CENTRIFY WHITE PAPER, JUNE 2013

Addressing Monetary Authority of Singapore (MAS) Internet Banking and Technology Risk Management Guidelines (IBTRMv3) through Centralised Identity and Access Management in Active Directory

Management of security risk in information and information technology covered in the MAS IBTRMv3 requirements

Abstract

The Monetary Authority of Singapore (MAS) lays out a comprehensive set of IT security requirements that are an ongoing focus for IT managers in banks in Singapore. In particular, the MAS guidelines for Internet Banking and Technology Risk Management (IBTRMv3) address security and risk management issues in a comprehensive manner, covering everything from identity assurance and access controls to accountability and audit. This White Paper details how Centrify Suite and Active Directory can address a large portion of security controls and risk management requirements addressed in MAS IBTRMv3. In addition, requirements related to monitoring of IT security controls as detailed in the guidelines are discussed in the context of the capabilities of Centrify DirectAudit. The White Paper demonstrates how to address these requirements in a robust and cost-effective manner by leveraging existing Active Directory infrastructure to centrally manage both Windows and, critically, non-Windows systems, applications and databases. It then details Centrify's unique ability to extend Active Directory with a suite of integrated solutions for cross-platform identity, access and privilege management and detailed user activity monitoring of UNIX, Linux and Windows systems.

Table of Contents

Introduction

MAS IBTRMv3 Definition of IT Security Risk

Per the MAS IBTRMv3[1]: As banks rely increasingly on information technology and the internet to operate their business and interact with the markets, their awareness and recognition of the magnitude and intensification of technology risks should correspondingly be more perceptive and discerning, both for individual banks and the financial industry as a whole. In this networked and market-driven environment, it is critical that banks have flexible, adaptable and responsive operating processes as well as sound and robust risk management systems.

The board of directors and management of a bank are responsible for managing its risks, including technology risks which are becoming more complex, dynamic and pervasive. The risk management process requires the board and management to review and appraise the cost-benefit issues on what and how much to invest in controls and security measures relating to computer systems, networks, data centres, operations and backup facilities.

The aim of the MAS IBTRMv3 set of guidelines is to require banks to adopt risk management principles and security practices which will assist them in:

- Establishing a sound and robust technology risk management framework.
- Strengthening system security, reliability, availability and recoverability.
- Deploying strong cryptography and authentication mechanisms to protect customer data and transactions.

All banks must erect a sound and robust risk management process that will enable them to identify, assess, measure and respond to technology risks in a proactive and effective manner.

MAS IBTRMv3 has thoughtfully detailed the requirements for information security risk management taking into account technical, operational and business audiences that must be part of a disciplined and effective IT risk management program. These requirements will not only make the task of compliance for MAS-regulated organisations easier but, are an overarching framework that will make compliance with other mandates and regulations like PCI DSS and SOX simpler as well. In addition, the MAS guidance fits well with organisations already following accepted standards such as COBIT, ISO and ITIL that help IT leaders establish and maintain control in their environments.

Centrify recognizes the multi-regulatory world financial organisations exist in and that current economic factors have increased the pressure to find cost-effective solutions that can leverage existing infrastructure and do not require additional infrastructure investment. This has also led to a new focus on standards-based solutions that can be deployed uniformly within organisations, and can deploy across on-premise, private and public cloud resources. Such solutions must be simple to deploy, easy to manage, and help IS managers streamline operations while at the same time offering a sophisticated degree of control over a complex environment of heterogeneous systems applications and databases.

Centrify solutions broadly support the requirements detailed in the MAS IBTRMv3 and complementary regulations and standards that aim to provide guidance to senior management, risk management and IT security specialists in regulated institutions (such as banks) in the management of security risk in information and IT, such as SOX, PCI-DSS, APRA PPG234, and many others[2]. In addition, Centrify solutions can benefit any enterprise in Singapore or South East Asia working to implement guidance similar to MAS IBTRMv3's comprehensive security controls.

This white paper will discuss how Centrify's integrated suite of identity and access management solutions are a critical part of any IT security risk management strategy and details the numerous sections of MAS IBTRMv3 that can be directly addressed using Centrify Suite and Microsoft Active Directory.

[1] See: http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/IBTRMV3.pdf
[2] For additional whitepapers on SOX, PCI-DSS, APRA, etc. see http://www.centrify.com

The Fragmentation of Identity and Access Management within the Distributed Environment

Key provisions of MAS IBTRMv3 address the security risks around identity and access management within distributed, cross-platform environments – risks, it should be noted, that are pervasive in organisations and not exclusive to regulated organisations. Frequently within regulated organisations you'll find that IT infrastructure has fragmented along platform lines, with some part of the staff focused on managing the Microsoft Windows-based infrastructure, and additional groups focused on managing UNIX/Linux systems, Mac OS X workstations, Mobile devices, SaaS, on-premise applications, databases, and the like.

Regulated organisations have broadly adopted Windows as the platform of choice for user desktops and basic network file and print services. Microsoft Exchange has been deployed for email, and other Windows Server-based solutions such as SQL Server and SharePoint are being used. In the Windows environment, Microsoft provides a comprehensive identity management solution through Active Directory, and the Identity Lifecycle Management applications provide lifecycle management for user identities. IT departments have invested millions of dollars deploying Active Directory, with the result that they have built a highly scalable and fault-tolerant domain controller infrastructure as part of ongoing initiatives to meet security and business continuity objectives. The broad adoption of Windows as a core infrastructure also fits with the organisational initiatives to trim costs through adopting technology that can be adopted uniformly across organisations. Within this Windows estate, Active Directory is the core, strategic infrastructure.

Organisations have also widely deployed UNIX and Linux servers for enterprise-class applications and databases. But no single identity management solution enjoys anything like the pervasiveness of Active Directory within the Windows environment. Regulated IT organisations are dealing with a plethora of identity stores deployed to manage their UNIX/Linux platforms, including:

- Significant usage of locally managed /etc/passwd text files on individual systems.
- Use of Sun's outdated Network Information Service (NIS or NIS+).
- Use of LDAP-based directories such as OpenLDAP or the Sun ONE Directory.

Mac workstations are also a popular choice among many regulated organisations, particularly for engineering and design applications. While identity management solutions exist for Mac networks, they represent yet another identity system for IT staff to manage. Many of the key cross-platform integration features needed by administrators are lacking in the solutions that come from Microsoft and Apple.

The same identity store proliferation continues with Mobility and also SaaS.

Access control features are built into Active Directory and are heavily used to manage access to Windows resources. However, few solutions exist to expand access control to non-Windows environments. IT managers are often faced with implementing proprietary layered solutions that are costly and difficult to manage.

The identity management challenges multiply as we move up from the system layer to applications. As new Java and web applications are rolled out on platforms such as Apache, JBoss, Tomcat, IBM WebSphere and BEA WebLogic, developers are creating even more identity stores through the use of text files or database tables. Database platforms such as IBM's DB2 and Informix, along with enterprise applications such as SAP, add yet another set of individual identity stores.

Thus, the fact is that in many organisations, identity and access management for UNIX, Linux and Mac OS X systems, applications (SaaS or on-premise), mobility and databases is quite fragmented compared to Windows.

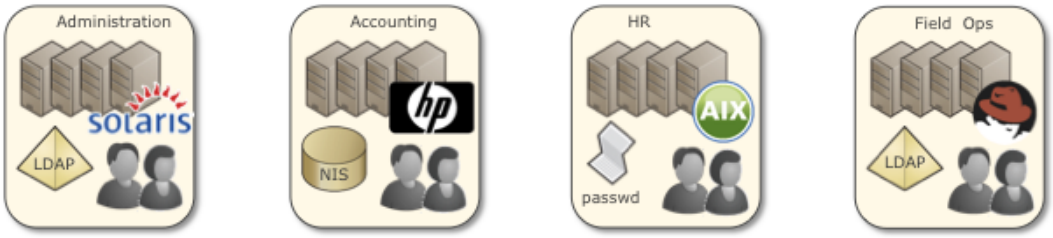


Figure 1-2. The fragmentation of identity management in the distributed environment: one user, multiple accounts, multiple identity stores, and fragmented (or no) policy mechanisms.

As the regulated organisations' dependence on information systems has grown, so too has recognition of the enormous challenges involved in keeping them secure and available. MAS IBTRMv3 in particular is driving security initiatives to secure information systems, and the data that they hold, and to design risk-based security plans. Because not all systems will require the same level of security and attention, role-based access controls, delegated administration, and fine-grained privilege management features are becoming increasingly important. IT auditing tools are also needed by security managers charged with monitoring systems for unauthorised or suspicious activity, and by independent IT auditors who will be periodically checking to ensure that the security controls in place are working as intended.

Centrify's Vision for Unified Identity and Access Management

Centrify's vision is to help organisations strengthen IT security and streamline operations by centrally securing their cross-platform servers, workstations and applications using Microsoft Active Directory. By enabling IT departments to control users' access to these resources, authorise what they can do, and audit their actions, Centrify eases compliance requirements and reduces the risk of internal and external security threats. And, by extending an organisation's existing Active Directory infrastructure to embrace non-Windows servers and applications, Centrify simplifies an organisation's IT infrastructure and reduces costs.

Figure 4-1. Centrify eliminates the need for multiple identity and access management solutions in the distributed environment by consolidating management in Microsoft Active Directory: one user, one account, one directory, one policy mechanism.

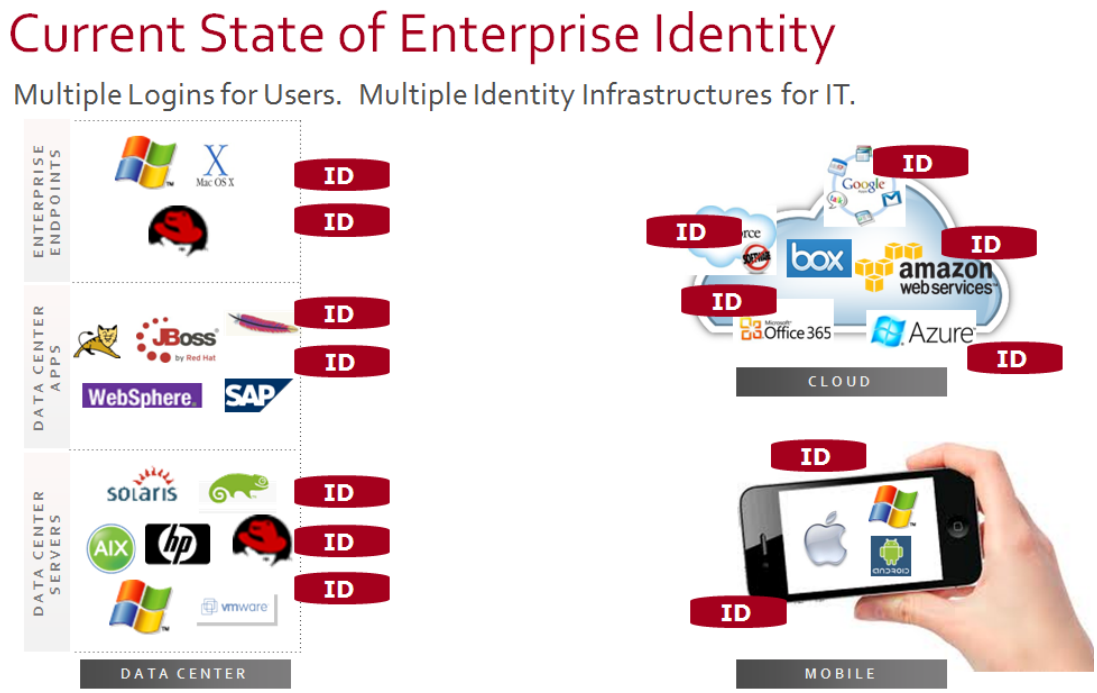
Centrify delivers on this vision through the Centrify Suite, an integrated family of Active Directory-based auditing, access control and identity management solutions. Centrify solutions are next-generation technology, built on a common architecture that embraces open standards, making them quick-to-deploy, easy-to-manage, and cost-effective compared to complex and proprietary legacy products.

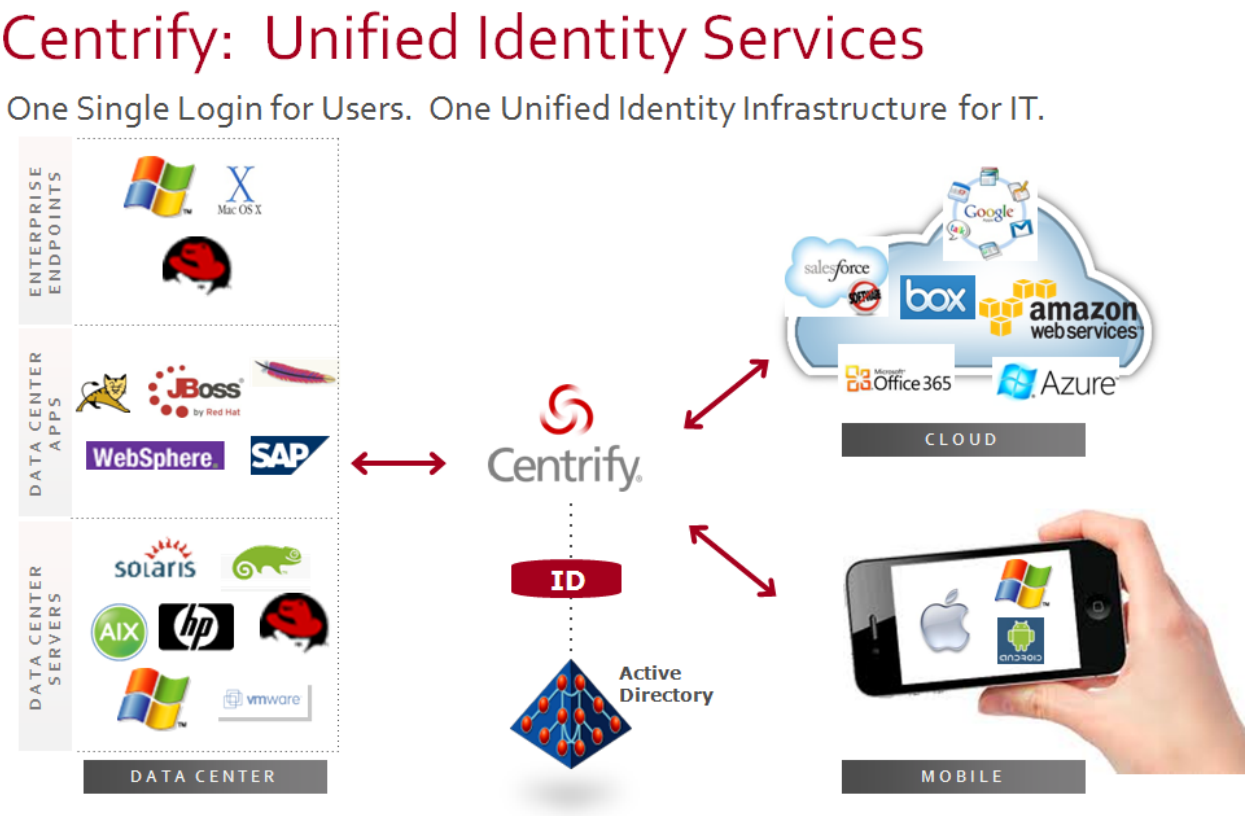
The Centrify Suite is comprised of the following solutions:

- **Centrify DirectControl.** Secures over 350 flavors of UNIX, Linux, Mac and also Mobility platforms such as iOS (iPhones, iPads) and Android (including Samsung KNOX) using the same authentication and Group Policy services deployed for a Windows environment. DirectControl also provides Active Directory-based single sign-on solutions for popular web-based servers (e.g., Apache, WebLogic and WebSphere), databases (e.g., DB2) and enterprise applications (e.g., SAP).

- **Centrify for SaaS.** Centrify for SaaS eliminates password sprawl with Single Sign On (SSO) for SaaS apps while giving enterprise centralised control over access to ever-increasing numbers of SaaS applications.
- **Centrify DirectAuthorize.** Centrally manages and enforces role-based entitlements for granular control of user access and privileges on Windows, UNIX and Linux systems.
- **Centrify DirectAudit.** Delivers auditing, logging and continuous, real-time monitoring of user activity on Windows, UNIX and Linux systems.
- **Centrify DirectSecure.** Provides trust-based protection of sensitive information by dynamically isolating and protecting cross-platform systems and enabling end-to-end encryption of data-in-motion.

For a comprehensive overview of Centrify solutions, review our White Paper: "Centralised Identity and Access Management of Cross-Platform Systems and Applications with Active Directory and the Centrify Suite".





The following sections provide an overview of how each solution's key features and benefits map to MAS IBTRMv3 compliance requirements:

MAS IBTRMv3 Requirements Checklist to Centrify Suite Mapping

MAS IBTRMv3 vs. Centrify overview			
Section	#	Summary of Requirements	Centrify Solution
Risk Management Framework	2.4.1	For each type of material risks identified and analysed, risk mitigation and control strategies that are consistent with the value of the information asset and level of risk tolerance, are developed and implemented by management. Risk mitigation entails a methodical approach in prioritising, evaluating and implementing appropriate risk-reduction controls and security measures that emanate from the risk assessment process.	Risk analysis will identify that tasks related to identity management as an area of risk and in need of control strategies, particularly around de-provisioning of users in both local and web based applications. Centrify DirectControl as well as Mobile/SAAS solutions can provide the type of single-point of management solution that is required to address these risk factors.
Security and Control objectives	4.1.2	The strength and type of encryption algorithm adopted by the financial institution are commensurate with the degree of confidentiality and integrity required for its internet systems. Only encryption algorithms that are well-established international standards are used by the financial institution. Such algorithms should be subjected to rigorous scrutiny by an international community of cryptographers; or approved by authoritative professional bodies, reputable security vendors or government agencies.	Centrify DirectControl is FIPS-140-2 certified. This provides a high confidence that appropriate crypto is used at all times and that the overall integrity of the Centrify solution is guaranteed.
	4.1.3	All cryptographic keys are created, stored, distributed and changed under the most stringent conditions. No single individual has knowledge of the entire key, or have access to all the constituents making up these keys. The frequency at which cryptographic keys are changed is based on the sensitivity of the encrypted data and operational criticality.	FIPS 140-2 provides assurances about cryptographic key use. Centrify provides many configuration options to tune keys under its control to be appropriate for the environment and threats being faced. For example the life-times of kerberos keys can be tuned via group policy. The important fact here is not only that it can be done, but that it can be done via a well understood and easy to use mechanism – namely Group Policies – which means it is a practical and easy thing to do and maintain. Unlike many 'could be done in principle, but who has the time for that' security settings, Centrify strives to make such tasks easy to design, easy to use and thus accessible to most organizations.
	4.1.4	Hardware security modules and similar tamper-resistant devices are used to perform encryption and decryption functions.	Centrify DirectControl provides SmartCard support for authentication purposes on selected operating systems.

MAS IBTRMv3 vs. Centrify overview			
Section	#	Summary of Requirements	Centrify Solution
	4.3.4	Standby hardware, software and network components are maintained to provide the capability for fast recovery.	DirectControl functions by utilizing existing Domain Controller infrastructure and thus does not require any additional hardware to function in a fault-tolerant manner. No specific configuration is required to achieve fault tolerant operation it is the default. This makes Centrify a very cost effective solution to deploy and maintain.
Security Principles and practices	5.1.1	Personnel involved in developing, maintaining and operating websites and systems are adequately trained in security principles and practices.	Centrify DirectControl utilizes Active Directory tools and techniques to accomplish most of the day to day maintenance required to deal with adds, moves and changes in the user population. This makes training for how to operate Linux/Unix computer effectively identical to how windows environments are managed, thus greatly reducing training costs and lowering misconfiguration risks.
	5.1.2	Segregation of duties is established for operating systems function, systems design and development, application maintenance programming, computer operations, database administration, access control administration, data security, librarian and backup data file custody.	DirectControl enforces separation of duties by leveraging Active Directory's rich delegation model to provide delegated administration of UNIX, Linux and Mac OS X systems. Each Zone can have its own set of administrators, and each administrator could have his/her own set of rights. For example, one administrator may be authorised simply to add or remove other users from Zone membership, while another administrator may also be authorised to change Zone properties. As separation of duties dictates, these Zone administrators do not need elevated privileges – for example, they do not need to be able to create or delete accounts just to update Zone membership or Zone properties. A single user could also be an administrator of multiple Zones, with different privileges on each Zone.
	5.1.2	Job rotation and cross training for security administration functions are instituted.	DirectControl enables full role based access control through Active Directory Security group membership. This makes it easy and reliable to change access privileges including administrative rights by simply change users group memberships.

MAS IBTRMv3 vs. Centrify overview			
Section	#	Summary of Requirements	Centrify Solution
	5.1.2	Access rights and system privileges are provided based on job responsibility and the necessity to have them to fulfil one's duties.	Centrify permits true least privilege access control for Windows and Unix platforms. Fine grained rights can be attached to roles. This includes the ability to carry out privileged tasks in Windows & Unix. Roles can assign the rights they contain to a Security group containing users and map these to a set of computers, being members of a separate security group. For example an OracleAdministrators role might contain the right to 'su' to the oracle users on Unix as well as to create an Oracle privileged desktop under Windows. Through a role assignment, Staff in the OracleAdministratorsRoleGroup would be given the OracleAdministrators rights for the target group or Oracle servers being members of the OracleServersGroup. This makes role changes trivial. It also makes bringing up new Oracle Servers easy – just make them a member of the OacleServersGroup and all staff that should have access will automatically be granted it. This group based role management is far superior and flexible to the OU based structures that typically get used in Windows. Having the system of role assignments work identically across Windows and Unix makes training, monitoring and general assurance easy and achievable.
	5.1.4	No one is provided concurrent access to both production systems and backup systems, particularly data files and computer facilities.	By modeling access on Security Groups, assuring specific business rules are enforced, such as prohibiting concurrent access, is straight forward. It is easy to programmatically assure that the members of two or perhaps more groups form a non-intersecting set.
	5.1.4	Access to backup files or system recovery resources are duly authorised for a specific reason and a specified time only.	Centrify Roles can have time-boxing restrictions such that they only allow access during certain times of a week with Mon-Sun 24-hour granularity.
	5.1.5	Personnel from vendors and service providers, including consultants, who have been given authorised access to the organisation's critical network and computer resources are subject to close supervision, monitoring and access	Role assignments can have an activation and deactivation date pre-programmed. In combination with role-based hourly time-boxing, this makes it possible to grant access to a group of people (say external consultants) starting on a particular date, during business hours only (Mo-Fr 8-5) and automatically terminating a few days later. This avoids the risk of accidentally forgetting to de-provision consultants. As the times can be reset, its easy to re-use such role-assignments again and again.
	5.1.7 (a)	Two-factor authentication is implemented for privileged users (systems, technical, operations, development, programming, support etc).	Two factor authentication including the use of smart cards can be set up in AD and Centrify interoperates with these authentication mechanisms.

MAS IBTRMv3 vs. Centrify overview			
Section	#	Summary of Requirements	Centrify Solution
	5.1.7 (b)	Strong controls are implemented for remote access by privileged users.	Centrify can be used to reduce the usage of shared accounts and thus force individuals to identify themselves properly prior to being granted access to a system. Once logged in they may then be granted the right to elevate privilege.
	5.1.7 (c)	The number of privileged users is restricted.	Centrify makes it possible to grant fine-grained privileges for both Windows and Unix users. This makes it possible to avoid 'open slather' root / Administrator access and instead grant access to just specific activities, such as to start a backup. This can greatly reduce the number of users who need to hold broad high-privileged access. Using Centrify it is easy to see who has high privileges on which systems making it possible to gauge any changes in the size of the population of privileged users.
	5.1.7 (d)	Privileged access is granted on a "need-to-have" basis.	Fine grained 'least privilege' access control is often avoided in windows and unix environments as 'too hard and expensive' to administer. Using Centrify allows not only fine grain controls to be implemented beyond what is usually found on Unix / Windows alone, but it is also easy to manage via Security Group memberships. This makes Centrify a real enabling technology for least-privilege access control.
	5.1.7 (e)	Audit logging of system activities performed by privileged users are maintained.	Centrify Audit can be configured to record all privileged activities both on Windows and Unix platforms. Centrify DirectAudit captures detailed session events, metadata and video linked definitively to Active Directory identities. All session activity, including system input and output is recorded. Sessions and logs are centrally stored for real-time monitoring and historical reporting and analysis. Role-based control of audit data ensures authorised access to DirectAudit session data.
	5.1.7 (f)	Privileged users do not have access to systems logs in which their activities are being captured.	Centrify Audit includes circumvention controls that deny even Domain Administrators from disabling the audit service on Windows platforms. In addition logs are stored off-system in MS-SQL server which can be secured against access by most Administrative staff, thus protecting the audit data from unauthorized access even by Domain Administrators.
	5.1.7 (g)	Regular audits or management reviews of the logs are conducted.	Centrify Audit makes it easy to identify sessions that are worth investigating through its intuitive query system and session groupings. The included workflow system makes it quick to pass sessions to co-workers for inspection. In addition, Centrify Insight, a Splunk App, organisations can analyse and report on authentication, authorisation and other events occurring on UNIX, Linux and Mac OS X systems managed by Centrify DirectControl.

MAS IBTRMv3 vs. Centrify overview			
Section	#	Summary of Requirements	Centrify Solution
	5.1.7 (h)	Sharing of privileged IDs and their access codes is prohibited.	Centrify DirectControl includes tools to retire or restrict shared accounts such that users are forced to use their own credentials to authenticate before using privileged desktop creation tools or 'sudo' to assume user ID's for administrative purposes. This leaves a clear audit trail in the Windows Security Log (even for unix logins) without reducing the ability to access system uids such as 'oracle', 'apache' or similar.
	5.1.7 (i)	Vendors and contractors are disallowed from gaining privileged access to systems without close supervision and monitoring.	Centrify Audit can be configured to grant access only when auditing is in place and able to record the sessions over the network. There are facilities in place to grant rescue rights to certain individuals to manage the system in unusual circumstances.
	5.1.7 (j)	Backups of data are protected from unauthorised access.	All Centrify DirectControl data resides in Active Directory and thus the same backup practices that apply to AD also apply to Centrify meta data. Thus once a compliant mechanism for AD is arrived at, Centrify is already automatically dealt with – no additional effort required. Centrify Audit Database information does require separate consideration, but is no different from backing up any high value data store, so mechanisms for this will already be designed and in place for other databases and can simply be re-used for the Centrify Audit data.
	5.2.1 (a)	Deploy hardened operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of updates, patches and enhancements recommended by system vendors; change all default passwords for new systems immediately upon installation.	An important part of hardening an operating system is to reduce the number of identity stores, which Centrify achieves. It is also important to aim for a low complexity solution for role assignments as errors in this space can have catastrophic effects. By managing access privileges, particularly the ability to elevate privilege via AD Group memberships the risk in making changes to roles is vastly reduced.
	5.2.1 (k)	Maintain access security logs and audit trails.	The Centrify Audit product is critical in providing 5.2.1 k) logging and audit information at a level of detail and an ease of access that makes the analysis of faults faster and easier. By doing live session recording – akin to a video camera on the shoulder of the session operator – there is never any question on who did what and when on which system, from which system.
	5.2.1 (l)	Analyse security logs for suspicious traffic and intrusion attempts.	Centrify Audit query facilities assist in the search for suspicious and unusual activity in the audit logs.

MAS IBTRMv3 vs. Centrify overview			
Section	#	Summary of Requirements	Centrify Solution
	5.2.1 (z)	Deploy strong user authentication in wireless local area networks and protect sensitive data with strong encryption and integrity controls.	The Centrify MDM solution assists with wireless security in that it makes it easy for mobile devices to participate in a WPA2-AES enterprise (certificate based) wifi networking environment.

Resources and Contacts

Centrify Suite Overview

http://www.centrify.com/

Additional White Papers

Centrally Controlling, Securing and Auditing Access to Cross-Platform Systems and Applications Using the Centrify Suite

http://info.centrify.com/Centralized-identity-access-management-cross-platform-systems-applications.html

Privileged User Activity Auditing: The Missing Link for Enterprise Compliance and Security

http://info.centrify.com/privileged-user-activity-auditing-white-paper.html

Asia Pacific Contacts

Matt Ramsay
Regional Director, APAC
Centrify Asia Pacific

Direct: (+61) 1300 795 789
Mobile: (+61) 0423 93 0423
matt.ramsay@centrify.com