act of 2002. In The Public Company Accounting Reform and Investor Protection Act. Washington DC: US Congress
14. Burkett, J.S., (2012) Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. Information Security Journal: A Global Perspective, 21(1), pp.47-54
15. Calder, A. and Watkins, S., (2008). IT governance: A manager's guide to data security and ISO 27001/ISO 27002. Kogan Page Ltd
16. White P. (2008) Identity Management Architecture: a new direction, in 8th IEEE International Conference on Computer and Information Technology, pp. 408-413
17. Dabrowski M, Pacyna P. (2008) Generic and Complete Three-Level Identity Management Model. Proceedings of 2nd International Conference on Emerging Security Information, Systems and Technologies, 2008, pp. 232 237
18. Buecker A (2011) Introducing the IBM Security Framework and IBM Security
19. Jellema L (2011), Oracle SOA Suite 11g Handbook, Oracle Press
20. DeLooze L. L. (2006), Creating a Balanced Scorecard for Computer Security, IEEE Information Assurance Workshop, West Point, NY, 2006, pp. 15-18
21. Sharma J. K. (2014), Quantitative Techniques in Management, Third Edition, Laxmi Publications, 2014