An Overview of Access Control Practices: Guidance from ITIL, COBIT 5 and ISO/IEC 27002

L. Tekeni; R. Botha; and K. Thomson
School of Information and Communication Technology
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
E-mail: {Luzuko.Tekeni;ReinhardtA.Botha;Kerry-Lynn.Thomson}@nmmu.ac.za

Abstract

Access control is one of the oldest aspects of information security. Several IT (Information Technology) best practices, guidelines, frameworks and standards discuss access control. Although these documents discuss very similar concepts, not all of the access control issues are discussed at the same level of detail. Therefore the purpose of this paper is to provide a holistic view of access control as described by the major IT best practices, management frameworks and standards. The ITIL (Information Technology Infrastructure Library) lifecycle access management activities are used as a framework. Further, the access control views from COBIT 5 (Control Objectives for Information and Related Technology) and ISO/IEC 27002 (International Organization for Standardization) are integrated into this framework.

Introduction

Information security is important to any organization. Organizational processes, networks and systems are valuable assets (ISO/IEC27002, 2013); therefore they need to be protected. Organizations need to ensure that their security is effective and adequate at all times (Saint-Germain, 2005). Access control is one of the oldest aspects of information security in an organization. Its main purpose is to manage the provision of user access rights to ensure that resources can be appropriately shared between properly authenticated users. Consider an example of access control decision making as illustrated in Figure 1.

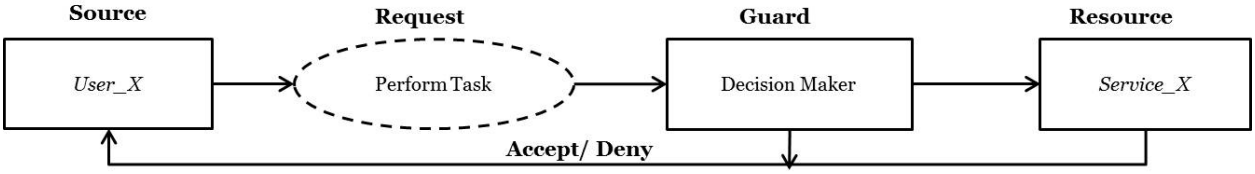

Figure 1: Access control decision making (based on Lampson, Abadi, Burrows, & Wobber, 1992)

In Figure 1 the `Source' (User X) requests access from the `Guard' (Decision Maker) to perform a specific task on a particular `Resource' (Service X). In order to make a decision the `Guard' needs to know the `Source' of the request to determine the identity. This is called authentication. Furthermore, the `Guard' must also verify the access rules associated with the required `Resource' by the `Source'. This is called authorization (Lampson et al., 1992). Therefore, once the `Guard' completes authentication (Who is accessing?) and authorization (What can be accessed?), the decision is made to either `Accept' or `Deny' the required `Resource'.

However this happens when the user attempts to access a particular resource: thus a *run-time* decision. Furthermore, this decision is based on a set of access rules which must be created first. Therefore, there is also an *administration-time* activity of setting up those access rules. Considering administration of access control separately from the operational access control to ensure that the policies and objectives are not

compromised is not a new idea (Sandhu, Bhamidipati, & Munawer, 1999). We, therefore, must consider the activities both from a *run-time* and *administration-time* perspective.

As can be expected access control to information systems has been discussed by many, including in IT best practices, management frameworks and standards. Among these, the most commonly used are ITIL (OGC, 2007), COBIT5 (ISACA, 2013) and ISO/IEC 27002 (ISO/IEC27002, 2013). Although ITIL is considered as best practice guidelines, COBIT 5 as a management framework, and ISO/IEC 27002 as a standard, we will collectively refer to them as frameworks. While all these frameworks discuss access control, each discusses issues from a unique perspective. However, not all of the access control issues are discussed at the same level of detail. Hence, this paper provides a holistic view of access control practices by integrating the views from ITIL, COBIT 5 and ISO/IEC 27002. The ITIL lifecycle access management activities are used as a framework to structure the discussion around the access control lifecycle.

Firstly, this paper introduces ITIL, COBIT 5 and ISO/IEC 27002. Secondly, an approach that will be used through the analysis of access control views is provided, along with the ITIL lifecycle access management activities. Furthermore, the access control views found from COBIT 5 and ISO/IEC 27002 are integrated into the ITIL lifecycle access management activities. Thereafter, the main access control themes found from these three frameworks are discussed. Finally, remarks and the conclusion of the paper are stated.

Introducing ITIL, COBIT 5 and ISO/IEC 27002

Many organizations are under pressure to control access to their business systems and services. Organizations should use IT best practices, guidelines, frameworks and standards as guidance when implementing access control. ITIL, COBIT 5 and ISO/IEC 27002 all discuss the concept of access control. However access control views are scattered through the frameworks. This could make it challenging to use them during access control implementation.

Much research has been done in an attempt to integrate them (Sahibudin, Shari, & Ayat, 2008). Furthermore, the access control issues are not discussed at the same level of detail. To understand the differences, think of these three in this way: COBIT 5 discusses what to monitor and control, ITIL clarifies how to go about implementing the processes for performing that, while ISO/IEC 27002 discusses the process for securing those services (Greenfield, 2007). As the focus of this paper is the analysis of access control views within ITIL, COBIT5, and ISO/IEC 27002, the following subsections focus not only on an overview of these frameworks, but also provides a direction with which the information concerning access control views can be located within them.

ITIL

Information Technology Infrastructure Library (ITIL) is a best practice guidelines introduced by the Office of Government Commerce (OGC) situated in the United Kingdom (UK), to provide best practices for IT service management in an organization (Nastase, Nastase, & Ionescu, 2009). This framework discusses issues related to different entities such as “people, processes and infrastructure technology”, to provide cost effective and high-quality IT services (OGC, 2007). ITIL comprises of five publications, namely (Verma, 2014): Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

Service Strategy discusses the concept of identifying market opportunities for new services, while Service Design is concerned with developing a strategy into a designed document (Greenfield, 2007). On the other hand, Service Transition deals with the implementation of the activities laid down by the Service Design and Service Operation focuses on the operational side to ensure that services are delivered. Furthermore, Continual Service Improvement provides consistence between the other four publications. It focuses on how the service can be improved over time (Verma, 2014).

In ITIL, the access management process is described in the Service Operation publication. Views are clearly defined in the access management section (4.5) as lifecycle activities.

COBIT 5

COBIT 5 is a management framework developed by ISACA (Information Systems Audit and Control Association) for IT governance and IT management (Sahibudin et al., 2008). This framework defines 34 control objectives in a hierarchy of processes and domains (Ridley, Young, & Carroll, 2004). These processes are subdivided into four domains: Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Evaluate, Direct and Monitor (EDM) (Greenfield, 2007). Under each domain, the process objectives, key activities, input, output, performance measures, Work Product (WP) and Best Practice (BP) are discussed.

There is no specific section that discusses access control views in this management framework. However, access control views could be found in any of the four domains mentioned above. During the integration of access control views in COBIT 5, the Deliver and Support domain discuss more access control views than the other domains.

ISO/IEC 27002

This is an information security standard introduced by International Organization for Standardization (ISO) and by the International Electro-technical Commission (IEC) for information security management (Sahibudin et al., 2008). The main purpose of this standard is to provide guidelines and general principles for "initiating, implementing, maintaining and improving information security management in an organization" (ISO/IEC27002, 2013). The three areas of information security, Confidentiality, Integrity and Availability, are covered in this standard. Furthermore, the standard contains 14 security control clauses in which access control is included (ISO/IEC27002, 2013). Each of these 14 clauses defines a number of main security categories in them.

Although access control views are primarily found in section 9 under the access control clause, other sections also make references to access control related views.

Table 1 below highlights key differences and similarities between these frameworks.

Table 1: Differences and Similarities between ITIL, COBIT 5 and ISO/IEC 27002

Parameters	**ITIL**	**COBIT 5**	**ISO/IEC 27002**
Purpose	IT Service Management	IT Governance	Information Security Controls
Created by	OGC	ISSACA	ISO/IEC
Targeting	Lifecycle of IT Services	34 Processes and 4 Domains	14 Security Control Clauses
Access control details	SOP: Access Management	Within those 4 Domains	Section 9: Access Control

Next consider how we analysed these frameworks.

Analysis Approach

As pointed out earlier, access control must be considered from both an *administration-time* and a *run-time* perspective. Clearly access control is not a once-off activity, but requires administration to be done from time to time, and the actual access control decision is made every time an attempt to access a resource is made. This nature of access control is best acknowledged by ITIL which view access management activities as part of a lifecycle. We therefore decided that structuring our analysis according to the ITIL access management activities will ensure a holistic view.

Figure 2 conceptually positions the access management activities identified by ITIL in terms of *administration-time* and *run-time* perspectives.

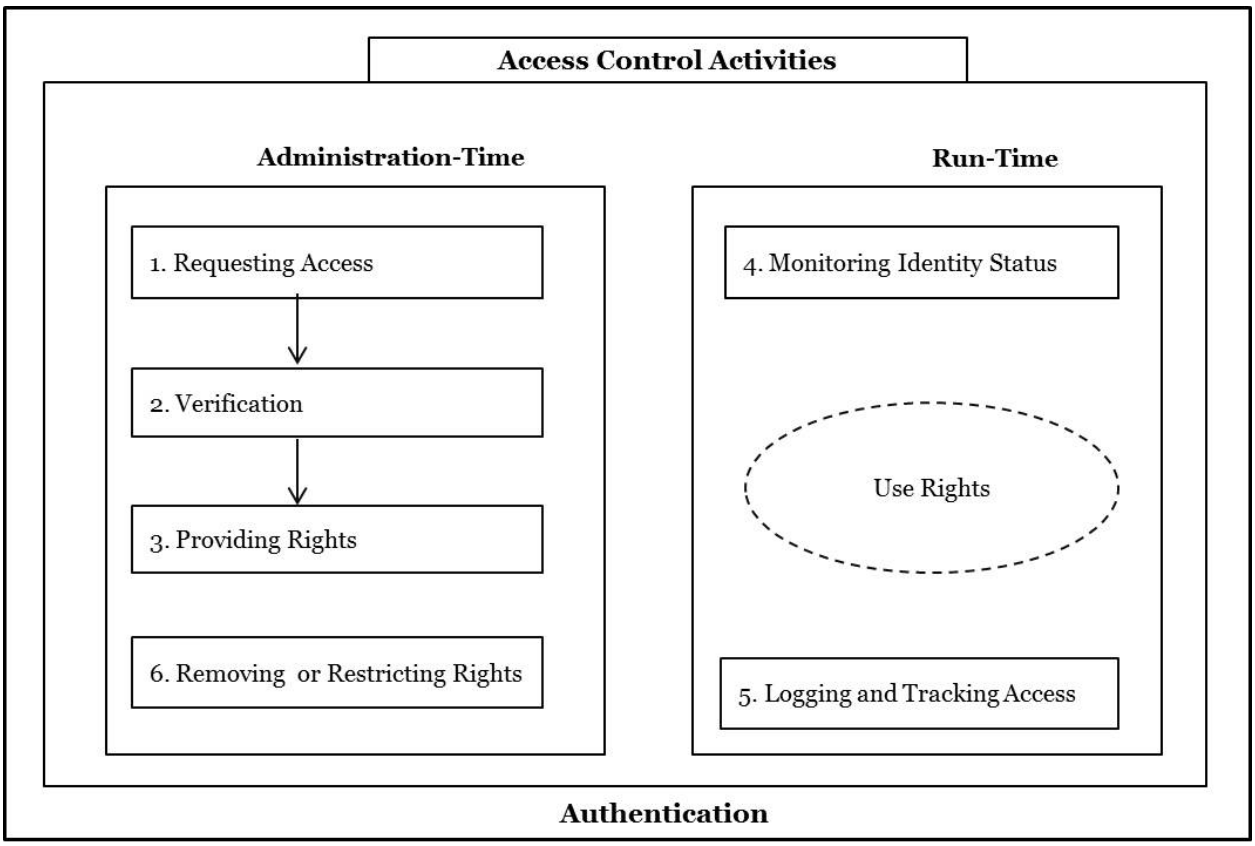

Figure 2: Activities for Access Control Analysis

The first three activities, namely, 'Requesting Access', 'Verification', and 'Providing Rights', ensure that users will receive the access rights they require. The 'Monitoring Identity Status' and 'Logging and Tracking Access' activities continually takes place to ensure that access rights reflect the business requirements and are not misused. Anomalies and changes to business requirements may in turn trigger some of the administration-time activities. Finally, the 'Removing or Restricting Rights' activity ends the lifecycle of the access rights.

Access Control Analysis

This section looks at what guidance is available regarding access control views by using ITIL lifecycle access management activities as a framework. The discussion integrates material from ITIL (OGC, 2007), COBIT 5 (ISACA, 2013) and ISO/IEC 27002 (ISO/IEC27002, 2013). In order to facilitate easier integration of the views, the following cross-referencing mechanisms are used:

- For ITIL specific concepts, the reference would indicate the ITIL lifecycle and the relevant section in the lifecycle documentation. For example, (SOP, 11.4) refers to Service Operation Processes section 11.4.

- For COBIT 5 specific concepts, the reference would indicate the framework and the process number. For example, (COBIT 5, BAI06-BP1). The references will use the acronyms introduced in section 2.

- For ISO/IEC 27002 specific concepts, the reference would indicate the standard and relevant section in the documentation. For example, (ISO/IEC27002, 8.1).

- Where a statement relates to more than one document the reference would be combined, separated by a semi-colon.

Activity 1: Requesting access

The first step towards gaining access to resources is requesting access. Users (Employees, Contractors and Visitors) could request access to a specific service or a set of services. These requests may originate from different sources. ITIL (SOP, 4.5) identifies four sources, namely HR (Human Resource) Management, a Service Request by the user, RFC (Request for Change), and a request from the Manager. Whenever someone is hired HR is required to initiate a request. The request is based on the user's business job requirements and access policies of the organization (IS0/IEC 27002, 9.2.2). The HR department must verify the user's identity and should ensure that his/her job requires the services being requested. To accomplish such a goal the request should be automated. In other words, HR systems for allowing access to information systems and services should be in place prior to employment (ISO/IEC 27002, 9.2.1).

This applies to the current services, but when there is a new service being deployed in the organization, the RFC will initiate the request. Such requests could happen when there are large upgrades to the system that affect a large number of user access rights within a particular group of users (SOP, 4.5.6). It is thus imperative that the change management processes consider the impact of user access.

General service requests, which may also include requests to access a service/system, are handled by the IT service desk. Such service requests should be classified and prioritized in order to assess the risks they might pose to the organizational processes and services (COBIT 5, DSS02-BP1). These requests must be recorded as they could help in future investigations (ISO/IEC 27002, 12.4). Some requests may not come from the user, but could originate from the manager of a particular department. This could happen when the manager assigns an internal user to perform a task that requires more access rights than currently available to that user. The request will then be channelled via the service desk.

Once a request is received, the next step is to verify that the user is who he/she claims to be and that he/she really needs the access. The next activity will discuss the verification process.

Activity 2: Verification

Verification according to ITIL is an administration-time activity that follows requests for access. It involves two actions. Firstly, the requester must be authenticated to ensure that he/she is who he/she claims to be (SOP, 4.5.5.2). Secondly, it must be ensured that he/she really needs the service (COBIT 5, DSS05-WP6). The process is illustrated in Figure 3.

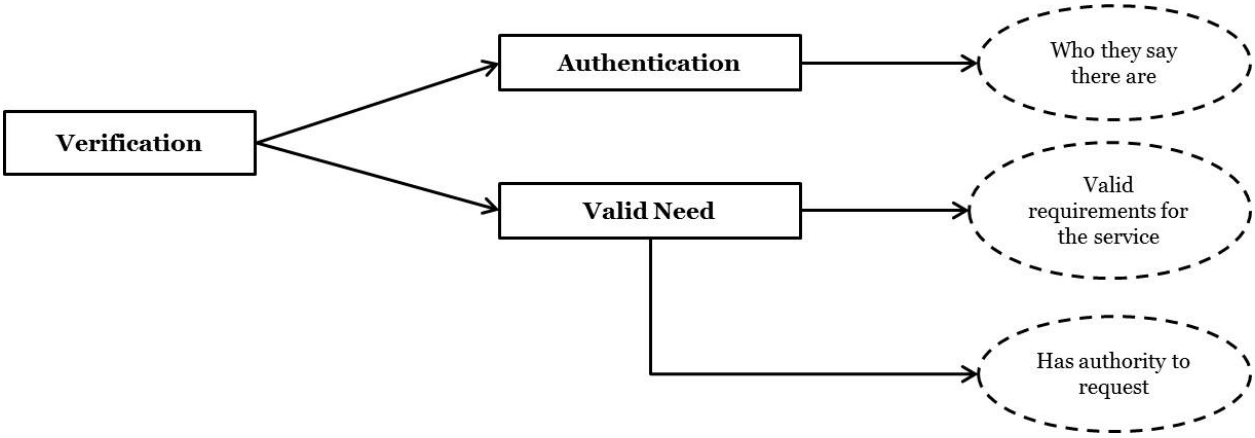

Figure 3: The Verification Process Activity

Sometimes the need might be validated from the fact that the requester is not the grantee, and that the requester has the authority to request this. Other times, if the requester is the grantee, logical mechanism such as usernames and passwords might not be sufficient. In that case physical mechanisms such as a user visiting the Service Desk with a suitable identification document may be required. However, for an indirect request, where a manager might request access for his/her users, a username and a password might still be acceptable as this is really just an execution of the manager's rights to request access.

Where the access request deals with sensitive services other verification mechanisms such as hardware tokens (e.g. smart cards) and biometrics (e.g. fingerprints or signatures) (SOP, 4.5.5.2), may be required.

Once the request has been verified the user could be provided the access rights required. This is further discussed in the next activity.

Activity 3: Providing rights

As soon as the verification process is complete the user is eligible to be given access rights in order to perform his/her day-to-day activities (ISO/IEC 27002, 9.2.2). Access rights are provided according to the user's job requirements and should be used for business purposes (COBIT 5, DSS06-02). One of the challenges in providing access rights arises when the user holds multiple access rights for different tasks. These multiple access rights could conflict with one another (SOP, 4.5.5.3). For example, a user needs to log the total number of hours worked per day for the purpose of calculating the salary earned (Task 1). However, Task 2 requires the user to approve the number of hours logged. This could be seen as a potential conflict or conflict of interest. However, such conflict can be avoided by carefully designing roles (SOP, 4.5.5.3).

At present most organizations are implementing the concepts of role-based access control when providing access rights to users (Bao, Song, Wang, Shen, & Yu, 2008). Role-based access control provides two steps: firstly, mapping roles to access rights and secondly, mapping users to their roles (Zhou, Varadharajan, & Hitchens, 2012) as depicted in Figure 4.

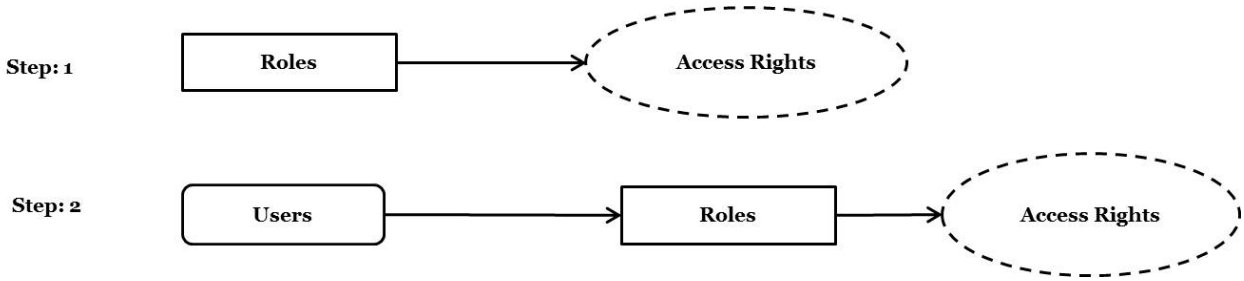

Figure 4: Role-Based Access Control Mappings

This makes the provision of access rights much simpler than providing each user access rights that are not mapped to a particular role. Since the user might have two or more roles assigned to him/her, each of the roles assigned should be recorded and documented (COBIT 5, DSS05; ISO/IEC, 9.2.2).

Activity 4: Monitoring identity status

In the previous activity users were mapped to their roles according to their business needs and requirements. As users continue in these roles changes to the roles may be required, and changes to access rights might arise (SOP, 4.5.5.4). It then becomes challenging to monitor the user's identity status or changes. Access control should cater for prevention of redundant user IDs and accounts (ISO/IEC 27002, 9.2.1), keep track of the date and time of changes, the type of change, the type of file accessed and also the program used to execute the change (COBIT 5,EDM03) when doing monitoring. The changes should be explicitly authorized by the appropriate authority prior being approved (ISO/IEC 27002, 12.1.1, 12.1.2).

A change could be triggered by the user changing his/her password. In this case automated tools could be useful to monitor such a change and automatically update the involved database or systems. Of course these changes could be legitimate or illegitimate. If the change is legitimate the records on the database will show that the user is actually active on the system. Whereas if the change is illegitimate, the database probably needs to integrate with intrusion detection tools which will lookout for passwords changing at the same time or odd patterns in passwords.

Today most organizations use tools, such as intrusion detection tools (COBIT 5, DSS05-BP7), to monitor their systems (Vigna, Gwalani, Srinivasan, Belding-Royer, & Kemmerer, 2004). Although changing the password of the user could be seen as minor, "big" changes such as job changes, promotions or demotions, transfers, resignation or death, dismissals, disciplinary action, and retirement (SOP, 4.5.5.4) can be challenging to monitor if automated tools are not in place.

It is of interest to discuss disciplinary action and dismissals. These might bring harm to the organization's valuable assets due to user's behaviour during the disciplinary action or dismissal period. In serious cases of misconduct, user access rights, duties and privileges should be temporarily suspended (ITIL: SOP, 4.5.5.4; ISO/IEC 27002, 7.2.3) and if necessary, he/she can be escorted off the organizational premises. Similarly, during suspension, all access should be restricted until the employee is ready to resume duties. And again, automated tools should be in place to re-activate the access rights revoked when appropriate.

Activity 5: Logging and tracking access

Threats originate not only from the outside world, but internal users can initiate threats unintentionally if policies are not followed. Users could breach the policies or misuse the organization's resources (SOP, 4.5.5.5). However, this can be minimized by implementing intrusion detection tools for tracking and logging user activities (ISO/IEC 27002, 12.4.1; COBIT 5, DSS05-BP7; ITIL: SOP, 4.5.5.5). When the user is suspected of resource misuse the logged files could help to speed up the investigation process (IS0/IEC 27002, 12.4.1; COBIT 5, DSS05-WP9). Even when there is a change in a user's identity or role, the change needs to be logged and be kept for the minimum duration period specified by the organization's security policies (ISO/IEC 27002, 9.2.5).

Access control should not only track unauthorized user access activities, but also track authorized user activities (ISO/IEC 27002, 19.2.5). A user can be given access rights to execute a task but never uses them. This could bring harm to the organization. For example, if a user has legitimate access rights and chose not use them, the access rights get compromised by the third party. This introduces vulnerability to other organizational systems unnecessarily. This activity is also accountable for making sure that the user access rights that were provided in activity 3 are properly used for their purpose. Clearly this activity should also be utilized when there is a change within the organization and those changes must be logged at all times.

Activity 6: Removing or restricting rights

Activity 3 discussed the concept of providing access rights to users. This activity is responsible for revoking those rights whenever the need arises. The process of removing or revoking access rights can take place when the user is dismissed, dies or resigns (ISO/IEC 27002, 7.2.3; SOP, 4.5.5.6). Removing rights needs to be performed in a timely manner to prevent unauthorized access by the dismissed user. Having the user de-registration procedures in place (ISO/IEC 27002, 9.2.1), which should be developed by information security management, could speed up the process.

The removal of the access rights process does not mean the user access rights should be completely erased as these could be needed again. Rather, the access rights should be deactivated. The same for restricting access rights to the user. Restricting access rights could be triggered when the user has changed roles, is under the disciplinary process or is on temporary leave for a short period of time (COBIT 5, APO07; ITIL: SOP, 4.5.5.6; ISO/IEC 27002, 7.2.3). However, a record of access rights should still be kept until the user is ready to resume his/her duties (COBIT 5, EDM03).

Discussion

The previous section identified six ITIL lifecycle access management activities and used them as a framework when integrating access control views found in ITIL, COBIT 5 and ISO/IEC 27002. This section serves to uncover the main access control themes found in these frameworks as discussed in section 2. Each of the six ITIL lifecycle access management activities are illustrated in Table 2 to highlight these main access control themes.

In Table 2, if minimal information is provided in a framework regarding a chosen theme, the (✓) will be shown. Furthermore, the (✓✓) shows that the framework has detailed information regarding the chosen theme. If the table entry is empty, there is no information contained in a framework for the chosen theme.

Table 2: A Summary of access control themes from COBIT 5, ITIL and ISO/IEC 27002

ITIL Activities	Access Control Themes	COBIT 5	ITIL	ISO/IEC 27002
Requesting Access	Automate access requests		✓✓	✓✓
	Classifying and prioritizing requests	✓✓		
	Record and document access requests	✓	✓✓	✓✓
	Originating sources of requesting access		✓✓	✓
Verification	Authentication	✓	✓✓	✓✓
	Verifying business needs		✓✓	✓✓
Providing Rights	Designing of roles		✓✓	✓✓
	Record and document roles		✓✓	✓✓
Monitoring Identity Status	Changes to access rights		✓✓	✓✓
	Intrusion detection tools	✓✓	✓✓	✓
	Prevention of redundant user IDs			✓✓
Logging and Tracking Access	Log files	✓	✓✓	✓✓
	Intrusion detection tools	✓✓	✓✓	✓✓
	Proper use of access rights	✓✓	✓✓	✓
Removing and Restricting access	Resignations		✓✓	✓✓
	Suspensions	✓	✓✓	✓✓
	Dismissals	✓	✓✓	✓✓

As can be seen in Table 2, many similarities exist between ITIL and ISO/IEC 27002. Where ITIL provides detailed information regarding a theme, similar detailed information is often provided in ISO/IEC 27002. For example, as can be seen in Table 2, both ITIL and ISO/IEC 27002 discuss the theme of 'Automate access requests' and that these requests should be recorded and documented at all times. The same applies to 'Verification' and 'Providing Rights' activities where 'Authentication' and 'Designing of roles' are also discussed. Similarly, when no information is provided for a theme in ITIL, no information is provided in ISO/IEC 27002 most of the time. For example, 'Classifying and prioritizing requests' is not detailed in either ITIL or ISO/IEC 27002. However, it is not always the case that information provided by ITIL is also provided by ISO/IEC 27002. For example, as shown in Table 2, ISO/IEC 27002 discusses the theme of 'Prevention of redundant user IDs' while ITIL does not.

Conversely, COBIT 5 addresses some of the themes which are not discussed in either ITIL or ISO/IEC 27002. For example, as shown in Table 2, the theme of `Classifying and prioritizing requests' under the 'Requesting access' activity is discussed by COBIT 5 but not by ITIL or ISO/IEC 27002. Where ITIL and ISO/IEC 27002 discuss a theme, COBIT 5 does not always provide information for that theme as can be seen from Table 2. For example, Table 2 highlights that information is not provided by COBIT 5 for certain themes such as 'Designing of roles' and 'Record and document roles' under the theme of 'Providing Rights'. Therefore, it can be determined that COBIT 5 is not as detailed as ITIL and ISO/IEC 27002 in terms of access control.

Based on this discussion, it can be argued that a combination of ITIL, COBIT 5 and ISO/IEC 27002 gives a more comprehensive view of access control as themes that are not covered in one framework or standard are covered by another framework or standard.

Conclusion

Access control is a critical feature in any organization, as valuable assets must be protected. This paper has shown that access control is well established, as it is discussed in ITIL, COBIT 5 and ISO/IEC 27002. However, not all of the access control issues are discussed in the same level of detail. No framework should be used in isolation when implementing access control in organizations. Therefore, it can be argued that a combination of ITIL, COBIT 5 and ISO/IEC 27002 gives a holistic view of access control as themes that are not detailed in one framework are detailed by another framework. Consider an abstracted holistic view of access control summary illustrated in Figure 5.

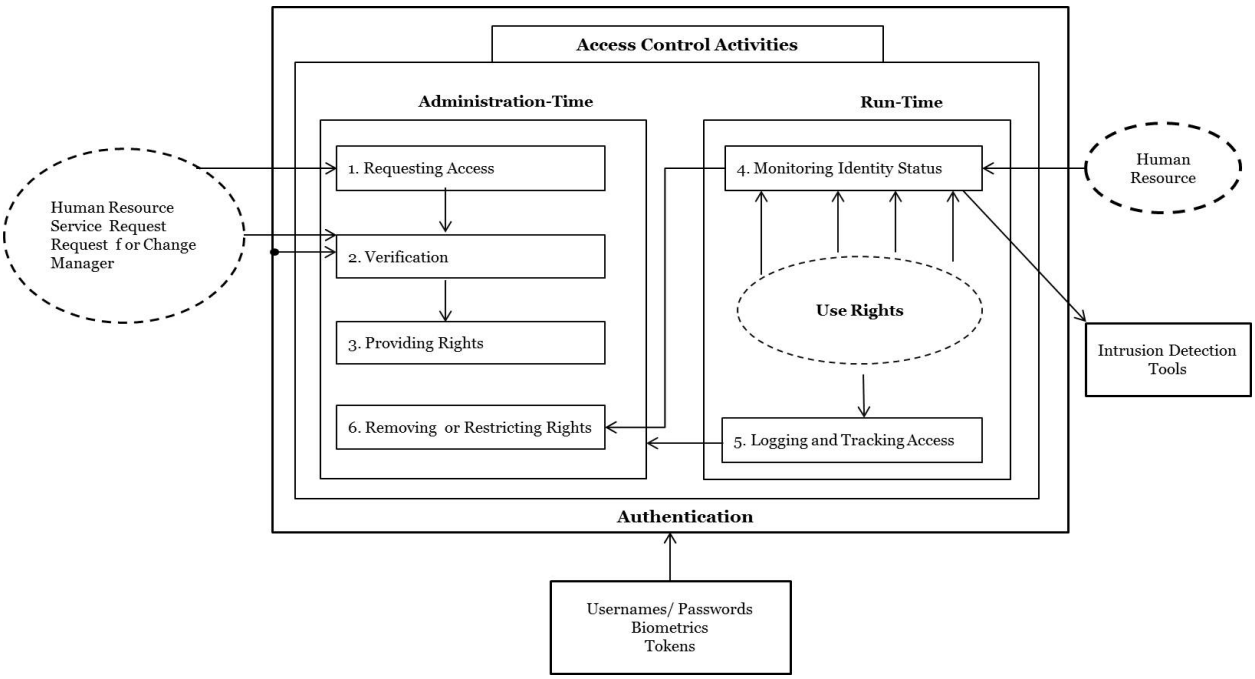

Figure 5: Summary: A holistic view of access control

In Figure 5, as previously mentioned, access requests might originate from any of the four sources identified by ITIL (SOP, 4.5). Thus the request needs to be authenticated and it must be verified that the request originating from the HR (for example), as illustrated by the three arrows pointing to the 'Verification' activity in Figure 5, before the required access rights are provided. Of course, the first three activities ensure that the requester will receive the access rights he/she requires (*administration*-time).

Whenever someone changes a job, resigns, retires, dies, is dismissed or is under the disciplinary process, the HR is notified. These needs to be monitored and necessary actions must be taken, as shown by the arrow from the 'Monitoring Identity Status' to the 'Removing or Restricting Rights' in Figure 5. These changes should be monitored using 'Intrusion Detection Tools' (*run-time*) as argued by COBIT 5 (COBIT 5, DSS05-BP7).

Further, the access rights provided should be tracked and logged as shown in Figure 5. Finally, the administrators of these access rights might need to look at the log files when performing some administration activities, as illustrated by the arrow between 'Logging and Tracking Access' and 'Removing or Restricting Rights' in Figure 5.

This paper could be useful for people involved with access control. The paper provided a holistic view of access control that has been built through analysing ITIL, COBIT 5 and ISO/IEC 27002. The integrated view frames access control in terms of the ITIL access management activities. Access control should not be a once-off effort, but a continuous one. Access rights should be managed across its lifecycle: access rules must be developed and requested (*administration-time*), used and the use monitored (*run-time*), and eventually revoked (*administration-time*). It is also important that access control does not stand alone, integration with organizational systems, such as the HR systems, as well as with other security services, such as authentication and intrusion detection services. Cross references in section 4 provides pointers to additional details regarding specific issues in the integrated view.

Acknowledgements: This work is based on the research supported in part by the South African National Research Network (SANReN).

References

Bao, Y., Song, J., Wang, D., Shen, D., & Yu, G. (2008). A role and context based access control model with UML. *The 9th International Conference for Young Computer Scientists* (pp. 1175-1180). Washington, DC, USA.

Greenfield, D. (2007). *ITIL, COBIT, and ISO 17799 provide a blueprint for managing IT services*. Retrieved 22 April 2015, from http://www.informationweek.com/standards-for-it governance/d/d-id/1062203?page number=1

ISACA. (2013). *COBIT 5 process assessment model (PAM)*

ISO/IEC27002. (2013). *Information technology - Security techniques - Code of practice for information security controls*. International Organization for Standardization/International Electronical Commission (ISO/IEC).

Lampson, B., Abadi, M., Burrows, M., & Wobber, E. (1992). Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems (TOCS)*, *10*(4), 265-310

Năstase, P., Năstase, F., & Ionescu, C. (2009). Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. *Economic Computation & Economic Cybernetics Studies & Research*, *43*(1), 16.

OGC. (2007). *ITIL: Service operation*. London: TSO (The Stationary Office).

Ridley, G., Young, J., & Carroll, P. (2004). COBIT and its Utilization: A framework from the literature. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences* (pp. 8-pp). Big Island, HI.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. *2008 Second Asia International Conference on Modeling & Simulation* (pp. 749-753). Kuala Lumpur, Malaysia

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60-66.

Sandhu, R., Bhamidipati, V., & Munawer, Q. (1999). The ARBAC97 model for role-based administration of roles. *ACM Transactions on Information and System Security (TISSEC)*, *2*(1), 105-135.

Verma, M. (2014). Comparison of IT governance framework: COBIT, ITIL and BS7799. Retrieved 19 April 2015, from http://www.slideshare.net/meghnaverma3956/comparison-of-it-governance-frameworkcobititil-ds?related=5

Vigna, G., Gwalan, S., Srinivasan, K., Belding-Royer, E. M., & Kemmerer, R. (2004). An intrusion detection tool for AODV-based ad hoc wireless networks. *20th Annual Computer Security Applications Conference* (pp. 16-27). Tucson, AZ.

Zhou, L., Varadharajan, V., & Hitchens, M. (2012). Trusted administration of large-scale cryptographic role-based access control systems. *11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 714-721). TBD Liverpool, United Kingdom.