**Trusted Information
Sharing Network**
for Critical Infrastructure Protection

User-access management

A DEFENCE IN DEPTH CONTROL ANALYSIS

June 2008

FOREWORD

Access control is ultimately the 'gateway' through which all access—authorised and unauthorised—to information and assets must pass. As it is also the area of information security with the most direct inter-relationship with end-users, it is also one of the most challenging to address.

This report has been developed by the IT Security Expert Advisory Group (ITSEAG) which is part of the Trusted Information Sharing Network (TISN)[1] for critical infrastructure protection.

The TISN has previously released a series of papers designed to help CEOs and Boards of Directors understand the threats to the IT infrastructure of their organisations and to provide recommendations for mitigating those threats. Issues covered in these documents range from managing denial of service risks to information security governance. These papers are available from the TISN website: www.tisn.gov.au.

In developing this body of work, SIFT (www.sift.com.au) engaged in discussions with members of the ITSEAG and other relevant bodies including key stakeholders from the IT and information security sectors and owners and operators of critical infrastructure to gain an individual industry perspective on the issues. SIFT thanks all participants in these discussions for their contributions to the project.

---

[1] TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of nine sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAG), and the Critical Infrastructure Advisory Council (CIAC—which is the peak body of TISN and oversees the IAAGs and the EAGs). More information on TISN can be sought from www.tisn.gov.au or by contacting cip@ag.gov.au. The ITSEAG is one of the expert advisory groups within the TISN framework. The ITSEAG provides advice to the CIAC and the sector-based IAAGs on IT security issues as they relate to critical infrastructure protection. It is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. The ITSEAG Secretariat can be contacted on (02) 6271 7018.

Contents

Figures

Tables

Featured controls

User-access management scenarios

EXECUTIVE SUMMARY

Access to an organisation's information systems has greatly changed in recent years as Internet Protocol-based systems extend past the traditional systems security perimeters. A mobile workforce, third party access (i.e. contractors, suppliers and clients) and home based work are examples now common place. Therefore, access management is a key frontline strategy for all organisations to protect their information and systems.

'Access' in an information systems context has been defined simply as the ability to do something with a computer resource (e.g. use, change or view)[2]. Such a definition positions access control at the core of all information risk-management exercises. This central importance of user-access management is consistent with survey findings: The Deloitte Global Security Survey found that 50 per cent of respondents listed access and identity management as among the top initiatives pursued in 2007[3].

Two objectives for user-access management are established by the ISO 27001 *Standard for Information Security Management Systems*:

- ensure authorised user access

- prevent unauthorised access to information systems.

In order to achieve these two objectives, the following key components of user-access management must be analysed and understood:

- Assets—what is the organisation trying to protect?

- Users—who are the authorised users—both personnel and automated processes—within and outside the organisation?

- Privileges—which users require access to which assets, to what extent, and in what circumstances?

As established by the defence in depth strategy, user-access management requires controls to be implemented at the levels of people, processes, and technology[4].

The **people** component of this triad is generally acknowledged to be the most difficult to assess and control. Attacks on access control at the people layer will commonly revolve around an abuse of trust. For example, attacks such as phishing will generally require users to accept or perform an action before a malicious payload is delivered[5].

At a **process** level, operational management of user access is essential to ensure that access controls are consistent, sustainable and well documented.

---

[2] NIST, *Special Publication 800-12*, http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter17.html
[3] Deloitte, *2007 Global Security Survey,*
www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf.
[4] TISN, *Defence in Depth, June* 2008, http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications
[5] It is noted that recent attacks have involved the use of malicious code compromising visitors to infected websites, and as such are effectively targeting the technology layer rather than the people layer and rely less on an abuse of trust than a poor technical security profile.

At a **technology** level, the opportunity exists to harness technology to strictly enforce access control as determined or defined in considering the people, processes and data resources in place. However, as with all technology, the controls may be able to be defeated or subverted and as such mechanisms for detecting attacks should be established.

As every organisation is different—with varying work conditions, employee culture, processes and supporting technology—the importance of considering these risk factors in the context of the organisation is magnified. The organisation's individual circumstances will influence risk identification, risk analysis and risk treatment. Specific elements for consideration when examining the user-access management environment are:

- categories and classification of resources and assets that the organisation controls

- financial and social criticality of the business processes

- profile of the workforce

- geographic spread of facilities

- technology architecture.

Complementing the core principles of defence in depth, and the overarching principles of information security, user-access management itself has a series of core guiding principles, as follows:

- 'Categorisation' and 'classification'—clearly categorise and value all data and processing resources and enable the status of each resource to be correctly 'labelled'.

- 'Least privilege'—provide the least amount of access necessary for a given user to complete their business role.

- 'Need to know'—provide access to systems and information only where there is a need for the recipient of such access to have it.

- 'Controlled access'—define procedures to monitor, enable and disable access methods, and enforce security policy at all access points.

Effectively applying these principles to the organisation's data—both in transit and at rest—throughout the processes, technology and people in an organisation will ensure that user-access-related risks are appropriately controlled, allowing authorised access when required and unauthorised access to be prevented.

This report is a companion document to the full *Defence in depth* report, and extends the core principles in that report to the specific area of user-access management. This report includes supporting material such as practical implementation examples and specific focus area analysis on key topics within user-access management. When these controls are considered in the context of an organisational risk assessment, and a cohesive access control plan is developed, an organisation can ensure that its user-access controls are appropriate.

While this report places focus on technical and procedural controls, the importance of a highly technology and security-aware workforce should not be overlooked.

A brief overview paper has also been provided for Chief Executive Officers (CEO) and Boards of Directors, as well as a paper for Chief Information Officers (CIO) and Chief Technical Officers (CTO).

OVERVIEW

Defence in depth

This report provides a more detailed analysis of a specific topic area—user-access management—to complement the full *Defence in depth* report developed by the TISN.

As detailed in the *Defence in depth* report, the core principles of a defence in depth strategy are:

1. **Implement measures according to business risks.**
2. **Use a layered approach— as illustrated at right— such that the failure of a single control will not result in a full system compromise**.
3. **Implement controls such that they serve to increase the cost of an attack.**
4. **Implement personnel, procedural and technical controls.**
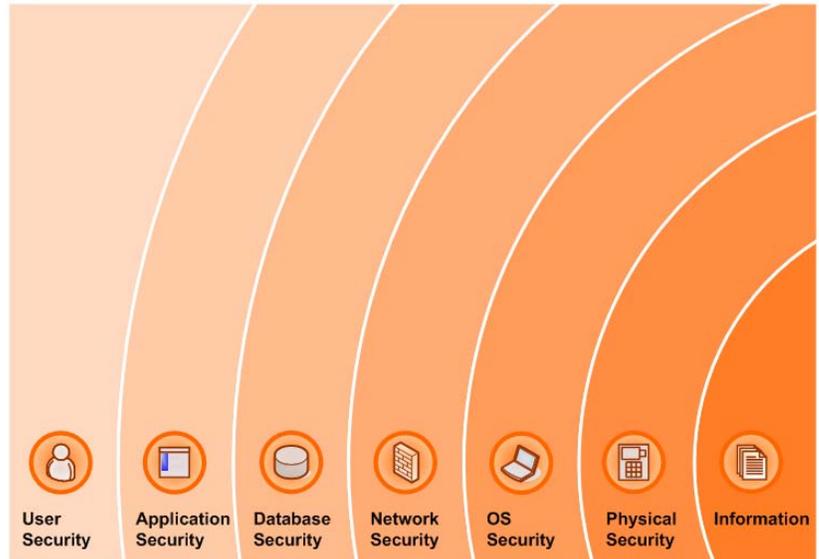
In implementing defence in depth controls, specific attention is provided to key areas shown in **Figure 1:**

Governance	Process
• Risk management	• User-access management
• Information security	• Identity management
• Policy & compliance management	• Incident response management
	• Audit management
People	**Technology**
• Personnel security	• Communications management
	• Infrastructure management
	• Network architecture management
	• Application security
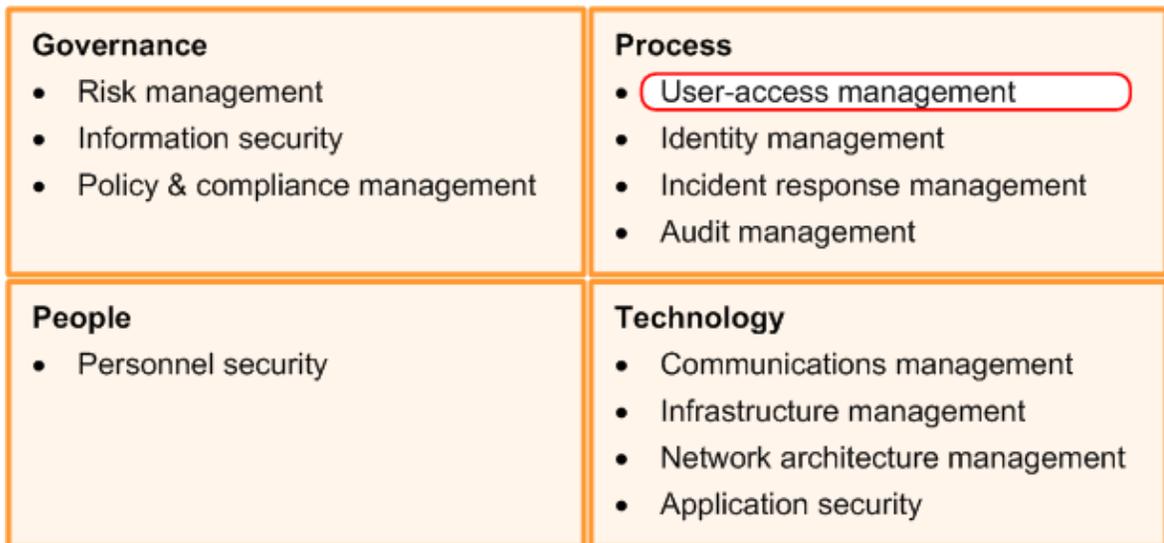
Figure 1: Key defence in depth focus areas

This report delves further into the user-access management focus area.

Structure of the report

The overview section of this paper provides an introduction to user-access management in the context of the defence in depth strategy developed in the TISN *Defence in depth* full report.

The report is divided into four main sections, following the lifecycle model for strategic implementation defined in the *Defence in depth* report as applied to user-access management (see Figure 1). These are:

- **Establishing context**—provides context for user-access management and introduces a number of prerequisite controls necessary for the implementation of effective user-access management within the defence in depth framework.

- **Risk analysis**—uses the risk-analysis methodology described in the TISN *Defence in depth* paper to develop criteria for assessing internal and external risks and threat trends that prompt the need for user-access management.

- **Implement user-access management**—provides a guideline for the implementation of a holistic approach to user-access management across governance, people, process and technology.

- **Monitor and review**—provides considerations to ensure ongoing relevance of the user-access management approach and considers emerging threats to user-access management.
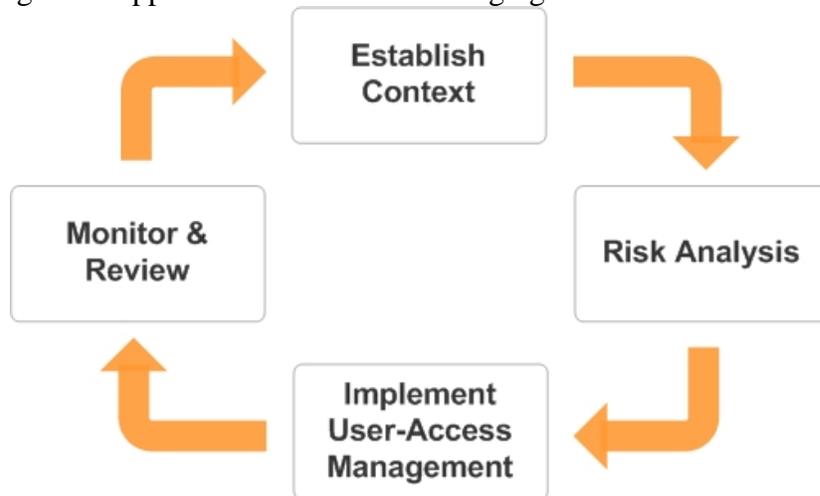
Figure 2: User-access management life cycle

User-access management

'Access' in an information systems context has been defined simply as the ability to do something with a computer resource (e.g. use, change or view).

Given this definition of access, user-access management therefore involves managing who can use, change or view systems or information and the circumstances in which such access is permissible.

User-access management is defined by the ISO 27001 *Standard for Information Security Management Systems* to have the following objectives:

- ensure authorised user access
- prevent unauthorised access to information systems.

Expanding on the objectives from ISO 27001, a broad set of business-level objectives for user-access management can be defined as follows:

- allow only authorised users to have access to information and resources
- restrict access to the least privileges required by these authorised users to fulfil their business role
- ensure access controls in systems correspond to risk management objectives
- log user-access and system use, and ensure that the system can be audited in line with the system's risk profile.

To reach these objectives, the standard identifies four primary controls for managing access rights. These are:

- **User registration**—formal approval and documentation of user access to information systems allows an organisation to track and verify the individuals who have access to specific systems and services.
- **Privilege management**—formalised processes for granting and revoking privileges allow an organisation to track and audit changes to user-access rights and determine the privilege levels of specific individuals.
- **User password / token management**—as passwords remain commonplace, standard processes for allocating and resetting user passwords reduce unnecessary exposure of temporary or default passwords and minimise the effectiveness of social engineering attacks against security administration staff. Policies that mandate minimal levels of password length and complexity also reduce the effectiveness of common password attacks. However, passwords alone no longer provide a satisfactory solution for critical systems and services. The use of two factor models involving the use of tokens and/or other credentials (e.g. biometrics) also require similar holistic management processes.
- **Review of user access rights**—identify improperly assigned privileges and allow an organisation to realign granted access rights with authorised access rights.

As with a defence in depth strategy, user-access management cannot be addressed solely at a technical level. Rather, an effective layered approach to user-access management requires controls to be implemented at the four levels of:

- governance
- people
- process
- technology[6].

---

[6] NSA, *Defense in Depth*, www.nsa.gov/snac/support/defenseindepth.pdf

Figure 3: Governance, people, process and technology

Similarly, the layered approach to defence in depth recommends controls be implemented at multiple layers, including:

- network access controls

- system-level access controls

- host-level access controls

- application access controls

- data access controls

- physical access controls

- password controls.

Access-control theory

Given the importance of access control and user-access management to all areas of information security, this is an area in which significant theory exists to describe alternative models for access control. While this paper's intention is not to cover the underlying access-control theory in significant detail—there are many excellent texts available to address this—an awareness of the principles of these theories is valuable.

The primary theoretical models for access control are:

- **Discretionary access control.** Discretionary access control restricts access to objects based on the identity of subjects and/or groups to which they belong[7]. The access rights are usually created and assigned to users by the owner of the object or asset.

- **Mandatory access control.** Mandatory access control requires security clearance labels to be set for both users and objects/assets. Earlier approaches to mandatory access control, such as multi-level security, enforced the access rights of users by checking whether a user's clearance label was greater than or equal to the clearance label of the data they were attempting to access[8]. This approach has been reconsidered through a number of industry projects such as flexible mandatory access control and the labelled security protection profile[9]. These improved architectures adopt a general purpose approach to access control, enforcing security policy (authorisation rules) across all subjects and objects in a system,

---

[7] United States Department of Defense, *DoD Standard 5200.28-STD,* www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
[8] OWASP, *Mandatory Access Control,* www.cgisecurity.com/owasp/html/ch08s02.html
[9] Information Security Systems Organization, *Labelled Security Protection Profile Version 1.b*, www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/protection-profiles/lspp.pdf, 1999.

rather than the limited scope of users and data in multi-level security. For example, the flexible mandatory access control model which has been gaining popularity since the introduction of SELinux supports a wider range of authorisation rules including ability to[10]:

- plug and play different policy (rule) engines behind a well-defined abstract security interface without needing to modify the rest of the system

- configure example security servers to achieve a wide range of security goals through constraint-based models.

- **Role-based access control**. In role-based access control, roles are defined which have a number of permissions and privileges attached. Users are assigned roles (a user may be assigned more than one role) commensurate with their occupation and job requirements to allow them to complete their tasks and inherit the access rights of the roles they have been assigned[11].

ESTABLISH CONTEXT

The information security principles from the Secure *Your Information: Secure Your Business* paper relevant to this section are:

Principles of Information Security

1. Information Security is Integral to Enterprise Strategy

2. Information Security Impacts on the Entire Organisation

3. Enterprise Risk Management Defines Information Security Requirements

4. Information Security Accountabilities Should be Defined and Acknowledged

5. Information Security Must Consider Internal and External Stakeholders

6. Information Security Requires Understanding and Commitment

7. Information Security Requires Continual Improvement

Figure 4: Applicable principles of information security for establishing the risk context

The need for user-access management in an IT environment is widely accepted. The Deloitte Global Security Survey found that 50 per cent of respondents listed access and identity management as among the top initiatives pursued in 2007.

---

[10] OpenSolaris, *OpenSolaris Project: Flexible Mandatory Access Control,* http://opensolaris.org/os/project/fmac/
[11] Harris S, *CISSP Exam Guide,* McGraw-Hill/Osborne

The *Defence in depth* report discussed the three main components necessary for analysis in order to allow an organisation to effectively establish the risk context within which the defence in depth strategy is to be implemented:

- enterprise strategy
- internal environment, assets and systems
- threat environment.

This report—looking purely at user-access management—will present a subset of this analysis in additional detail, providing a discussion on the two main components necessary for analysis in order to support the implementation of a comprehensive user-access management program:

- internal environment, assets and systems
- threat environment.

Internal environment

Internal environments will vary between organisations of different structure, assets, classifications, missions and risk tolerance. How these vary will affect the way in which risk classifications and identifications are measured and how user-access management is handled within the organisation.

The need for user-access management arises from the need for organisations to be able to control the accessibility of information and systems. As noted in the *Defence in depth* report, a number of key trends are driving the importance of a holistic view of information security. These trends are of particular relevance to user-access management:

- **Deperimeterisation.** The external boundaries of networks become more difficult to define as interactions between customers, business partners and suppliers continue to grow and increase in complexity. Access controls are necessary to generate and enforce the divisions of functions and capabilities that these parties can control.

- **Mobile workforce.** Employees increasingly are required to work in non-conventional environments with flexible arrangements and requiring flexible access to information and systems.

- **Decentralisation of services.** As services become more broadly accessible, user-access management helps contain the availability of services to only authorised users.

- **Increasing value of information.** The need to protect information from unauthorised disclosure increases commensurately with the value of information.

Components of user-access management

There are three key components to be analysed and understood for the design and implementation of an effective user-access management system. These are:

- assets
- users
- privileges.

Assets

Protecting critical infrastructure assets is a primary objective in using a defence in depth strategy[12]. In user-access management, all assets in an organisation fall under scope for consideration. At a high level, these assets (as defined in the TISN *Defence in depth* report) are:

- physical assets
- information assets
- intangible assets.

Of particular note, it is vital that organisations account for all technology that is used to transmit, store or manipulate information data, when developing an effective user-access management system. IT systems to consider include:

- physical infrastructure—including workstations, mobile devices, printers, servers and USB devices
- network infrastructure—including routers, switches, hubs, and wireless access points
- file systems
- applications—including operating systems, host-based applications, network-based applications and web-based applications
- application function access
- data storage.

Users

Within the context of user-access management, users are the entities which control, use or manipulate the resources/assets that user-access management aims to protect. Access controls are the tools used to enforce proper accessibility of resources to users.

Each organisation will have its own unique set of users. Depending on the organisation's industry and the approach taken to business and IT services—particularly the degree to which the organisation pursues an internal or outsourced service model—the following types of users will exist in varying degrees:

- employees
- contractors
- service providers and outsourcers.

Additionally, certain systems may require specific user accounts outside these categories, such as:

- Accounts shared between groups of users.

---

[12] Straub KR, *Information Security: Managing Risk with Defence in Depth*, August 2003, www.sans.org/reading_room/whitepapers/infosec/1224.php

- Accounts used for system-to-system authentication.

Privileges

Privileges are an authorisation or set of authorisations which dictate which actions users can perform on organisation assets, particularly information system assets[13].

Access privileges can be restricted or controlled based on a wide range of access criteria[14], including:

- **Identity**—controlling access based on the identity of the user.

- **Roles**—controlling access based on the role held by the user.

- **Location**—controlling access based on the physical location of the user; for example, allowing access to a critical system from the organisation's local network only.

- **Time**—controlling access based on the time of system use. For example, allowing use of a given system during business hours only.

- **Transaction**—controlling access based on the status of a given action. For example, allowing access to view details relating to open support tickets, but revoking access to the tickets once closed.

- **Access modes**—controlling access through limiting the user's mode of access. For example, providing read-only access, as opposed to read/write/create etc.

Of the items above, roles are of specific importance in role-based access control, as discussed in the *Overview* section of this report, but are also of general importance through the underlying principle of understanding the organisation's access needs.

Roles are not to be confused with 'positions' or 'titles' in an organisation. In the context of access control, a 'role' refers to membership of a group, where that group has a consistent set of access requirements for all group members[15]. As such, a single user may have multiple roles, and a single role will generally have multiple users holding that role. The intent of such an approach is to provide scalability to the user-access management process.

When analysing roles within an organisation, the following considerations are important:

- Role definitions[16]. Well-defined roles will encompass a number of privileges that are applicable to the specific duties to which a role corresponds. Roles enable simple updating for generic changes to job responsibilities without having to update privileges for every individual user assigned that role. Some common roles under different business units are listed below:

[13] Shirey, R, *RFC 2828 – Internet Security* Glossary, May 2000, www.faqs.org/rfcs/rfc2828.html.
[14] NIST, *Generally Accepted Principles and Practices for Securing IT Systems*, September 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
[15] Gonzales-Webb S, *Implementing Role Based Access Control in Healthcare*, May 2007, www.va.gov/rbac/docs/EHT_20070502_SW20_11_TEPR-RBAC_Presentation.ppt
[16] NIST, *An Introduction to Role-based Access Control,* December 2005, http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm

Sample organisation roles	
Management	**Business division**
• Board	• Line managers
• Chairman	• Team leaders
• Executives	• Team members
IT specific roles	**Other**
• IT administrators	• Internal organisation users
• Developers	• Third party partners
• Testers	• Customers/clients
• Help Desk	

Table 1: Roles split by business division

- The implementation of role-based access control within an organisation requires a complete understanding of roles and their access requirements. Thus, the primary driver for role engineering is to support this implementation by deriving staff roles from job functions and business processes. Only once these roles and their required information and resource access are defined can role-based access control be effectively implemented and deployed within an organisation. A methodology for deriving roles via the role engineering method is described below[17]:
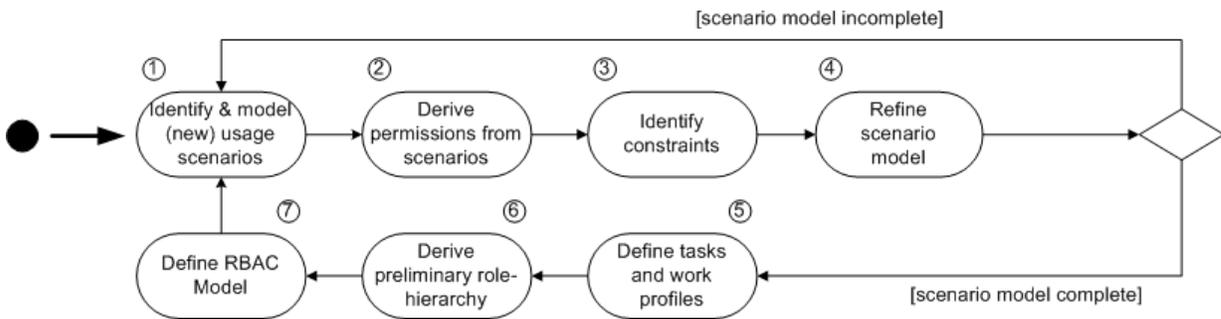
Figure 5: Role engineering

- Identify and model usage scenarios—system usages are identified and modelled in terms of scenarios.

- Derive permissions from scenarios—for each scenario the minimum access operations required are identified.

- Identify constraints—constraints to be enforced on each permission are defined, such as separation of duties or time dependencies.

---

[17] G. Neumann and M. Strembeck. *A Scenario-driven Role Engineering Process for Functional RBAC Roles*, 2002, 7th ACM Symposium on Access Control Models and Technologies, wwwi.wu-wien.ac.at/home/mark/publications/sacmat02.pdf

- Refine scenario model—review the scenario model from the first step. Define any generalisations or sub-scenarios.

- Define tasks and work profiles—tasks are a collection of scenarios. Profiles are a collection of tasks. This stage defines tasks by grouping scenarios.

- Derive preliminary role hierarchy—use the work profiles and defined permissions to create a role hierarchy. A common approach is to have senior and junior roles with senior roles inheriting junior permissions.

- Define RBAC model—use the role hierarchy, defined permissions and constraints as input into the RBAC model. Redundant roles can be removed and new role constraints and hierarchies can be developed, merged and separated.

- Role hierarchy. Frequently, roles for access control are developed in tiers, where higher tiers command higher accessibility. There may be certain roles (e.g. systems administrators) where higher tiers have a superset of the privileges offered by roles in its subsidiary tiers. Organisations should ensure that if role hierarchies are used, separation of duties is maintained. A model for a role hierarchy can be found at **figure 6**.
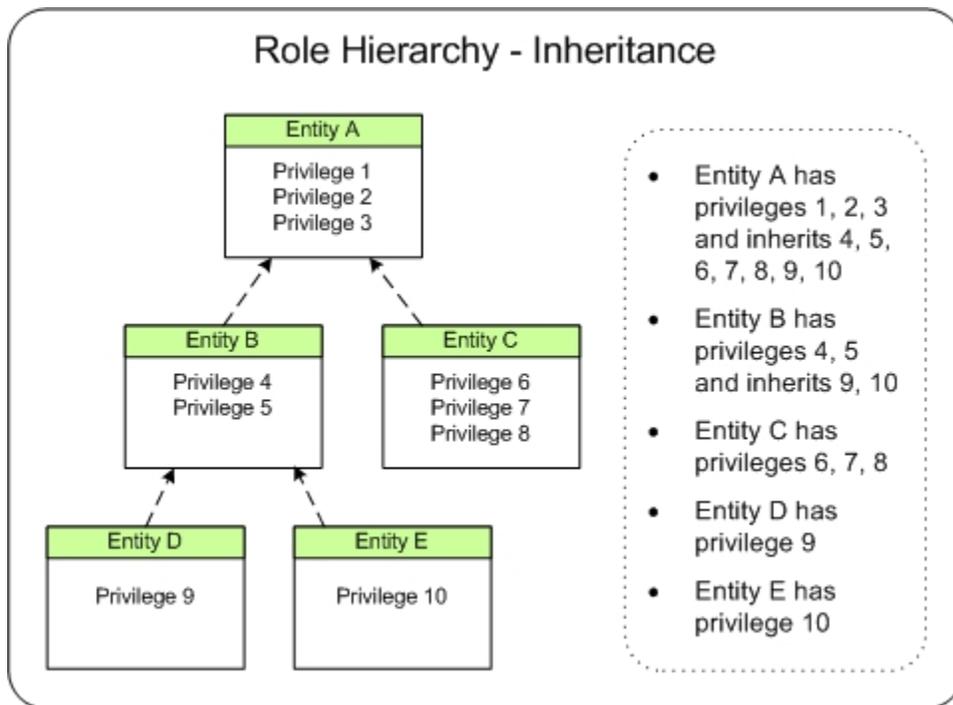
Figure 6: Role inheritance in hierarchy RBAC

Threat environment

As access control is ultimately the 'gateway' through which all access—authorised and unauthorised—must pass, the threat environment for user-access management includes a significant range of attacks aimed at defeating or subverting access-control mechanisms to achieve unauthorised access to systems or information.

Attacks against access-control systems can generally be categorised into groups of attacks based on the element of the control that they exploit:

- the human factor (people)

- technical aspects of access control (technology)

- weak processes/poor management of processes (process).

The human factor

A common adage in information security is that people are the weakest link[18]. Of the four pillars of defence in depth (governance, people, process and technology), the people component is generally acknowledged to be the most difficult to assess and control. These difficulties may lead to fundamentally weaker protection of assets as people become a proxy for malicious attack. The 2007 Deloitte Global Security Survey highlighted this well, finding that 79 per cent of participants cited the human factor as the root cause of information security failures, and 91 per cent of participants indicated concern about employee security weaknesses.

Attacks on the human factor commonly revolve around an abuse of trust. Attacks such as phishing and Trojans require users to accept or perform an action before any malicious payloads are delivered. These attacks continue to threaten organisations despite increasing user-security awareness[19] as a result of increasingly sophisticated social attacks. Users may also breach security measures knowingly for their own purposes, whether for malicious intent, monetary gain, workflow shortcuts or other motivations. For example, a senior finance executive could circumvent access restrictions in order to modify underlying financial data to manipulate financial reports.

Furthermore, users are generally more prone to making errors than technology. Small errors could lead to direct disclosure of sensitive information or inadvertently opening vulnerabilities to provide an attacker with access to sensitive information or other assets. Such errors could include:

- disclosing sensitive information in publicly accessible forums such as the internet

- sending sensitive information (such as credentials or financial data) to unauthorised parties (e.g. via email)

- failing to carry out sensitive information-related operational or management procedures in line with documented processes.

---

[18] Tan, A, *People: Your network's weakest link*, 11 Oct 2005, ZDNet Asia, http://news.zdnet.co.uk/internet/security/0,39020375,39228254,00.htm
[19] PricewaterhouseCoopers, *The Global State of Information Security 2007,* 2007, www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B/$FILE/PwC_GISS 2007.pdf

Technical aspects of access control

Many access controls are most strictly enforced at the technology layer of defence in depth. There may be cases where such access controls are susceptible to attacks which compromise or immobilise the controls. These weaknesses may exist due to reasons including:

- poor design and development

- poor configuration

- inadequate security testing of controls

- issues with underlying systems.

A sample of various user-access management technologies that have suffered weaknesses or incorporate trade-offs of usability/functionality against security is provided below:

- **Single sign-on.** The use of a single authentication mechanism for all systems means users have to manage only one set of credentials but it also creates a single point of failure for security. As a result, more attention must be paid to the management process of this single credential to ensure a broad access compromise is avoided. Additionally, single sign-on under some configurations may result in the principle of least privilege being difficult to enforce due to implementation constraints.

- **Biometrics.** The use of personal physical characteristics as authentication credentials is also subject to security risks. Early testing has indicated that biometrics may be vulnerable to copying or forgery[20], and once compromised can never be revoked, particularly if posted on a public forum as evidenced by the experiences of a German government minister, whose fingerprints are now freely downloadable[21]. Furthermore, given that copying biometrics requires physical proximity, there may be a risk of physical harm to the users of systems under attack. Many other issues exist with respect to biometrics, as summarised by the Biometrics Comparison Chart[22] developed at the US National Center for State Courts.

- **Multi-factor authentication.** In general, two-factor (or more) authentication provides improved access control security but if incorrectly implemented it can also introduce weaknesses, particularly in credential matching. If both factors are not cross-referenced to the same identity but are checked only for validity, unauthorised access can occur.

- **Remote access solutions.** Teleworking increases organisational flexibility and productivity of employees but the remote connectivity increases the attack surface of the organisation. If user-access rights are not adequately managed, unauthorised network access may occur.

---

[20] Busch C, Daum H, *Evaluation of Biometrics*, 2004, Fraunhofer Institute www.inigraphics.net/press/topics/2004/issue1/1_04a08.pdf.

[21] Goodin D, 'Get your German interior minister's fingerprint here', 30 March 2008, *The Register*, www.theregister.co.uk/2008/03/30/german_interior_minister_fingerprint_appropriated

[22] National Center for State Courts, *Biometrics Comparison Chart*, 2002, http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html

Along with the above, additional complexity in access control arises as a result of the use of new technologies such as web services and service oriented architecture. The issues associated with these technologies are dealt with more fully in the *Monitor and review* section of this report.

Weak processes/poor management of processes

Clear policies and procedures are necessary for user-access management operations to be consistent, sustainable and well documented. If processes poorly capture the necessary operations required to perform user-access management-related tasks, assets may become exposed to significant risks as described in the *Risk analysis* section of this paper.

Well-defined and accurate processes may not always be followed by users. Possible reasons for breaching documented procedures include:

- for malicious intent

- processes may be considered too stringent or resource-intensive

- genuine error.

If, for any reason, users do not conform to documented policies and procedures, their actions may leave the related assets susceptible to compromise. Vulnerabilities arising in common user-access control procedures include:

- **Users creating accounts without approval.** Accounts created in this way may be used for fraudulent or malicious activity. Even if generated for non-malicious use, the accounts may have incorrect access privileges which could be abused by other parties.

- **Test accounts not being deleted after usage.** Test accounts frequently possess higher levels of access to systems and related information and are often not directly allocated to individuals. Processes that do not account for the termination of privileged accounts on a timely basis leave assets at risk.

- **Access privileges not changing commensurately with internal role changes.** When users change positions within an organisation, there almost always will be a change in the access privileges required, whether increasing, decreasing or a complete remapping of associated roles and privileges. If a user retains access levels from previous roles, it may be possible for the user to breach separation of duty controls, contrary to regulatory requirements and organisational access control policy.

RISK ANALYSIS

This section provides specific considerations for the risk-definition, analysis and evaluation processes. Organisations should consider the use of the assessments suggested in this section within their specific enterprise risk-management framework. The risk-analysis process should follow the general methodology described in the *Defence in depth* report[4]. The three steps to be followed are:

- identify risks

- analyse risks

- evaluate risks.

The key objective of the risk analysis phase is to analyse the organisation's information and business processes in order to determine their importance to the business, their level of exposure to threat factors, and the corresponding requirement for access controls.

Organisation context

The discussion considered in the *Establish context* section of this report provides insight into the different user threats and vulnerabilities facing organisations. However, as every organisation has different work conditions, employee culture, processes and supporting technology, the importance of considering these risk factors in the context of the organisation is magnified. Understanding individual differences between organisations will enhance the risk-assessment process, from risk identification to risk evaluation, allowing organisations to build a scope of consideration around the key issues and assets which require most attention. Some factors requiring consideration include:

- **Financial and social criticality of the business.** Organisations that are highly profitable or are operating components of a nation's critical infrastructure are likely to be at an increased threat of targeted and highly skilled malicious attacks. However, not all components and processes within the business may have significant financial and social consequences attached, and where this is the case it is important to consider threat information in this context. Key issues to consider include:
  - the stakeholders of the services and products provided by the organisation
  - potential financial consequences of a compromise within a specific business area
  - the potential flow-on impacts of a disruption to the organisation's operations
  - the competitive environment of the industry.

- **Profile of the workforce.** A mobile, flexible workforce and the increasing use of outsourced services have complicated the control structure required by organisations to manage their staff. Depending on the workforce structure, service providers and employment arrangements, as well as staff understanding of technology and security, the risk introduced by users will vary significantly from organisation to organisation. Key issues to consider include:
  - the employment arrangements for the organisation's workforce
  - the contractual arrangements for the organisation's service providers, vendors and contractors
  - the frequency with which staff members work remotely
  - staff understanding of technology used by the organisation
  - staff understanding of organisational policy on the use of information and assets.

- **Geographic spread of facilities.** Geographic dispersal of modern organisations further reduces the level of control on information access. Having numerous remote locations potentially provides additional weak points via which organisations are susceptible to

attacks. Certain members of staff may have access (both electronically and physically) to information assets in different locations. Key issues to consider include:

- locations of key assets

- use of centralised vs decentralised access control for remote locations

- physical security arrangements for the organisation's facilities.

- **Technology architecture.** The technology used by an organisation will also influence the risk exposure. Platform selection, access points as well as the number of applications used for the day to day business processing will have an impact on the level of risk faced by the organisation. Key issues to consider include:

  - entry points for the organisation's users

  - the location within the technology environment that key information assets are stored, processed and displayed

  - current access-control technologies.

User-access assessment methods

There are a number of methods to assess vulnerabilities associated with user access management, with the scoping of these tests largely dependent on the organisational context and any specific security concerns to be addressed. Using the methodology of risk identification, analysis and evaluation, a diagram outlined in **Figure 7**, along with the following assessment types can be used to provide additional insight into the extent of exposure to user-access management risks:

- social engineering assessments

- information security policy review

- physical security assessment

- infrastructure assessment

- application assessment

- user-account and access review.
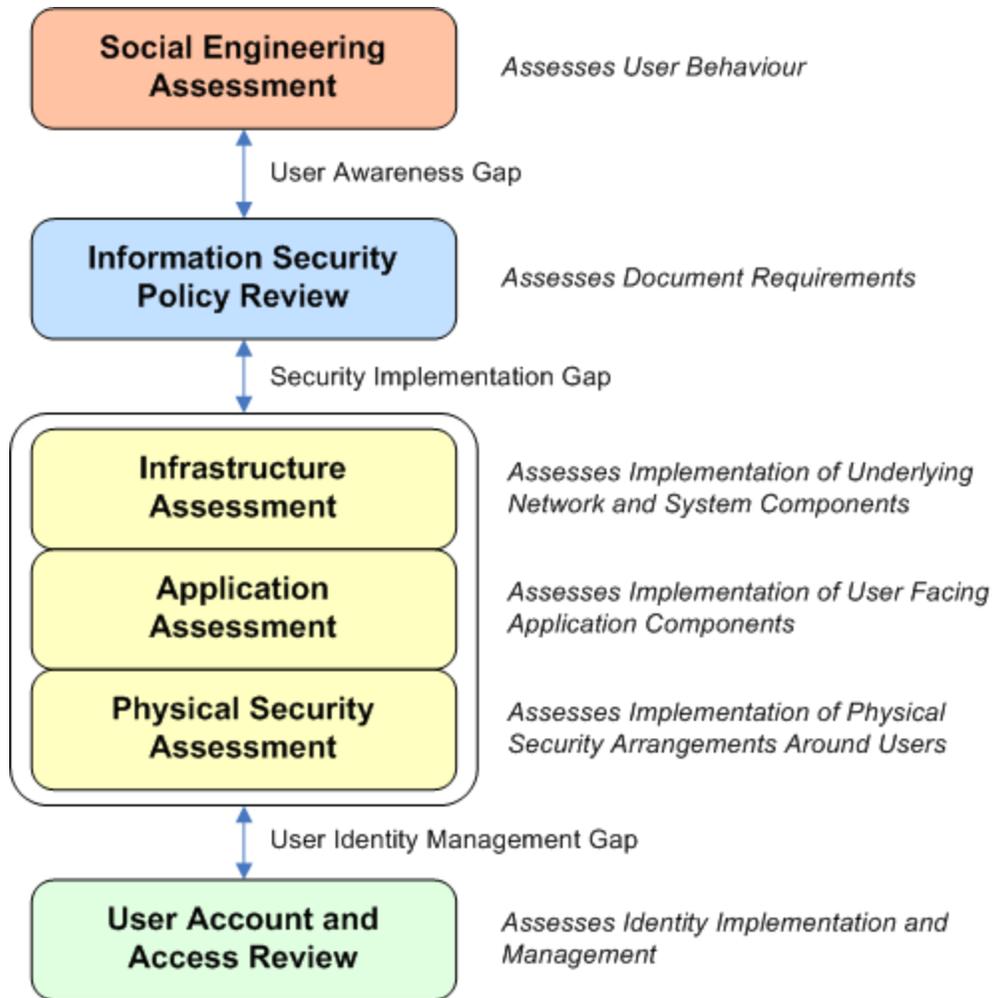
Figure 7: User-access vulnerability assessment techniques

Social engineering assessments

Social engineering is the use of influence and persuasion to take advantage of people in order to obtain information with or without technology[23,24]. Through a social engineering assessment, organisations are able to develop a view of staff awareness of information security and organisational behaviour objectives. The gap between the information security policies and procedures and the actual behaviour of users can be assessed.

---

[23] Mitnick KD & Simon LS, *The Art of Deception: Controlling the Human Element of Security,* 2002, John Wiley and Sons
[24] Karakasilitis A, Furnell SM & Papadaki M, *Assessing End-User Awareness of Social Engineering and Phishing,* 2006,
http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Karakasiliotis%20Furnell%20Papadaki%20-%20Assessing%20end-user%20awareness%20of%20social%20engineering%20and%20phishing.pdf

A typical user-access management-related exercise is to obtain, through non-technical means, a staff member's user-access credentials, for example, by way of impersonation. When conducting a social engineering risk assessment, the purpose is to seek and identify deficiencies and non-compliance in employee behaviours and established processes which could lead to unauthorised access. Assessments should be attached to clearly defined goals such as assessing[25]:

- the percentage of employees who click on a link in a phishing-like email
- help desk personnel in following protocol when the assessor is impersonating a staff member who cannot log in
- how employees react when followed through a door into a secure area.

Social engineering assessments can include some or all of the following phases:

- policy analysis
- reconnaissance
- account information disclosure assessment
- portable device usage assessment
- physical access assessment
- phishing assessment
- gap analysis
- documentation of possible risks and issues.

While the ideal target for the analysis is all staff, this is rarely practical or financially possible. A select spread across the organisation should be considered as potential targets, including:

- random sample of staff members
- reception desk staff
- IT help desk staff
- human resources staff
- contract/outsourced staff.

The overall intent of such an assessment is to identify systemic issues within the organisation, as opposed to focusing on the failings of individual staff members.

Information security policy review

Completing a review of policies and procedures in place for users and administrators will allow organisations to identify gaps in controls or potential areas where controls can be exploited.

---

[25] Zeltser L, *How to Integrate Social Engineering into an Information Security Assessment,* 2008, www.zeltser.com/social-engineering/

In order to assess an organisation's policy, a typical review will consider not only the comprehensiveness of the security requirements, but also the practicality of the policy for users, implementers and administrators. The assessment process should include:

- strategy and regulatory consistency review

- review of best practices

- review of policies, procedures and standards

- gap analysis

- documentation of possible risks and issues.

Specific to user-access management, a typical review of policy will include corporate requirements documented in the following areas:

- user-password management

- operational procedures and responsibilities

- acceptable usage of computer systems

- network access-control standards

- physical security management

- application development standards

- access-control and authentication mechanisms.

Infrastructure assessment

An infrastructure security assessment aims to determine vulnerabilities in the networks and hosts that support an organisation's information systems which may result in unauthorised access to data or resources. System and component vulnerabilities may allow attackers to subvert controls to gain access to the system. Additionally, an infrastructure security assessment will develop an understanding of the level of compliance of implemented infrastructure security controls with the organisation's security policy framework discussed above.

Specific to determining the management of user access, typical infrastructure security assessment will determine the ability to:

- gain unauthorised access to networks and systems

- view or manipulate network traffic without authorisation

- affect the availability of infrastructure supporting critical information systems.

The assessment process will typically be performed from both an internal and external perspective to indicate the different risk exposures. An internal assessment will determine the risk from a malicious insider who will already have some level of network or system access and potentially detailed insider knowledge. An external assessment will determine the risk from outsiders on the public internet or connected extranets.

A comprehensive infrastructure security assessment should include the following review components:

- vulnerability assessment and penetration testing of server systems
- system hardening assessment of server systems
- review of network architecture and security design
- review of firewall rule sets and network device configuration
- review of standard desktop operating environments.

Specific to user-access management, typical infrastructure assessment should consider the following areas:

- authentication infrastructure review
- remote access infrastructure review
- network traversal assessment
- review of access permissions
- review of intrusion detection and logging processes.

Application assessment

An application security assessment aims to identify vulnerabilities in applications and information systems deployed within the organisation that support business operations and process or store organisation data. Vulnerabilities in the application can lead to easy circumvention of access controls or the ability to gain access to application infrastructure or sensitive stored information. The assessment will provide an indication of the level of compliance of implemented application security controls with the organisation's security policy framework.

An application security assessment will typically determine the effectiveness of user-access controls including the ability to:

- gain unauthorised access to application data or functions
- launch attacks against legitimate users through the application
- compromise other user accounts or impersonate other users.

A comprehensive application security assessment will commonly include a review of application architecture and security design, and the following components by testing:

- input validation and output sanitisation mechanisms
- authentication and authorisation mechanisms
- subsystem interactions
- logging and audit trails
- error and exception handling

The following aspects of user-access management should be specifically considered during the assessment:

- authentication and authorisation mechanisms
- session management
- audit trails
- access to data via subsystems.

Physical security assessments

A physical security assessment considers the organisation's implementation of physical security controls across the organisation's facilities. Specific to user-access management, the assessment aims to determine potential weak points where an attacker could gain unauthorised access, or determine where user access is currently uncontrolled. A physical security assessment will allow the organisation to develop an understanding of the level of compliance of the implemented systems and processes to the organisation's security policy framework.

Specific to determining the management of user accesses, typical physical security assessment will determine the ability to gain unauthorised access:

- through the physical parameter
- to sensitive-zoned areas.

Assessments of physical security can be conducted from an insider or outsider perspective and cross over into elements of social engineering assessment.

A comprehensive physical security assessment should include an assessment of the following components:

- environmental security design
- monitoring systems
- entry point controls (mechanical and electronic)
- intrusion detection processes.

User-account and access review

The objectives of a user-account and access review is to determine the access rights and privileges assigned to information system user accounts within the organisation and to ensure that such access is consistent with business objectives and security principles. An account review can identify areas in which assigned access rights are not aligned accurately with roles to be identified and facilitate the revocation of unnecessary rights and privileges. An access review allows anomalous or unauthorised access to organisation data or resources to be detected and action to be taken.

A typical user-account and access review will determine:

- unnecessary access rights and privileges that have been assigned to users
- alignment of user accounts with the principles of least privilege and separation of duties
- anomalous or unauthorised use of privileged or administrative access rights

- anomalous or unauthorised use of access rights to sensitive data or resources

Tasks typically executed during a user-account and access review include:

- obtaining user-account lists and corresponding access rights
- reviewing assigned access rights against staff roles and required access rights
- identifying unnecessary privileges for removal
- obtaining audit trails of privileged access rights use and access logs for sensitive data or resources
- reviewing audit trails and user access logs against staff roles and job functions
- identifying anomalous or unauthorised access to data or functions.

Accommodating organisational context

As differences in organisational structures, work processes and technology implementations exist, the use and focus of these vulnerability assessment approaches will differ according to the specific attributes of each organisation.

Criticality of financial and social consequences. The criticality of the industry in which the organisation operates will typically influence the frequency and depth of assessments required. Industries where financial or social impacts from an information security breach are high will require more frequent assessments to be conducted and assessments to be performed to a greater depth. Critical infrastructure industries will require that all areas of information security be assessed to gain an appropriate understanding of the risk present.

Diversity of the workforce. Organisation-specific workforce factors such as the flexibility of working hours, the ability to remotely access organisational resources and the diversity of individual business units and roles within the organisation will influence areas of focus for assessments to some degree. A more diverse workforce will provide greater scope for social engineering attacks and remote access capabilities will increase the attack surface of an organisation. Thus, greater emphasis will need to be placed on social engineering and remote-access aspects to identify risks in a diverse organisation. Organisations that have a more narrowly focused workforce can typically concentrate assessments on more traditional information security aspects such as physical infrastructure and application security.

Geographic spread of facilities. Organisations with premises at multiple locations will typically require a greater assessment focus on the consistency of physical security and compliance with organisation security policy across facilities. In addition, network connectivity between sites and remote-access deployments will require specific assessment to identify risks arising from the additional interconnectivity.

Complexity of the technology architecture. The higher the levels of complexity of the technology architecture within an organisation, the higher the risk that a misconfiguration or security flaw exists within the implementation that may compromise information security. As a result, more complex architectures will require additional focus and greater depth of testing in areas such as infrastructure and application security. Furthermore, if the organisation's technology architecture involves a large number of distinct information systems, a greater emphasis on user-access and account reviews will be required for the systems deployed.

User-access management scenario: Access control for large-scale corporate data repositories	
Description	Corporate data repositories are designed to hold all of an organisation's electronic data to allow for detailed analysis and data mining, typically aggregating it from multiple information systems. The implementation of large-scale data repositories presents a substantial user-access management challenge as the aggregation of data removes a number of inherent boundaries and access restrictions present in the individual systems from which the data was sourced.
Objectives of user-access management	• Maintain consistency of user-access rights with the access rights implemented in the individual information systems. • Prevent unauthorised access to data. • Detect unauthorised access to data in the event of a security control failure. • Ensure access rights changes are accountable.
Risk analysis	A number of specific risks exist in relation to user-access management within large-scale data repositories: • User-access rights within the repository become inconsistent with access rights in individual information systems and allow users to access data within the repository that they could not otherwise access. • A failure in a repository security control may result in large-scale compromise of organisational data. • The scale of the repository may become too large for any one team or department to manage, thus requiring delegated management—conflicts may arise during the performance of user-access management activities within overlapping administrative domains. • The repository may store financial or personal information which may require regulatory or legal compliance.

Implementation	In order to respond to the risks identified above and to provide effective user-access control to data repositories, the following control items are recommended:
	• Governance
	  o Maintain a list of designated personnel responsible for authorising access.
	  o Establish appropriate policy for managing repository user access and security.
	  o Determine and define compliance requirements and verify that they have been addressed.
	• People
	  o Educate employees on the need to protect the data repository and actions required to improve security.
	  o Revoke access to the data repository upon staff termination.

| | Process Implement a user-provisioning and de-provisioning process for granting or revoking access. Implement account and access review processes to detect inconsistent access privileges granted to users or suspicious data access and activity. Implement monitoring of application and system logs, and intrusion detection or prevention devices. Technology Build access management controls on a centralised identity store. All user-access management activities should be performed on the one instance of the identity store to ensure a single consistent source of identity information is available. Implement encryption technologies to prevent unauthorised viewing of data in storage and transit. Implement strong authentication for repository users. Deploy network access controls to segregate data repository systems from the main corporate network. Deploy host access controls to prevent unauthorised access to underlying data repository server systems. Implement application-level access controls to enforce access rights to data and analysis functions. Implement logging and audit trails to allow user activity and user-management activity to be tracked. |
| Further information | Oracle, *Security and the Data Warehouse*, April 2005, www.oracle.com/technology/products/bi/ db/10g/pdf/twp_bi_dw_security_10gr1_0405.pdf |

User-access management scenario 1: Access control for large scale corporate data repositories

IMPLEMENT USER-ACCESS MANAGEMENT

The information security principles from the *Secure Your Information: Secure Your Business* paper relevant to this section are:
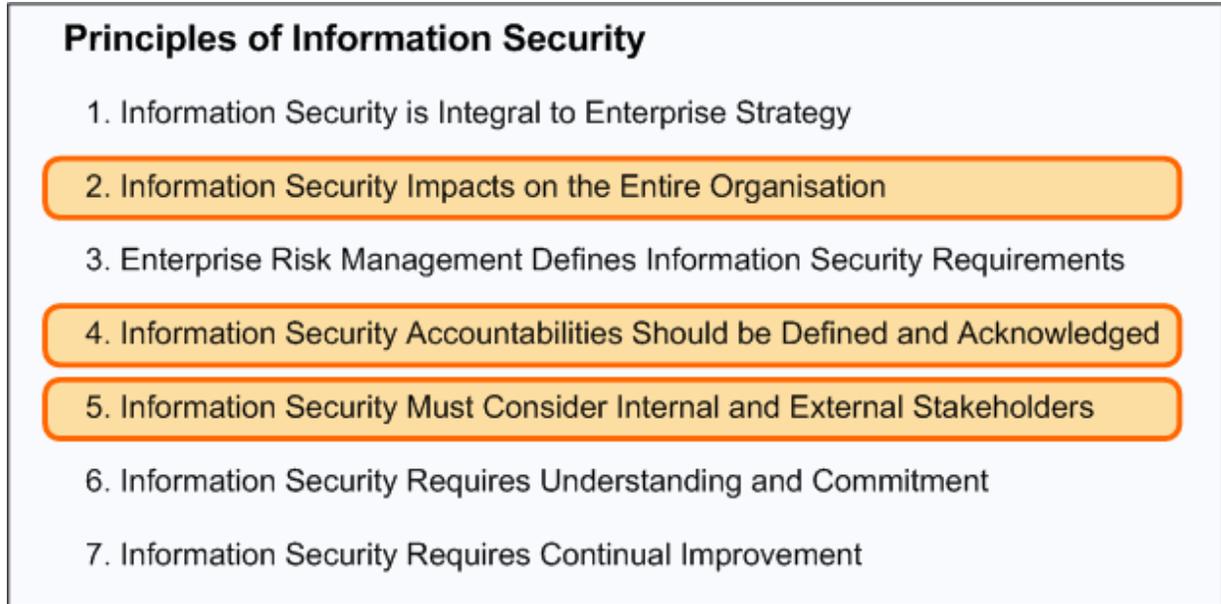

Principles of Information Security

1. Information Security is Integral to Enterprise Strategy

2. Information Security Impacts on the Entire Organisation

3. Enterprise Risk Management Defines Information Security Requirements

4. Information Security Accountabilities Should be Defined and Acknowledged

5. Information Security Must Consider Internal and External Stakeholders

6. Information Security Requires Understanding and Commitment

7. Information Security Requires Continual Improvement

Figure 8: Applicable principles of information security for implementing user-access management

In order to successfully implement user-access management controls within an organisation, a comprehensive and accurate understanding of personnel, roles and system/information access requirements is needed. This requirement is discussed in more detail in the *Establish Context* and *Risk Analysis* sections of this report.

Given such an understanding, organisations can then look to implement controls with regard to their people, processes and technologies, in order to effectively implement and manage access in line with requirements, and to mitigate risk.

It is noted that user-access management is only one control area within the full spectrum of information security and should be implemented in concert with complementary controls to provide for defence in depth. For further analysis and discussion of the principles of defence in depth, it is recommended that the reader refer to the *Defence in depth* papers prepared for the IT Security Experts Advisory Group (ITSEAG), available from www.tisn.gov.au.

This paper deals holistically with the implementation of user-access management controls. It also provides guidance on specific control techniques that may be applicable to support an organisation's user-access management initiatives.

The *Implement user-access management* section is presented as follows:

- **Core principles.** Details the core principles underpinning user-access management and providing the basis for subsequent controls.

- **Implementing governance controls.** Details the key objectives and approaches to providing information security governance oversight to user-access management.

- **Implementing people controls.** Details the key objectives and approaches to implementing user-access management controls in the management of personnel within an organisation.

- **Implementing process controls.** Details the key objectives and approaches to implementing procedural user-access management controls.

- **Implementing technology controls.** Details the key objectives and approaches to implementing specific technical controls into a comprehensive user-access management scheme.

Core principles

The core principles of user-access management are:

- **UAM-P1.** Provide the least amount of access necessary for a given user to complete their business role: 'Least privilege'.

- **UAM-P2.** Provide access to systems and information only where there is a need for the recipient of such access to have it: 'Need to know'.

- **UAM-P3.** Enforce security policy at all access points.

- **UAM-P4.** Define procedures to monitor, enable and disable access methods.

UAM-P1: Least privilege

Through providing the minimum level of access necessary for a user to complete their business role, an organisation minimises the opportunity for such access to be abused. In addition to referring to the need to provide the minimum level of access, 'least privilege' also implies that the access required be granted for the shortest amount of time possible in order to further reduce the potential for damage to occur[26].

UAM-P2: Need to know

The 'need to know' principle takes the concept of least privilege one step further by stating that in situations where a user has necessary approvals to access a given resource or piece of information—for example, the necessary security clearance level—that access should not be granted or used unless there is a genuine need for the information/resource to be accessed by that user at that time.

An example of the implementation of such a principle is organisations holding large amounts of customer data—such as banks and government agencies—with front-office staff servicing customers. Although the front-office staff are likely to have access to *all* possible records—as any customer could come in to any branch and expect to be able to be helped—the customer service staff are prohibited from viewing the data unless there is a genuine business need.

---

[26] Barnum S & Gegick M, *Least Privilege*, https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/351.html, September 2005

UAM-P3: All access points

In order for user-access management to be effectively implemented, controls must be established across all available access points. These controls should have:

Consistency—users should not be able to access unauthorised information by changing the access point through which they are connecting.

Controls relative to the risk posed by a given access point—for example, requiring two-factor authentication for internet-based access to information and only one-factor authentication for access from a local network connection.

UAM-P4: Monitor, enable, disable

User-access requirements will change over time as new systems are introduced, roles change within organisations, personnel move between roles, and personnel join and leave the organisation. Given this regularly changing access environment, the organisation must have defined and documented procedures to allow for the monitoring of user access, and processes for effectively and efficiently enabling and disabling access.

Implementing governance controls

Information security governance is the process of establishing and maintaining a framework, supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives[27].

In the context of user-access management, this refers to the importance of the organisation ensuring that access-management controls are both efficient and effective at achieving business-level objectives including:

- **Allow only authorised users to have access to information and resources.** A primary goal of user-access management is to prevent unauthorised access to the organisation's sensitive information, assets and systems.

- **Restrict access to the least privileges required by these authorised users to fulfil their business role.** As discussed in the core principles of user-access management above, this is the concept of ensuring access is granted on a 'least privilege' basis. Such restrictions ensure that users are not granted access beyond their requirements. Through limiting the access that users have to a given system, it is possible to constrain the amount of damage that can be done either through malicious intent or through unintentional/accidental actions. This corresponds closely to the risk-management concepts underpinning defence in depth, through reducing risk by reducing the potential consequences of a security incident.

- **Ensure access controls in systems correspond to risk management objectives.** Information security is one element of the broad field of risk management within organisations. User-access management is then one element within this area of information

---

[27] NIST, *Information Security Handbook: A Guide for Managers sp800-100,* 2006,
http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

security. Given the distance that often exists between the risk-management function within an organisation and teams implementing user-access controls, it is possible for these controls to be out of alignment with the ultimate risks they are seeking to mitigate. It is important that user-access management be implemented with specific threat/risk assessments and information classifications understood and targeted.

- **Log user-access and system use, and ensure auditability is maintained in line with the system's risk profile.** As well as ensuring that access is correctly allocated on a 'least privilege' basis, the defence in depth approach requires attention be given to not only protecting systems against unauthorised access but also detecting such access and appropriately responding to it. In order to detect unauthorised user access, it is necessary for a range of access-related items to be auditable, including user-access changes, use of special or high privileges, access to specific sensitive assets, and authentication failures.

Implementing people controls

In addition to specific governance, process and technology controls, a defence in depth approach to user-access management requires that the human element also be addressed.

The implementation of people controls to achieve user-access management is focused on determining and defining the access requirements that will underpin the corresponding process and technology controls that enforce access control. Additional controls will focus on security education and training of staff and the fostering of a security culture within an organisation.

Least privilege

The principle of least privilege applies across a number of people controls with the aim of reducing the risk of unauthorised access to organisation resources. By minimising the amount of access each user is granted such that users only have access to the specific resources that they require to perform their job functions[28], the risk that a user—either maliciously or inadvertently—is able to access unauthorised resources is reduced. Furthermore, the consequences of a compromised user account are also minimised as the range of actions that can be performed or the information that can be accessed through the account is limited.

Least privilege is often applied to a number of people controls and the following aspects should be considered when implementing controls:

- **Definition of staff roles and access privileges.** Careful determination of roles and privileges in line with this principle will provide staff with the access required to perform their duties but nothing further[29]. To maintain the efficiency of provisioning processes, these access requirements must be defined before the user-creation process.

- **Managing staff role changes.** Least privilege should also be considered to minimise granted privileges at any time. Thus, when an employee's role changes their access privileges also require an update to allow them to perform any new business functions that

---

[28] Ferraiolo D & Kuhn R, *Role-Based Access Controls*, 1992, http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html
[29] Purcell JE, *Employee Management Security Controls*, March 2007, www.giac.org/resources/whitepaper/application/247.php

are part of their new role. At the same time, any access privileges related to roles and functions which they no longer perform should be revoked.

- **Dynamic access criteria.** The concept of least privilege can be extended to organisation-specific access criteria such that an employee is only granted access to specific information or resources when certain conditions are met. For example, access to a specific client's financial information is only granted when the user has been actively assigned to the client and the user has been granted the general right to access client financial information. One form of this extension to traditional role-based access control is Enterprise Dynamic Access Control developed by the United States Navy[30].

- **Managing staff termination.** Least privilege is also the underlying principle for removing access for a staff member upon termination of employment. Given that the terminated employee will no longer have any requirement to access organisation information or resources, their access should be revoked or disabled to prevent unauthorised access through their user accounts. This can be managed through the exit process conducted by the organisation's human resources department.

Separation of duties

Dividing a set of functions between two roles deters fraud because a single role or user is unable to perform all the actions required to complete a transaction. However, it is important to note that fraudulent activity is still possible with separation of duties enforced, but will typically require the compromise of another user's account or collusion between users of different roles[31]. This greatly increases the chances of detection through whistle-blowing, process or technology controls and demonstrates the layered approach of a defence in depth strategy. The following aspects should be considered during implementation:

- **Definition of staff roles.** In defining staff roles within an organisation, careful consideration should be given to separating functions related to high-value or sensitive actions and transactions. A common example is to separate the initiator of a payment from the authoriser such that no role is capable of both creating and approving payments[32]. A similar principle can be applied to other critical actions such as security device configuration or user-account changes.

- **Dynamic separation of duties.** Dynamic separation of duties provides a more flexible approach by determining access based on additional criteria or attributes of the user28. For example, a dynamic policy may allow a user to be assigned both initiator and authoriser roles but prevent them from taking on both roles for the same transaction. This allows staff to remain flexible in their duties while maintaining appropriate levels of separation.

- **Managing staff role changes.** Any changes to defined roles, or staff movements between roles, will need to be assessed to ensure that required levels of separation are maintained.

---

[30] Fernandez R, *Enterprise Dynamic Access Control Version 2 Overview*, January 2006, United States Navy
[31] Szabo N, *Patterns of Integrity – Separation of Duties*, 2004, http://szabo.best.vwh.net/separationofduties.html
[32] Swanson M & Guttman B, *NIST - Generally Accepted Principles and Practices for Security Information Technology Systems*, September 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

In user-access management itself, the following roles should be separated:

- Implementation of access requests.

- Authorisation and approval of access requests.

- Monitoring and audit of user access and implemented changes.

Education and training

While most user-access management-related controls are aimed at enforcing access restrictions by limiting or revoking privileges, the education and training of employees targets the root cause by attempting to address the human element of security. Information security education and training should not simply be focused on providing set procedures to be followed or a list of specific actions to be avoided but, to be most effective, should also educate staff on underlying principles.

By equipping its staff with an understanding of information security and information security risks, an organisation is better poised to adapt and react to security issues that threaten sensitive data or resources[33]. Appropriate training of employees will also assist in fostering a 'culture of security'[34] that will allow staff to make informed decisions and respond appropriately to new or unexpected security threats.

A comprehensive education and training program should provide some degree of coverage of the following user-access management areas:

- **Acceptable use.** Staff should be educated on the acceptable use of organisation resources and made aware of access limitations such as the 'need to know' requirement, and the reasons behind these restrictions.

- **Security awareness.** Employees who are aware of security risks will be more vigilant against threats that target the human factor, such as social engineering, and more aware of actions they can take to better protect organisation assets[35].

- **Verification of authorisation**. Staff should be educated to verify authorisation for any request to access sensitive data or resources, regardless of the source.

Personnel security

A number of people security controls can be implemented in the recruitment phase to support user-access management. The following list provides some examples and their user-access management considerations:

- **Employment agreements.** Employment agreements such as employment contracts and non-disclosure agreements provide a measure of contractual protection against unauthorised access to organisation information or resources. By specifying job

---

[33] Coe K, *Closing the Security Gap*, August 2003, HR Magazine, www.shrm.org/hrmagazine/articles/0803/0803coe.asp

[34] Mendham T, *A Secure Culture*, February/March 2006, CIO Enterprise Focus: Security

[35] Wilson M & Hash J, *NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program*, October 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

requirements and tasks within employment agreements, the employee is made aware of their duties and responsibilities. Signing these documents is formal acknowledgement and acceptance of the conditions of employment.

- **Background checks and personnel screening.** Background checks and screening of potential employees provides a level of assurance that an employee satisfies certain criteria and will not pose a risk to the hiring organisation. Background checks and screening should consider factors such as trustworthiness, qualifications, psychology and behaviour, employment history and criminal history[36].

- **Job rotation.** Job rotation, when applied in conjunction with the principle of separation of duties, reduces opportunities for fraud and collusion by allowing more employees to examine and participate in business processes[29]. This increases the chances of a non-colluding employee detecting irregularities and also reduces the amount of time a malicious employee has to attempt to subvert organisation processes.

Controls

The following tables provide a good oversight into the different types of staff control mechanisms that should be incorporated into an organisation:

---

[36] CERT Publication, *Personnel Security Guidelines*, September 2004, www.us-cert.gov/control_systems/pdf/personnel_guide0904.pdf

People control: Staff roles and access requirements definition	
Description	The development of clear roles and appropriate access requirements allows security to be maintained whilst enabling staff to perform the functions required of their position.
Defence in depth	The definition of staff roles and access requirements increases the difficulty of compromising organisation data or resources by ensuring that the principles of least privilege and separation of duties are applied to staff roles and their granted access levels.
Objectives	• Prevent unauthorised access to systems by employees • Limit the range of actions that can be performed and data that can be accessed in the event of an account compromise • Limit the ability for an employee to subvert organisation business processes and commit fraud

Implementation	• Define staff roles
	   o Identify job functions within the organisation
	   o Create logical groupings of job functions into roles
	   o Re-engineer business processes to ensure appropriate separation of duties
	   o Document staff roles and assigned job functions
	• Define role access privileges
	   • For each staff role, determine and document data and resource access requirements for all assigned job functions
	   • Assign appropriate privileges to each role

References	• NIST - Generally Accepted Principles and Practices for Security Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf • Employee Management Security Controls http://www.giac.org/resources/whitepaper/application/247.php • SANS Technology Institute—Role Based Access Control to Achieve Defense in Depth http://www.sans.edu/resource/securitylab/311.php • NSA—Defense in Depth Strategy http://www.nsa.gov/snac/support/defenseindepth.pdf

Featured control 1: Staff roles and access requirements definition

People control: Staff commencement management	
Description	The commencement of employment of a staff member requires that they be assigned an appropriate role and be granted the privileges required to perform their job function. Awareness of the security policy is also necessary.
Defence in depth	A staff commencement procedure reduces the attack surface of an organisation by ensuring that user accounts are created only after appropriate approval and user-access rights are granted in line with job function and adhere to the principle of least privilege. Providing staff with knowledge of security policies builds a foundation of security awareness and vigilance.
Objectives	• Prevent unauthorised access to resources by employees • Prevent unauthorised physical access to facilities in line with business needs • Raise new staff awareness regarding policy requirements and role responsibilities specific to security • Limit the range of actions that can be performed and data that can be accessed in the event of an account compromise
Implementation	• Implement a user-provisioning procedure • Execute an account request form approved by involved functional managers • Assign access cards and keys to the employee • Create user accounts on required systems • Grant privileges on created user accounts in line with job function and role • Document all access granted, both physical and electronic • Provide security training as part of the induction process
References	• NIST - Generally Accepted Principles and Practices for Security Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Featured control 2: Staff commencement management

People control: Staff termination management	
Description	Staff termination management involves the maintenance of appropriate access controls related to an outgoing staff member.
Defence in depth	A staff termination procedure reduces the attack surface of an organisation by ensuring that obsolete user accounts and access rights are no longer available and cannot be used or targeted by a malicious user. Instead, an attacker must compromise active accounts with a greater risk of detection. An additional layer of protection can be provided through ensuring that frontline staff are aware of the termination, in order to reduce social engineering risk.
Objectives	• Prevent unauthorised access to resources through access previously assigned to a terminated staff member • Provide awareness of staff member termination to key personnel • Maintain legitimate access availability following termination

Implementation	• Implement a user de-provisioning procedure
	  o Execute sign-out form by involved functional managers
	  o Execute sign-out form by terminated party
	  o Disable terminated employee user accounts on all systems
	  o Recover access cards, keys, and other authentication tokens from the terminated employee
	  o Advise key staff members of termination
	  o Review sign-out forms to ensure removal of all access
	  o Escort the terminated employee from the premises
	  o Reassign control and ownership of data and resources previously assigned to the terminated employee
	• In the event of a genuine risk of a staff member causing malicious damage to the organisation's information or systems, an emergency de-provisioning procedure to provide for immediate access removal is also recommended.

References	• NIST - Generally Accepted Principles and Practices for Security Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Featured control 3: Staff termination management

People control: Staff role change management	
Description	Managing staff role changes includes the holistic approach to handling changes in user-access requirements in the event of a job functional change, promotion or transfer between departments.
Defence in depth	New access rights must be verified against documented roles and responsibilities. Old access rights should be disabled if not required, as if the user is terminated from the previous position. Relevant managers must provide approval before privileges are granted for the new position. Further controls should be implemented for roles requiring access to sensitive resources.
Objectives	• Provide ongoing validation that staff access is supported by business requirement • Reduce information leakage between intentionally segregated parts of the organisation (e.g. 'Chinese walls')

Implementation	• Develop formal access review and approval processes for role changes:
	  o Enforce documentation and review of required user access and its necessity for business purpose
	  o Review existing access provisions and revoke access not required for business purposes
	• Conduct periodic audits of access changes after role changes to assess compliance with roles-based access policy

Reference	• Mallery et al—*Hardening Network Security*, McGraw-Hill Osborne Media, 2005, p468 • Chillakanti, C—*Role-based Information Security: Change Management Issues*, ACM International Conference Proceeding Series; Vol. 90, 2004

Featured control 4: Staff role change management

People control: Education and training	
Description	The education and training of users to raise security awareness within an organisation.
Defence in depth	Education and training aims to address the human element which is often considered the weakest link in the information security chain. By instilling security awareness within all staff members, an organisation is more capable of reacting appropriately to new security threats and detecting malicious activity through increased vigilance.
Objectives	• Increase security awareness and vigilance among staff members • Reduce susceptibility to social engineering attacks

Implementation	• Hold information security awareness workshops and training courses for employees covering:
	  o Information security principles
	  o Information security risks
	  o Social engineering
	  o Information security procedures
	  o Actions to avoid
	• Provide a point of contact for information security enquiries
	• Develop and distribute security awareness material
	  o Brochures
	  o Posters
	  o Workstation desktop wallpapers

References	• Mark Wilson and Joan Hash, *NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program*, October 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Featured control 5: Education and training

Implementing process controls

Because a large part of user-access management relates to organisational processes, the following process issues identified in the full *Defence in depth* report are relevant for consideration with respect to user-access management controls:

- the presence of documented methods to govern the operations of the organisation

- the existence of formal training in these methods

- the degree to which the organisation effectively implements the methods, observes compliance and assesses performance

- good procedural design and good adherence to the process

- the need for information classification.

Processes in user-access management are generally captured in an access control policy and associated standards and procedures. Key processes within user-access management include:

- user provisioning—requesting, establishing and issuing user accounts

- user de-provisioning—closing user accounts

- access change management—adding or removing access from an existing user account

- user-access audit and review

- access-breach detection—processes to support the identification of access breaches.

User provisioning—requesting, establishing and issuing user accounts

User-provisioning processes require significant flexibility to deal with the variation in access requirements and user types in organisations. Valid user accounts can be required for:

- employees
- contractors
- vendors
- partners

- customers
- groups of users
- other recipients of a service.

Access by these users may then be required to an equally broad range of assets and information including:

- inbound or outbound network access
- email
- inclusion in a published user directory
- access to a database

- access to a file server
- access to an application
- other system access requirements.

In order to gain access to information and systems—for all such scenarios above—users should be required to proceed through a formal user registration process, incorporating the following:

- authorisation of access by the relevant system owners via a formalised and documented process

- acknowledgement by users of their understanding and acceptance of the conditions of their access to the relevant information and systems.

As a result of the breadth of user-access requirements described above and in the *Establish context* section of this report, these processes must be flexible and timely.

Privileged access

Privileged access is any access where the user can bypass established system controls. This would include, but is not limited to, database administrator (DBA), network and system administrators and default ('root') operating system accounts. Privileged access methods should be subject to the following additional requirements:

- the creation of privileged user access should require authorisation of both the relevant system owners and also the information security manager

- privileged access rights are to be assigned to different user accounts from those used for day-to-day activities—ie, staff should not use privileged accounts for their primary job role

- all changes to privileged accounts should be logged and auditable.

Although privileged access implies a degree of trust in the user being granted such access, core principles such as 'least privilege' and 'need to know' should continue to be applied.

User de-provisioning—closing user accounts

A key process in information security is the correct removal of access privileges at the point of staff termination, or where the account is no longer required. As is identified in the list of prospective users above, many users may not be staff of the organisation and user access records may not be easily centralised with the human resources department.

Key elements of the de-provisioning process include:

- ensuring that all user accounts allocated to a user are known and addressed

- having an established timeframe for disabling an account and subsequently removing the account

- completing de-provisioning tasks in a timely manner to remove any potential for access to systems after leaving an organisation or role

- having the capability to implement an 'urgent' de-provisioning in emergency situations to immediately mitigate the risk of a rogue employee

- ensuring that files associated with those user accounts are backed up or otherwise archived before the accounts are removed.

At a technical level, redundant user IDs—that is, user IDs associated with terminated staff— should not be reissued to other users. The reissue of previous user IDs magnifies the risk of the new user gaining unintended access levels associated with the previous user.

Access change management—adding or removing access from an existing user account

Access rights should be reviewed and updated/revoked before a user changes job roles or leaves the organisation. This process will generally be instigated either by the human resources department (in the case of permanent staff) or the IT department (in the case of consultants or other third parties).

When transfers of employment may lead to breakdowns in 'Chinese wall' implementations, additional criteria and/or controls should be placed on staff members. Staff transfers of this kind may be limited or discouraged altogether.

User-access audit and review

As defined by the *Defence in depth* strategy, it is necessary not only to implement controls to protect against unauthorised access, but also to implement controls to detect such access and respond appropriately. In order to detect incorrect access privileges, all user-access profiles should be subject to the following reviews, coordinated by the Information Security Manager:

- Review of all user-access rights by the system owners on a periodic basis (recommended to be at least every six months).

- Review of all privileged (e.g. administrative) access rights by the system owners on a periodic basis (recommended to be at least every three months).

- Regular monitoring by the system administrators of access activity to identify and remove inactive/redundant accounts—for example through identifying accounts not used in the past 90 days.

In addition to the review of privileged accounts conducted by the system owners, it is also recommended that the Information Security Manager complete an independent review of privileged user access on a regular basis.

The frequency of all the above reviews is to be agreed by the system owners and the Information Security Manager, based on the risk and threat profile of the relevant system and the specifics of the user base.

In addition to these process reviews, technical testing of access-control components is also recommended and can include:

- password strength testing—using a password-cracking tool to attempt to break weak passwords

- access-control testing—using penetration-testing techniques to attempt to circumvent access-control mechanisms.

Access breach detection—processes to support the identification of access breaches

In order to detect unauthorised access or incorrect access privileges, all user-access profiles should be subject to weekly or daily monitoring by the system administrators. Technical controls are also available to support the identification of unauthorised access through heuristic

analysis of user behaviour. This involves analysis of user-access patterns over time, and attempts to detect anomalous activity that could indicate unauthorised access is occurring.

At a process level, the key requirement created by such a scenario is the need for organisations to have clearly defined the 'normal' access requirements of staff and to have identified critical assets and systems for specific monitoring.

In the event of a breach being detected, organisations should seek legal advice regarding their specific requirements under both Australian and international law. Specific legislation exists in the US state of California—known as Senate Bill 1386 (SB1386)—and a number of other US states, and is currently being considered in Australia and many other countries.

Dependent on the specific legislation and the type of data subject to breach (as legislation is generally targeted at information related to individual consumers), there may exist obligations for an organisation to make a disclosure, contact the subject of the records breached, or otherwise report and respond to the event.

Given such legislation, it is important for organisations to have internal processes designed to respond to such breaches, with specific involvement of legal and communications teams within the organisation.

Process control: User-activity auditing	
Description	User-activity auditing is the process of verifying the appropriateness of access rights and abuses of those rights.
Defence in depth	User-activity auditing examines access to information from all areas of the organisation, ensuring that a single failure to identify unauthorised access does not go unnoticed. By reviewing all permissions and the appropriateness of their use, the cost of attack is increased due to the additional effort required by attackers to conceal their actions.
Objectives	• Identify unauthorised access to systems and information resources • Prevent unauthorised access by identifying superfluous access rights

Implementation	• Obtain and review information access rights:
	  o Retrieve user accounts and permissions
	  o Ensure accounts do not have excessive access rights
	  o Ensure adequate account logging is in place
	  o Interview stakeholders to ensure permissions are current
	• Review access logs and audit trails:
	  o Gather system and security device log files
	  o Aggregate and correlate audit data
	  o Identify anomalous behaviour
	  o Identify unauthorised access

Reference	• NIST - Generally Accepted Principles and Practices for Security Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf • Linares M - Identity and Access Management Solution www.sans.org/reading_room/whitepapers/services/1640.php

Featured control 6: User-activity auditing

Process control: Account and password policy	
Description	Policy must be developed and implemented to support effective account management and protection. This policy should provide clear guidance regarding account username and password constraints. Circumstances in which accounts should be disabled or temporarily suspended must be identified and clearly documented.
Defence in depth	To implement defence in depth, the policy should include controls which provide requirements for configuration, maintenance, monitoring and change management for passwords and accounts.
Objectives	• Ensure practicality of account and password policy for users. • Reduce the risk of account intrusion.

Implementation	• Identify systems impacted by password and account policy
	• Define password controls:
	  o Define minimum password review cycle (monthly)
	  o Define minimum complexity and length (at least seven characters and including numeric, alphabetic and symbols)
	  o Define maximum age of passwords (90 days)
	  o Define password renewal requirements (user's new password cannot be the same as any of their previous four passwords)
	• Define account management controls:
	  o Define minimum account review cycle (90 days)
	  o Define maximum number of login attempts allowed prevents brute-force attacks (maximum six attempts)
	  o Define account username naming conventions (unique)
	• Inform users of policy requirements:
	  o Communicate policy to business units and identify timeframe for compliance
	  o Provide user support services to maximise policy effectiveness

Reference	• Vanover R—Lock IT Down: Make a Password Policy Part of Your Security Plan, http://articles.techrepublic.com/5100-1035-103 • NIST—Generally Accepted Principles and Practices for Security Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Featured control 7: Account and password policy

Process control: Access-control change management	
Description	Change management facilitates effective administration of systems, resources, and access controls, including maintenance of privileges and roles definitions. Audit of these procedures provides assurance of administration and management activities.
Defence in depth	Access-control change management enables defence in depth through providing tiered levels of user access based on business need. Through escalation and approval of potential changes, a layer of oversight is provided.
Objectives	• Maintain ongoing business relevance for all access allocated • Minimise unauthorised changes to access controls • Ensure visibility of all changes made to access controls

Implementation	• Develop standardised procedures for reviewing change management of access controls
	  o Identify all instances where access changes are required by the business
	  o Identify roles and responsibilities for access change control auditing
	  o Develop documentation tools
	  o Develop detailed review and escalation steps
	• Maintain knowledge of changes to access controls
	  o Implement real-time monitoring of access control updates where possible
	  o Inspect access-control lists (ACL) and access logs for applications and databases

Reference	• Schwartz, M—*"IT Compliance Institute—Access Control: 10 Best Practices"*, www.itcinstitute.com/display.aspx?id=3265 • NIST—Generally Accepted Principles and Practices for Security Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Featured control 8: Access-control change management

Process control: Access revocation	
Description	Access revocation is the process of removing building, system and information access rights in the event of malicious activity being identified, changes to user role or the termination of an employee.
Defence in depth	Access revocation contributes to defence in depth by increasing the difficulty of compromising organisation information or resources. This is done through minimising assigned privileges and access rights upon role change or employment termination. The access revocation process is also used as a reactionary measure to limit impacts of a security breach when malicious activity is detected.
Objectives	• Revoke access to resources for identified threats • Minimise damage by reacting to attacks promptly
Implementation	• Develop procedures to revoke access for staff, encompassing: o Building access o System access o Network and remote access o Application access o Telephone system access • Develop procedures for reinstating access where revocation has been in error
Reference	▪ NIST - Generally Accepted Principles and Practices for Security Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Featured control 9: Access revocation

Process control: Privilege management	
Description	Privilege management is the process of restricting privilege allocation and escalation within an organisation in accordance with least privilege principles, and auditing changes to user privileges to ensure adherence to least privilege principles.
Defence in depth	Privilege management enhances defence in depth by reducing the opportunities available for fraudulent activity or collaboration with outside attackers by staff, and ensures users can only access information relevant to business purposes.
Objectives	- Prevent fraudulent activities or collaboration with outside attackers by users - Ensure business relevance of all allowed user actions
Implementation	- Implement a standardised procedure for allocating and managing user privileges - Apply least privileges guidelines to job roles when determining required user privileges. - Document all user privilege allocation and changes - Develop formal privilege request and escalation procedures. - Maintain oversight of privilege escalations - Develop authorisation procedures for user privilege escalation. - Audit user privilege escalations for compliance with least privilege principles.
Reference	The Gilbane Report—*Privilege Management & Rights Management for Corporate Portals* Audit compliance with least privilege access, 2001, www.gilbane.com

Featured control 10: Privilege management

Implementing technology controls

First and foremost, user-access management is concerned with protecting organisational information resources. Therefore, user-access management security mechanisms must be applied to those resources in storage and in transit. While those resources will be identified during earlier phases of risk management, technical controls will be applied at the following layers to protect those resources:

- **Information**—individual documents, databases, and data points within can be controlled through cryptographic techniques.

- **Application**—applications are used to control how information resources are used and displayed and can therefore be used to control access.

- **Host**—information is stored on host systems which can be configured to control user access to data stored within.

- **Network**—user access to individual networks can be controlled to prevent unnecessary exposure to those not requiring access to information traversing those networks.

When selecting technology solutions for user access control, system designers should consult approved technologies under the Common Criteria (ISO 15408), as these certified products have been evaluated under a rigorous and standardised approach. Access control components assessed under the Common Criteria will have had the functional access control behaviours described in the Protection Profile or Security Target verified, with testing including consideration of the:

- subjects under control of the policy

- objects under control of the policy

- operations among controlled subjects and objects covered by the policy.[37]

Core principles and technology

As discussed in the *Core principles* section, part of the management processes for an organisation's technology include:

- **UAM-P1: Least privilege.** Technology offers an excellent opportunity to implement least privilege because components, permissions, and access can be both extremely broad and extremely granular at the technology level. Wherever an application or other technology action occurs, the process can be tuned to only execute in a 'pseudo prison', where no other actions on any other components—outside those required—are permitted.

- **UAM-P2: Need to know.** While processes and governance can mandate that people have no access to information they do not have a specific business need to access, technology

---

[37] Common Criteria, *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 2*, www.niap-ccevs.org/cc-scheme/cc_docs/CCPART2V3.1R2.pdf, September 2007

can be used to physically and virtually enforce these mandates. Typically, this is implemented in the form of access controls, most commonly at the application level.

- **UAM-P3: All access points.** Given that most access points to information within an organisation are now virtual (i.e. technology-based), identifying and implementing controls within the technology is often the most efficient course of action. This has become more apparent in recent times as telecommuting and remote-access solutions have become a greater part of everyday work.

- **UAM-P4: Monitor, enable, disable.** Once procedures for the monitoring, enabling, and disabling of access methods have been defined, technology can be used to make these more efficient. As stated in the discussion of UAM-P3 above, technology controls most access points to information and is therefore a reasonable and effective means of implementing management controls.

Specific user-access management information resources

User-access management technologies also add a significant amount of sensitive information to an organisation, which in turn must be protected. This information (e.g. access credentials) is often considered highly sensitive as it is, in essence, the 'keys to the kingdom'. An attacker that gains access to the necessary credentials can potentially leverage that information to gain access to all other resources in the organisation.

The following user-access management elements require protection in a defence in depth strategy:

- **User identifiers.** Often in the form of network usernames, user identifiers are bound to individuals and sometimes applications. Once a user is authenticated, the identifier is used to restrict access and bind actions to audit trails.

- **User authentication credentials.** These values are only available to the individual user to whom they are bound. They can be something a user knows, possesses, or is (i.e. a part of their physical make-up, such as fingerprint) and are used as proof of a claim of identity.

- **User roles and permissions.** Authorisation information can be held as roles and permissions assigned to users.

- **Access control lists.** Authorisation information can be held in the form of access control lists which are applied to resources, as opposed to users.

- **Cryptographic keys.** These secret tokens are used to unscramble information which has been encrypted.

In general, user identifiers, user roles and permissions, and access control lists can be public or private. However, maintaining their confidentiality is not strictly required for security. These items require only that their integrity be maintained. Conversely, user-authentication credentials and cryptographic keys must remain confidential as they act as access passes to organisational information and systems.

User-access management information paths

The information paths for specific organisational assets should be determined within each organisation and will depend on the individual usage of those assets. However, in general, specific user-access management resources have the following information paths, and security requirements along those information paths.

Information path

To be useful, information is transmitted between users and systems. This information can be compromised anywhere along the path travelled. Thus, all the information paths must be determined in order to allow for controls to be applied at all required points on the path.

The information contained in **Table 2** highlights that integration of the information resources links with the various information paths and the security requirements that are required to maintain confidentiality, integrity and availability of an organisation's information systems.

	Security reqs.		
	Confidentiality	Integrity	Availability
User identifiers			
Stored on the end-user's system		✓	✓
Transmitted to the authenticating system and application		✓	✓
Sometimes transmitted to centralised authentication services		✓	✓
User authentication credentials			
Stored on the end-user's system	✓	✓	✓
Transmitted to the authenticating system and application	✓	✓	✓
Sometimes transmitted to centralised authentication services	✓	✓	✓
User roles and permissions			
Stored on the end-user's system			✓
Stored in a centralised user repository		✓	✓
Transmitted to systems using centralised authentication services		✓	✓
Transmitted to end-user's system			✓
Access control lists			
Stored on the system being protected		✓	✓
Sometimes transmitted to the accessing system/application			✓
Cryptographic keys			
Sometimes stored on end-user's system	✓	✓	✓
Sometimes stored in a central key store	✓	✓	✓
Sometimes stored on backup media	✓	✓	✓

Table 2: UAM Information paths and security requirements

Defence in depth controls should be implemented to ensure security requirements are met and to ensure access-control technologies and credentials themselves are secure.

Data-access control

Data-access control is most often applied when the data needs to be stored and transmitted over an untrusted or untrustworthy medium. Such circumstances are often unavoidable but it is still necessary to control access to the information. Additionally, applying data-access control, even when not strictly required, adds an additional layer of protection in a defence in depth strategy.

Specific technologies used to implement data-access control include:

- **Public key cryptography.** This technology allows for information to be encrypted in such a way that it can be decrypted only by a certain set of users who possess the 'private keys' necessary, as designated by the user who originally encrypted the data.

- **Symmetric key cryptography.** This technology allows two interacting entities (users) to share a single 'key' which both encrypts and decrypts information. In this way the information can be distributed but read by only those provided the secret key.

- **Digital signatures.** Public key cryptography also allows for small 'fingerprints' or hashes of information to be encrypted with individuals' public keys, essentially forming a signature. This technology both verifies the source of the information as well as integrity of the data over time and between sender and recipient.

While there are many specific data-access control technologies available to organisations, they can also be difficult to manage and implement. It is therefore important that the application of these controls is based on business need and information sensitivity.

Application-access control

Applications present information to users and convert raw data into information that is useful to an organisation. As a result, it is the ideal location for implementing access-control mechanisms, particularly where custom applications are concerned. However, even commercial off-the-shelf applications offer very flexible application-access controls.

The following application-access control techniques can be applied:

- **Fine-grained access control.** Because applications implement the business logic of an organisation's information functions, they can be used to restrict access to those business functions at a very detailed level. This includes restricting access to individual data fields, processes, functions, contexts, user groups etc.

- **Fail closed (deny by default).** If an error or undefined state occurs in an application, it is important that it fail gracefully, and prevents access. In doing so, it will prevent unauthorised access by users who are able to cause errors as required.

- **Access logging.** As applications understand business context they are best placed to provide the most comprehensive and most appropriate audit trail.

- **Code security.** Modern application frameworks allow source code to be developed in such a way that individual routines have access criteria assigned during development. Once the application is running, the framework will validate the user identity before executing the previously marked routines.

Host-access control

Before accessing an application, and then during application execution, both the user and the application must access local host resources. Host-access controls limit and manage the level of access provided in these processes.

The following host-based user-access control mechanisms are available:

- **File and directory permissions.** In a computer system, information is stored in files and organised in directories. Applying permissions to those files and directories is possible in all modern operating system and can provide a strong access-control mechanism.

- **Program permissions.** These are a means of controlling programs, particularly client programs that have been taken over, and preventing them from accessing key system resources and information.

- **Host firewalling.** Implementing a firewall on the local host decreases the attack surface of the system. This mechanism is also part of most modern operating systems and usually requires only minor configuration changes.

- **Disk encryption.** If a system has access to sensitive information or is used to access sensitive information, that information can be protected from physical compromise by encrypting the entire hard drive, allowing only authorised users to access data.

- **Access logging.** Each individual host can log access at a variety of levels, be it at the file system, network stack or system kernel.

Network-access control

Network access control is the primary network perimeter security mechanism as well as a basic internal protection. In general, the role of network-access control is to prevent access to a system before any potential attacker can establish a direct connection to those systems.

The following is a sample of network-access control mechanisms available:

- **Network segregation.** In order to prevent access to networks, those networks must first be established and segregated. Segregation can occur at many levels but should be enforced whenever information access requirements within that network change to those outside, based on the 'need to know' principle.

- **Network authentication.** Implementation of protocols such as 802.1x ensures that only devices which have been adequately identified can join a network.

- **Perimeter firewalling.** This long-standing technique continues to significantly reduce the attack surface of an organisation. However, in today's environments, firewalling must extend to examining application protocols to prevent unwanted application traffic from entering the organisational perimeter.

- **Virtual local area networks.** One form of network segregation is the virtual local area networks, which creates a pseudo-network limiting access to only member devices.

- **Demilitarised zones.** The demilitarised zones are a network, especially segregated to be externally facing. The role of this network is to manage user trust and provide access to inner organisational resources only if a user is authorised.

Physical-access control

Physical-access control is necessarily a major part of user-access management. If a user is able to physically walk away with an information resource, the majority of electronic protections can be ineffective.

Defence in depth originated in the physical-access control domain and is therefore ideal for applying these principles in layers. Perimeters can be established at various distances from a resource, multiple choke points established, and monitoring mechanisms deployed throughout.

The following is a sample of physical-access control mechanisms available:

- **Network media control.** To protect against attacks which require proximity, access to network media such as network cables, network ports, and wireless access points should be restricted or limited.

- **Surveillance.** There are many forms of physical surveillance and monitoring available, including video cameras, infrared sensors and door alarms. Implementing one or more of these will aid in detecting and tracking physical intrusions.

- **Entry locks.** Each door or other entry provides an access point to the organisation. Implementing locks at various levels from the external entry to the door to the communications room will significantly increase attack cost.

- **Access tracking.** In order to monitor users who have access rights to a facility but may wish to abuse those rights, access tracking with proximity cards or other sign-in/sign-out mechanisms should be used.

- **Multiple perimeters.** Creating multiple physical perimeters is a core concentration of physical-access control. Perimeters are created through physical barriers such as fences and building walls, preventing access from less critical areas to more critical ones.

User authentication

User authentication is well supported by technologies. By using multiple technologies, it is possible to increase the cost of an attack significantly, with the goal of forcing the attacker to look for alternative attack vectors in less-critical processes.

The following is a sample of user-authentication mechanisms available:

- **Passwords.** Passwords or pass-codes are the most common type of authentication credential. In a multi-factor system, they are considered 'something you know'.

- **Tokens.** Tokens are small hardware devices that must be in the user's possession to prove identity and in a multi-factor system are considered 'something you have'. They are significantly harder to manage than passwords but typically require a physical compromise of a user.

- **Biometrics.** The use of personal physical characteristics, or 'something you are', provides another level of security, requiring an attacker to do more than steal a physical device or password. However, biometrics has significant management issues as described in the *Establish context* section of this report.

- **Multi-factor authentication.** Using a combination of passwords, tokens, and biometrics (often referred to as two-factor authentication when two are used), provides increased authentication strength. In line with defence in depth, the attacker must compromise multiple credentials in order for an attack to succeed when such a system is employed.

- **Standards enforcement.** Today's authentication systems implement policy management, allowing minimum security configurations such as password length, password complexity, maximum failed retries, and account lockout to be enforced.

- **Centralised authentication.** As the number of individual systems and applications grows and the number of users and credentials increases, authentication management can become prohibitive unless it is centralised. Directory services such as those based on LDAP (lightweight directory access protocol) can help to alleviate the burden. Additionally, most centralised authentication systems provide well-tested and highly secure protocols such as Kerberos.

Credential management

The strength of any authentication system is limited by the strength of the credentials it uses to verify users. Consequently, credential management is integral to user-access management as it protects both users and the systems they access.

The following is a sample of credential management mechanisms available:

- **Public key infrastructure.** Public key cryptography requires that users' keys be managed and maintained. In any large deployment, this requires 'certification authorities', including appropriate technology and operating procedures, to manage these keys.

- **Key generation and revocation.** The strength of modern cryptosystems relies on the strength of the keys it produces. Therefore, care must be taken to ensure keys are generated such that they are random and unpredictable, and that they are revoked system-wide in the event of a compromise.

- **Password hashing.** Storing and transmitting passwords in clear-text (unencrypted) leaves them vulnerable to being read by unauthorised users. The cryptographic process of hashing—creating a small digest from which the password cannot be easily gleaned—should be used as it provides a much safer alternative.

Logging and detection

Logging and detection integrates well with technology because anywhere technology is accessed, that access can be logged and analysed automatically. Various point and holistic solutions are now available to log, monitor, analyse, and provide an alert of suspicious activity.

The following is a sample of logging and detection mechanisms available:

- **Device logging.** There are many devices on the network which perform both security and business functions. The majority of modern devices such as routers, firewalls, gateways, antivirus management systems, can produce detailed logs of activity.

- **Correlation engines**. Given the vast amounts of log data available from the many network-attached devices creating audit trails, a correlation engine can be used to match and cross-reference this data to create a clear picture of events.

- **Centralised logging**. For maintenance purposes, log data should be passed to a central data store where it can be secured. Additionally, remote logging ensures that unauthorised access to a system cannot result in destruction of the audit trail.

- **Alarms and alerting.** In order for response mechanisms to be executed effectively, timely notification of any unauthorised access is paramount. In most of today's security products

and centralised logging systems it is possible to configure real-time alerting functions to notify administrators of any security events, including unauthorised users.

User-access management scenario: Remote access to unmanned sensors and platforms	
Description	Supervisory control and data acquisition (SCADA) systems are real-time process control systems used to monitor and control industrial equipment. A range of critical infrastructure industries use unmanned sensors or platforms as a component of their SCADA systems. Such industries include: • Oil and gas • Power generation and transmission • Water management Assets now exist that are unmanned, creating a new set of access control challenges—both for physical access control and logical access control in order to provide for remote operation. Programmable logic controllers (PLCs) allow valves, alarms, pressures and other elements to operate autonomously and report to a master terminal unit (MTU) which in turn reports to a remote host computer providing a human machine interface (HMI) to the operator. Unmanned sensors can be accessed by a variety of transport mechanisms, including: • Radio • Wi-Fi/WiMax (wireless) • Dial-up modem • Leased lines
Objectives of user-access management	The integrity and availability of SCADA systems and system components is crucial to ensure the safe and effective operations of the systems. The objectives of user-access management in the context of remote sensors and assets are: • Ensuring that unauthorised users are not able to connect to remote sensors and manipulate data or operations. • Ensuring that authorised users are able to connect to sensors on an as-required basis without interruption or obstruction.
Risk analysis	A number of specific risks exist with regard to remote access for unmanned sensors and assets: • Many technology components, by default, allow for anonymous access, or use default credentials. • Remote-access technologies for SCADA systems are often based around insecure clear-text communications protocols with no integrity verification mechanisms. • Generic accounts such as 'console' or 'administrator' render audit trails ineffective. • Proprietary protocols in many cases do not integrate with data encryption, authentication or authorisation controls.
Implementation	In order to respond to the risks identified above and to provide effective control of remote access to unmanned sensors and

<table>
<tr><td></td><td>

platforms, the following control items are recommended:

- Governance
  - Conduct a risk assessment of device connectivity and access controls.
  - Maintain a list of designated personnel responsible for authorising access. Verify this list annually.
  - Establish appropriate policy for accessing unmanned sensors or assets—including that direct access should only be used in emergencies.
- People
  - Revoke remote access within 24 hours for personnel terminated with cause, and within seven days for personnel who no longer require access.
- Process
  - All access to systems is to use individually allocated accounts. Where this is not possible, establish processes for management of audit trails associated with generic accounts.
  - Where technically feasible, establish monitoring processes or technologies to detect and alert attempted unauthorised access in real time. Where real-time alerting is not feasible, establish processes for reviewing access logs on a regular basis.
  - Establish and communicate strong password standards.
- Technology
  - Change or remove default user accounts and credentials.
  - Operate perimeter devices on a 'deny by default' model.
  - Implement encryption for sensor/platform management protocols where possible.
  - Segregate networks to minimise direct access to sensors.

</td></tr>
<tr><td>

Further information

</td><td>

- North American Electric Reliability Corporation (NERC) Standard Cyber Security Standards
- Dhameja S, SCADA System Security Management, 2007, www.infragardmembers.org/modules/content/index.php?id=44
- Lewis C, Coming of age: The economic case for large-scale use of wireless sensors is overwhelmingly favourable, July 2005, www.isa.org/InTechTemplate.cfm?Section=article_index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=45290
- Crocker M, Platforms, Pipelines, and Pirates, June 2007, http://goliath.ecnext.com/coms2/gi_0199-7175606/Platforms-pipelines-and-pirates-Special.html
- Smith P & Kimball M, Offshore Oil Rigs Chat, accessed 2008, www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentI

</td></tr>
</table>

	D=25117
	• Maynor & Graham, SCADA Security and Terrorism: We're Not Crying Wolf, 2006, www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

User access management scenario 2: Remote access to unmanned sensors or platforms

Controls

Technology control: Authenticate users	
Description	Electronic authentication is the process of establishing confidence in user identities electronically presented to a physical or information asset. This ensures only authorised users have access to system resources and/or data.
Defence in depth	A strong user-authentication policy combines multiple-factor authentication. This forces attackers to obtain multiple identification components in order to impersonate a user. Furthermore, enforcement of standard login/physical access configuration and use procedures reduces the likelihood of various authentication guess attacks.
Objectives	• Prevent unauthorised access to facilities, resources or data • Detect attempts to access resources by illegitimate users

Implementation	• Implement multiple factors of authentication based on the criticality of the facility, resources or data:
	   o Cryptographic tokens
	   o Biometrics
	   o Passwords/Passcodes
	• Enforce login policy
	   o Limited login attempts
	   o Enforce access criteria such as time of day
	   o Enforce standard access and login procedures
	   o Account lockout
	• Employ centralised authentication and directory services

	• NIST—Electronic Authentication Guidelines http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Featured control 11: Authenticate users

Technology control: Network-access control	
Description	Network-access control is the set of security controls restricting the access of systems, particularly end-user systems, to parts of the organisational network(s).
Defence in depth	A strong implementation of network-access policy reduces the impacts of a successful compromise by erecting barriers between networks. It can significantly increase the cost of an attack even if a single system is insecure.
Objectives	• Reduce the impact of successful compromise of point systems • Prevent unauthorised access to segments of a network

Implementation	• Segregate networks and components
	  o Create management networks for administrative functions
	  o Separate departmental networks
	  o Separate highly business-critical systems
	  o Create demilitarised zones for externally facing systems
	• Restrict physical access to network media to secured physical locations
	  o Restrict access to network ports
	  o Restrict visability of wireless networks
	• Implement segregation at all levels of the network stack
	  o At the physical layer, through physical disconnection
	  o At the data link layer, through switches and virtual local area networks
	  o At the network layer, through routers, NACLs, and VPNs
	  o At the transport layer, through firewalls and rules
	• Implement network authentications technologies
	  o Deploy 802.11x-enabled devices
	  o Administer port activation and deactivation functions

References	• Trusted Computing Group—Controlling Network Access and Endpoints https://www.trustedcomputinggroup.org/news/Industry_Data/Controlling_Network_Access_and_Endpoints_Nov2007.pdf

Featured control 12: Network-access control

Technology control: Host-access control	
Description	Host-access control is the implementation of security mechanisms and configurations at the system level to limit access to the host itself, or part thereof.
Defence in depth	Host-access control offers the opportunity to implement commodity software and configurations to apply across the 'protect, detect, react' paradigm. Furthermore, controls can be applied in layers to significantly decrease the chance a single mechanism failure will result in information compromise.
Objectives	• Prevent unauthorised access to systems and hosted applications • Detect and reduce the consequence of unauthorised access to systems

Implementation	• Configure the operating system to restrict user access
	   o Execute processes with least privilege
	   o Restrict file system access to only that required
	   o Log attempts to circumvent restrictions
	• Implement network access restrictions
	   o Implement a local firewall and IP address filtering
	   o Restrict outgoing application network access
	• Incorporate hosts into enterprise authentication infrastructure

References	• Microsoft—Windows Security Hardening Guide www.microsoft.com/downloads/details.aspx?FamilyID=15e83186-a2c8-4c8f-a9d0-a0201f639a56

Featured control 13: Host-access control

Technology control: Application-access control	
Description	Application-access control is the security measure implemented at the point (application) where users are presented with information.
Defence in depth	Applications offer an excellent opportunity to implement defence in depth measures for user-access management as they are often custom-built or extensively customisable. Controls can be holistic, integrated or detached and fine-grained.
Objectives	- Prevent unauthorised access to information resources based upon specific business rules and in specific contexts - Limit the impact of unauthorised access - Monitor and detect unauthorised access
Implementation	- Implement strong authentication - Use multiple factors - Validate authentication at each function or component - Implement strong access-control mechanisms - Deny access by default - Assign minimum access to all components - Implement access control in all application tiers - Implement logging and monitoring - Log all authentication attempts - Log failed access requests - Implement 'honey pot' functions and values to detect unauthorised access attempts.
Reference	- US Department of Homeland Security—Least Privilege https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/351.html - SIFT—The Use of 'Honey Pot' Web Services Methods www.sift.com.au/17/137/sift-note-200505.htm

Featured control 14: Application-access control

Technology control: Data-access control	
Description	Data-access control is the application of control mechanisms to information resources themselves such that the possession of a resource alone is not sufficient to access the information.
Defence in depth	Data-access control forms the first (or last from an attacker's perspective) defensive measure against unauthorised access. It significantly increases the cost of attack by requiring additional actions once access to a raw resource has been obtained.
Objectives	• Prevent unauthorised access to data • Limit the information leakage should an information resource be exposed to unauthorised parties
Implementation	• Place controls on data based on sensitivity and business need • Implement and manage public key infrastructure (PKI) • Apply cryptographic controls to information resources 　o Encrypt resources with identified users' public keys using recognised strong ciphers 　o Encrypt resources with additional organisation public keys to ensure availability in an emergency
References	• NIST—Cryptographic Algorithms and Key Sizes for Personal Identity Verification http://csrc.nist.gov/publications/nistpubs/800-78-1/SP-800-78-1_final2.pdf

Featured control 15: Data-access control

User-access management scenario: Individual document control	
Description	Individual document control refers to controls established on an individual file level to control the distribution of, access to and use of that file, both within the computing environment of the creator, and also after initial distribution.
Objectives of user-access management	At an individual document control level, user-access management seeks to control a user's ability to: • Open/read a document • Modify a document • Disseminate a document (e.g. via email) • Print a document • Save a copy of a document • Otherwise reproduce elements of a document More broadly, document control also seeks to provide improved: • Version management • Availability • Audit trails
Risk analysis	Establishing effective controls on an individual document level can be challenging since elements of the controls must be recognised and enforced by the software present on each system on which that document resides, and must be appropriately managed by staff. Specific risks include: • Employees may be careless in their use and distribution of data. • Software may be untrustworthy and may inadvertently or intentionally fail to enforce intended security controls. • The ramifications of data destruction (such as overwrites) may not be adequately understood, resulting in information loss. • Without effective controls over specific key pieces of information within an organisation, that information could be stolen, modified or deleted causing significant impact to the organisation's operations.

Implementation	Document control solutions are generally not used for high-volume transient documents. Document control is more often applied to high-value documentation that will generally have a formalised classification, approval and release process. Such documents will also generally have a degree of sensitivity mandating control over their use. Controls common to individual document management include:
	    o Governance. Implement an information classification policy and associated information handling requirements based on the policy requirements.
	• People
	    o Ensure users are trained in appropriate document handling processes and classification policies.
	• Process

	- o Complete regular reviews/audits of high-sensitivity document repositories to review all access. - o Segregate high-sensitivity documents from lower-sensitivity documents to remove the chance of inadvertent access or attempted access. - Technology - o Enforce data classification in high-sensitivity environments through technical controls. - o Implement software to control user rights to document access/modification and enforce handling controls. - o Implement document encryption solutions to make documents readable to only authorised users, both in transit and in storage. - o Encrypt resources with additional organisation public keys to ensure availability in an emergency.
Further information	- Proquis, What is Document Control?, accessed 2008, www.proquis.com/page.asp?page=8 - Sevinc P, Document Security, October 2005, www.ercim.org/publication/Ercim_News/enw63/sevinc.html - Proquis, What is Document Control?, accessed 2008, www.proquis.com/page.asp?page=8

User-access management scenario 3: Individual document control

Technology control: Credential management	
Description	Credential management is the maintenance of credentials with which users can authenticate access to a system. This may include passwords, physical tokens and biometrics.
Defence in depth	Credential management helps to reduce an organisation's attack surface area, by making it difficult to impersonate a user and gain access to restricted systems. It also helps mitigate the threat of attackers using previously compromised credentials, by limiting the period for which those credentials are valid.
Objectives	• Prevent unauthorised access to information systems through impersonation attacks • Enforce accountability (non-repudiation)

Implementation	• Enforce password policy through application functions
	  o Require users to change passwords regularly
	  o Require passwords to meet complexity standards
	  o Prevent password reuse
	  o Store passwords as cryptographic hashes
	• Employ authentication management infrastructure
	  o Implement key revocation functions
	  o Implement strong key generation and cycling functions
	  o Implement password modification functions
	  o Implement token resynchronisation functions and desynchronisation detection
	• Enforce standards for the user storage and handling of credentials
	  o Prevent clear-text transmission and storage of passwords
	  o Ensure secure handling and storage of tokens

Reference	• Microsoft Secure Password Guidelines www.microsoft.com/smallbusiness/support/articles/select_sec_passwords.mspx

Featured control 16: Credential management

Technology control: Logging and detection	
Description	Logging and detection enables early knowledge and recording of attempted illegitimate access and preserves evidence if required for future investigations.
Defence in depth	Logging and detection is the basis of user-access security response mechanisms and stretches across all technologies within an organisation. Logging user access at all levels ensures that one bypass or corruption of logs doesn't result in a complete loss of audit trail.
Objectives	• Detect unauthorised access to resources • Make users accountable for actions taken

Implementation	• Deploy centralised logging facilities for storing and monitoring:
	   o Router logs
	   o Firewall logs
	   o Server-access logs
	   o File-access logs
	   o Application-access logs
	   o Authentication-server logs
	• Configure technology to enforce regular review of logs to detect anomalies
	• Deploy correlation tools to track user access holistically
	• Employ intrusion detection systems

Reference	• NIST Special Publication 800-92: Guide to Computer Security Log Management http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

Featured control 17: Logging and detection

Technology control: Physical-access control	
Description	Physical-access control is the security mechanisms managing access to an organisation's physical resources and facilities.
Defence in depth	The reduction of availability of physical access to systems and documents significantly reduces the number of possible attacks and also increases the difficulty of performing many others. Physical security is also central to defence in depth, in that a physical compromise of a system or information is often the most severe and can nullify all electronic controls.
Objectives	• To prevent unauthorised physical access to facilities and technology infrastructure • To detect and track unauthorised physical access • To prevent outages and other availability issues

Implementation	• Deploy surveillance cameras to monitor access to facilities
	• Implement alarms to detect unauthorised access
	• Apply locks at all levels of facilities:
	   o System cases
	   o Server racks
	   o Server and communications rooms
	   o Building—internal access doors and elevators
	   o Building—external access doors
	   o Fences and external perimeter access
	• Implement sign-in and sign-out forms
	• Remove and disable all unnecessary access points to network media, including wireless

Reference	• *ZDNet Australia*—'10 Critical Physical Security Measures' www.zdnet.com.au/insight/hardware/soa/10-critical-physical-security-measures/0,139023759,339280172,00.htm

Featured control 18: Physical-access control

MONITOR AND REVIEW

The information security principles from the Secure *Your Information: Secure Your Business* paper relevant to this section are:

Principles of Information Security

1. Information Security is Integral to Enterprise Strategy

2. Information Security Impacts on the Entire Organisation

3. Enterprise Risk Management Defines Information Security Requirements

4. Information Security Accountabilities Should be Defined and Acknowledged

5. Information Security Must Consider Internal and External Stakeholders

6. Information Security Requires Understanding and Commitment

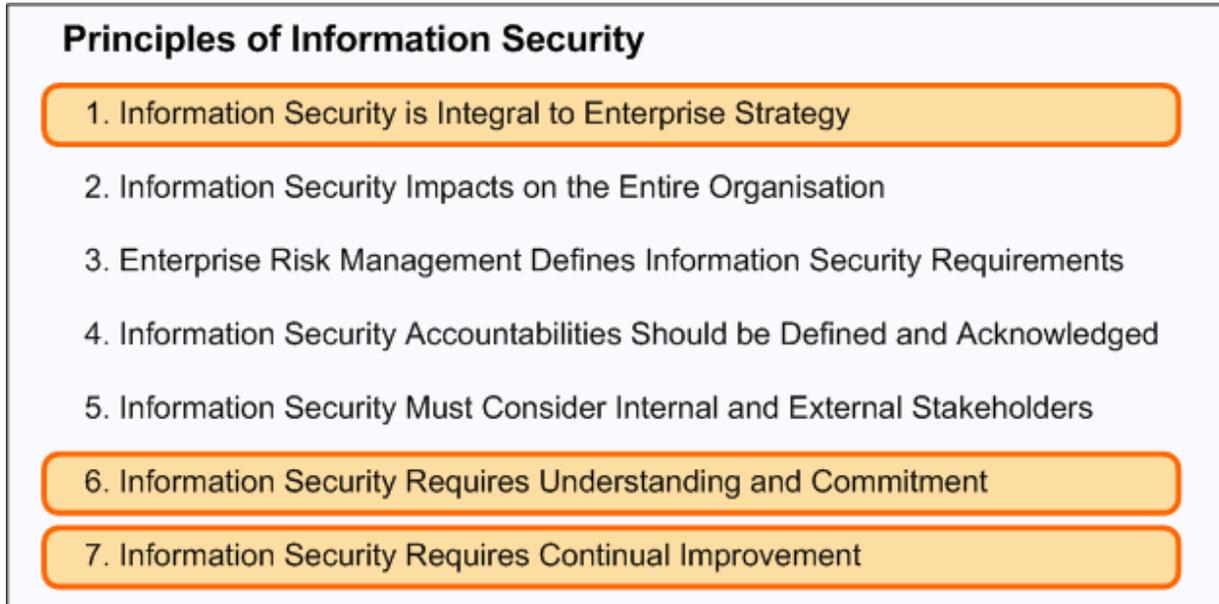7. Information Security Requires Continual Improvement

Figure 9: Applicable principles of information security for monitor and review

As with all areas of information security, the requirements for and threats to access control are continually evolving and new threats are emerging. As described in the full *Defence in depth* report, processes must be established for the identification of changes and development of appropriate responses to scenarios including:

- Security breaches.

- Weaknesses in existing controls.

- Changes in mission/business objectives.

- Changes in the security profile.

With respect to user-access management, this section will look specifically at the emerging technologies and trends influencing risk in this space.

Trends and emerging threats

Industry trends and emerging threats as at the date of this report, and requiring consideration for user-access management strategy being presently established include:

- Migration to browser-based web applications.

- Migration to cross-platform web services.

- Use of genuine credentials with malicious intent.

- Growing use of single sign-on technologies.

- Federated identity and trust broker relationships.

Migration to browser-based web applications

The past decade has seen a marked shift in the delivery of applications to end-users both publicly and internally within organisations. The web browser has become the platform of choice for practically all forms of client software due to its ubiquity[38], and most modern applications are developed for browser-based access.

This migration has also affected organisations as web interfaces for internal business-critical applications are being increasingly implemented. This poses a greater challenge for user-access management as new paradigms for authentication and access control need to be understood and implemented. A range of mechanisms have been developed to provide for identity and access management within web applications. These include:

- **Cookies**—elements of text provided by a web server to a user's web browser to be used over time (either during a short-term session or over a longer period) for authentication, tracking, and storing user preference information.

- **Session IDs**—elements of data used to identify a 'conversation' i.e. a series of exchanged messages.

Another challenge to user-access management within web applications is the presence of new classes of security vulnerabilities that may allow user-access controls to be subverted. Web application vulnerabilities such as cross-site scripting and SQL injection[39] potentially leave data and application functionality at risk of unauthorised access or tampering.

Migration to cross-platform web services

The growing adoption of web services for both internal middleware and for interfacing with external systems presents a significant challenge for user-access management. A typical deployment scenario for web services is to implement a middleware layer for integrating legacy systems internally, and to expose application functionality to external parties via 'software as a service' architecture. As these systems are often business-critical, the robustness of user-access controls around these web services is particularly important.

Specific considerations may include the authentication and access controls in place for both human and mechanical users of exposed web services. These controls may be implemented in a cross-platform manner by adhering to published security standards such as WS-Security and security assertion markup language (SAML), which offer a syntax for implementing controls such as encryption, digital signatures and authorisation tokens.

Another access management aspect of web services that should be considered is that they can potentially weaken network-level access controls. As web services commonly operate over

---

[38] Taivalsaari et al, *Web Browser as an Application Platform: The Lively Kernel Experience,* January 2008, http://research.sun.com/techrep/2008/smli_tr-2008-175.pdf

[39] OWASP, *Top 10 2007*, 2007, www.owasp.org/index.php/Top_10_2007

HTTPS, their communications are not restricted by corporate firewalls, and SSL/TLS encryption typically renders traffic inspection unfeasible. Thus, web services can be considered a potential mechanism for allowing system interactions to bypass network security controls in place.

Use of genuine credentials with malicious intent

The use of genuine user credentials for malicious purposes has been increasing in recent years. Such credentials are often obtained via an attack known as 'spear phishing', which is any form of highly targeted phishing attack[40]. Such attacks are aimed at targets ranging from a specific organisation down to an individual, seeking information or access credentials. As the attacks are highly targeted, more time and effort goes into making them appear legitimate, with the end result that detecting such attacks can be very difficult.

Spear phishing emails are designed to get recipient users to follow links in the message or open malicious attachments. These will then seek to either install malicious code on the user's computer or otherwise obtain personal information, such as usernames and passwords.

Having obtained valid user credentials, the attackers may then be able to access the organisation's systems or data as if they were a valid user. This may mean logging into the system during appropriate business hours and generally using the access in a non-suspicious way so as not to draw attention.

This type of attack introduces significant challenges to organisations from a detection point of view, as it now becomes necessary for organisations to be able to distinguish between authorised and unauthorised instances of a user account logging in and accessing data.

Growing use of single sign-on technologies

The growing adoption of single sign-on technologies presents a significant user-access management risk due to the convergence of identities and credentials. Within a single sign-on environment, each user has only one set of credentials that grants access to all the systems for which they are authorised. Thus, an attacker needs only to compromise one set of credentials to assume a user's identity across multiple information systems.

In addition to the greater risk posed by credential compromise, the management processes around single sign-on implementations may also face additional challenges compared with processes for managing individual systems. User single sign-on profiles will need to be carefully aligned with access requirements—the implications of incorrectly assigned privileges are likely to be greater in a single sign-on system.

Federation of identity and trust broker relationships

Identity federation involves the assembly of identity information from multiple sources within different administrative domains and the use of this information across different information systems and organisations. The trust broker relationships that are required to support the

---

[40] Microsoft, *Spear Phishing: Highly targeted scams*, September 2006, www.microsoft.com/protect/yourself/phishing/spear.mspx

federation of identity present a unique risk to user-access management. The reliance on a third-party system to broker the sharing of identity information across administrative boundaries[41] means an organisation must have a high degree of trust for the trust broker. Given that the trust broker performs authentication and authorisation checks on behalf of the organisation, it dictates the access rights of information system users that are authenticated through the broker.

Any failure of security controls within the trust broker can directly result in unauthorised access to data or resources as forged identity information from a compromised broker system will be processed and accepted by the organisation's information systems. Furthermore, as identity information is managed by a third party, an organisation involved in identity federation will need to address communication and accountability issues that may hinder or subvert the accuracy of information stored by the broker and used to determine access levels[42]. Failure to ensure the accuracy of identity information in a trust broker may lead to unauthorised access across a range of systems that are participating in identity federation.

---

[41] Scarlet S, *The Truth About Federated Identity Management*, October 2006, www.csoonline.com/article/print/221034
[42] Baldwin, Mont, Beres, Shiu, *On Identity Assurance in the Presence of Federated Identity Management Systems*, January 2008, www.hpl.hp.com/techreports/2007/HPL-2007-47R1.pdf

APPENDICES

Appendix A: Glossary

Access Control List (ACL)
A mechanism for limiting access to a system resource to identities that have had such access authorised.

ACSI 33
The Australian Government Information and Communications Technology Security Manual, developed by the Defence Signals Directorate to provide policies and guidance to Australian Government agencies on how to protect their ICT systems.

Authentication
The two-step process of verifying an identity claimed by or for an entity. First an identifier is presented, then verification information is presented to corroborate the identity.

Authorisation
The process of granting (or denying) access to a system resource.

Certificate Authority
An entity that issues digital certificates to other parties for the purposes of cryptography. A root *certificate authority* issues digital certificates to lower-level *certification authorities* for the purposes of identification and signing and is the foundation of the certificate chain of trust.

Chinese walls
Information barriers put in place within an organisation to prevent issues arising from conflicts of interest.

Common criteria
Common criteria is an international standard (ISO 15408) which provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standardised manner.

Credentials
Information that is used to prove the identity of one user or system to another.

Discretionary-access control
An access-control model which restricts access to objects based on the identity of subjects and/or groups to which they belong. The access rights are usually created and assigned to users by the owner of the object or asset.

Defence in depth
The coordinated use of multiple security countermeasures to protect an organisation's information assets.

Digital certificate
An electronic assertion of identity backed by a digital signature from a certificate authority.

Digital signature
A form of cryptography used to provide authentication and integrity for an electronic message.

ISO 27002
A set of established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organisation

Intrusion Detection System (IDS)
A system which detects anomalies in network behaviour for the purpose of identifying attacks

Mandatory access control
An access control model which requires security clearance labels to be set for both users and objects/assets. Systems enforce the access rights of users by checking whether a user's clearance label is greater than or equal to the data they are trying to access.

Phishing
A social engineering attack impersonating a trusted party in an electronic communication in an attempt to trick users into navigating to a spoofed version of a site controlled by the attacker and entering authentication credentials.

Privileges
The rights or permissions afforded to an entity to access information.

Provisioning
The initial setup or configuration process of assigning user privileges and authentication tokens and activating their identity for use within a system.

Public Key Infrastructure (PKI)
An infrastructure where users are issued proof of identity by certificate authorities for authentication and other cryptographic purposes.

Risk
A *risk* is an expectation of loss expressed as the probability that a particular *threat* will exploit a particular *vulnerability* with a particular harmful result.

Role-Based-Access Control (RBAC)
RBAC assigns 'roles' to users to define access rights. Roles are collections of allowable permissions and privileges that usually match a specific job or occupation. Users are assigned roles commensurate with their occupation and job requirements. The user then inherits the access rights of any roles they have been assigned.

Social engineering
A euphemism for non-technical or low-technology means—such as lies, impersonation, tricks, bribes, and blackmail—used to attack information systems.

Threat
Any potential circumstance, capability, action or event which could breach security or cause harm to an asset.

Trojan
A piece of software that masquerades as a legitimate program but executes a hidden payload typically used to install malware.

Vulnerability
A flaw or weakness in an information system's design, implementation or operation and management that could be exploited to violate the system's security policy.

REFERENCES

1.   NIST, Special Publication 800-12, http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter17.html

2.   Deloitte, *2007 Global Security Survey* www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf

3.   TISN, defence in depth, April 2008, [URL]

4.   NSA, Defense in Depth, www.nsa.gov/snac/support/defenseindepth.pdf

5.   United States Department of Defense, DoD Standard 5200.28-STD, www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

6.   OWASP, Mandatory Access Control, www.cgisecurity.com/owasp/html/ch08s02.html

7.   Harris S, CISSP Exam Guide, McGraw-Hill/Osborne

8.   Information Security Systems Organization, *Labeled Security Protection Profile Version 1.b*, www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/protection-profiles/lspp.pdf, 1999

9.   OpenSolaris, *OpenSolaris Project: Flexible Mandatory Access Control,* http://opensolaris.org/os/project/fmac/

10.   Harris S, *CISSP Exam Guide,* McGraw-Hill/Osborne

11.   Straub KR, *Information Security: Managing risk with defence in depth*, August 2003, www.sans.org/reading_room/whitepapers/infosec/1224.php

12.   Shirey, R, RFC 2828—Internet Security Glossary, May 2000, www.faqs.org/rfcs/rfc2828.html

13.   NIST, Generally Accepted Principles and Practices for Securing IT Systems, September 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

14.   Gonzales-Webb S, Implementing Role Based Access Control in Healthcare, May 2007, www.va.gov/rbac/docs/EHT_20070502_SW20_11_TEPR-RBAC_Presentation.ppt

15.   NIST, An Introduction to Role-based Access Control, December 2005, http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm

16.   G. Neumann and M. Strembeck. *A Scenario-driven Role Engineering Process for Functional RBAC Role*s, 2002, 7th ACM Symposium on Access Control Models and Technologies, wwwi.wu-wien.ac.at/home/mark/publications/sacmat02.pdf

17.   Tan, A, People: 'Your network's weakest link', 11 Oct 2005, *ZDNet Asia*, http://news.zdnet.co.uk/internet/security/0,39020375,39228254,00.htm

18.   PricewaterhouseCoopers, *The Global State of Information Security 2007*, 2007, www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B/$FILE/PwC_GISS2007.pdf

19. Busch C, Daum H, *Evaluation of Biometrics*, 2004, Fraunhofer Institute, www.inigraphics.net/press/topics/2004/issue1/1_04a08.pdf

20. Goodin D, 'Get your German interior minister's fingerprint here', 30 March 2008, *The Register*, www.theregister.co.uk/2008/03/30/german_interior_minister_fingerprint_appropriated

21. National Center for State Courts, Biometrics Comparison Chart, 2002, http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html

22. Mitnick KD & Simon LS, *The Art of Deception: Controlling the Human Element of Security*, 2002, John Wiley and Sons

23. Karakasilitis A, Furnell SM & Papadaki M, *Assessing End-User Awareness of Social Engineering and Phishing*, 2006, http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Karakasilioti s%20Furnell%20Papadaki%20-%20Assessing%20end-user%20awareness%20of%20social%20engineering%20and%20phishing.pdf

24. Zeltser L, How to Integrate Social Engineering into an Information Security Assessment, 2008, www.zeltser.com/social-engineering/

25. Barnum S & Gegick M, *Least Privilege*, , September 2005, https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/351.html

26. NIST, *Information Security Handbook: A Guide for Managers sp800-100*, 2006, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

27. Ferraiolo D & Kuhn R, *Role-Based Access Controls*, 1992, http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html

28. Purcell JE, *Employee Management Security Controls*, March 2007, http://www.giac.org/resources/whitepaper/application/247.php

29. Fernandez R, Enterprise Dynamic Access Control Version 2 Overview, January 2006, United States Navy

30. Szabo N, *Patterns of Integrity—Separation of Duties*, 2004, http://szabo.best.vwh.net/separationofduties.html

31. Swanson M & Guttman B, *NIST - Generally Accepted Principles and Practices for Security Information Technology Systems*, September 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

32. Coe K, 'Closing the Security Gap', August 2003, *HR Magazine*, www.shrm.org/hrmagazine/articles/0803/0803coe.asp

33. Mendham T, 'A Secure Culture', February/March 2006, *CIO Enterprise Focus: Security*

34. Wilson M & Hash J, NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program, October 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

35. CERT Publication, Personnel Security Guidelines, September 2004, http://www.us-cert.gov/control_systems/pdf/personnel_guide0904.pdf

36.   Common Criteria, *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components*, *Version 3.1 Revision 2*, http://www.niap-ccevs.org/cc-scheme/cc_docs/CCPART2V3.1R2.pdf, September 2007

37.   Taivalsaari et al, *Web Browser as an Application Platform: The Lively Kernel Experience*, January 2008, http://research.sun.com/techrep/2008/smli_tr-2008-175.pdf

38.   OWASP, Top 10 2007, 2007, www.owasp.org/index.php/Top_10_2007

39.   Microsoft, Spear Phishing: Highly targeted scams, September 2006, www.microsoft.com/protect/yourself/phishing/spear.mspx

40.   Scarlet S, *The Truth About Federated Identity Management*, October 2006, www.csoonline.com/article/print/221034

41.   Baldwin, Mont, Beres, Shiu, *On Identity Assurance in the Presence of Federated Identity Management Systems*, January 2008, http://www.hpl.hp.com/techreports/2007/HPL-2007-47R1.pdf