



---

---

## **SAS 70 - Type I Review**

---

---

**May 23, 2006**

**Version 3.0**

---

**This document is the property of Pinnacle Group Worldwide, Inc. and is intended for use by Pinnacle Group Worldwide personnel only. Distribution, reproduction, or modification of this document without the express written consent of Pinnacle Group Worldwide, Inc. is strictly prohibited. © 2006 Pinnacle Group Worldwide, Inc.**

---



May 23, 2006

An open letter to our customers:

Pinnacle Group Worldwide, Inc.'s commitment to provide secure and reliable services to you, our customers, is our number one priority. By continually improving our infrastructure, tools, and internal procedures, we believe that we are doing everything possible to meet and exceed your expectations.

In order to receive an outside perspective on the validity of the policies and procedures that we use to maintain our systems, we have commissioned a Certified Public Accounting firm to perform an independent review of the operations at Pinnacle Group Worldwide, Inc. The format and content of the review performed was in accordance with the guidelines set by the American Institute of Certified Public Accountants (AICPA) in their Statement of Auditing Standards Number 70: *Reports on the Processing of Transactions by Service Organizations* (SAS 70).

To perform the review, we engaged the Certified Public Accounting firm of Schramm & Company, P.C. The review was conducted April 19<sup>th</sup> – 21<sup>st</sup>, 2006.

Thank you for your support and the trust you have chosen to use Pinnacle Group Worldwide, Inc. We are confident that you will find value in this validation process and other investments we are making in our ability to serve you, as we remain committed to our mutual success.

## Table of Contents

<b>Section 1</b> .....	<b>5</b>
Independent Service Auditor's Report.....	5
Objectives and Scope of the Review.....	8
Approach Utilized .....	9
<b>Section 2</b> .....	<b>10</b>
Pinnacle Group Worldwide, Inc. Description of Controls.....	10
Description of Controls .....	11
Pinnacle Group Worldwide, Inc. Overview .....	12
<b>Section 3</b> .....	<b>15</b>
Information Provided by the Service Auditor .....	15

**Pinnacle Group Worldwide, Inc.**

## **Section 1**

### ***Independent Service Auditor's Report***

# SCHRAMM & COMPANY P.C.

*Certified Public Accountants & Valuation Consultants*

865 Technology Blvd., Suite B • Bozeman, MT 59718

Phone: (406) 586-4379 • Fax: (406) 587-4891

---

## Independent Service Auditor's Report

To the Pinnacle Group Worldwide, Inc. Executive Management:

We have examined the accompanying description of controls related to Pinnacle Group Worldwide, Inc. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Pinnacle Group Worldwide, Inc. controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied those aspects of internal control contemplated in the design of Pinnacle Group Worldwide, Inc. The control objectives were specified by Pinnacle Group Worldwide, Inc. management. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

Attached is the 2006 Report on Service Organization, which conforms with guidelines set forth in the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards Number (SAS) 70: *Reports on the Processing of Transactions by Service Organizations* and as amended by SAS 78: *Consideration of Internal Controls in a Financial Statement Audit*, SAS 88: *Service Organizations and Reporting on Consistency*, and SAS 98: *Omnibus Statement on Auditing Standards --2002*.

This year's report features a subset of the ISO 17799:2005 controls that are pervasive throughout Pinnacle Group Worldwide, Inc.

The SAS 70 Type I report includes a control narrative, provided by Pinnacle Group Worldwide, Inc. and results of design effectiveness testing of these controls, which are provided by Schramm & Company P.C., an independent auditing firm.

This review was not intended to report on compliance with the Gramm-Leach-Bliley Act (GLBA), the Healthcare Insurance Portability and Accountability Act (HIPAA), and the USA Patriot Act (USAPA).

Our examination was conducted for the purpose of forming an opinion on the description of Pinnacle Group Worldwide, Inc. controls related to system activities and the related general computer controls.

In our opinion, the accompanying description of Pinnacle Group Worldwide, Inc. controls (Section Two) presents fairly, in all material respects, the relevant aspects of Pinnacle Group Worldwide, Inc. controls that had been placed in operation as of April 20<sup>th</sup>, 2006. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied those aspects of internal control contemplated in the design of Pinnacle Group Worldwide, Inc. controls.

The relative effectiveness and significance of specific controls at Pinnacle Group Worldwide, Inc. and their effect on assessments of control risk at user organizations are dependent on their interaction with internal control, and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of internal control at individual user organizations.

The results of design effectiveness testing of controls at Pinnacle Group Worldwide, Inc. are as of April 20<sup>th</sup>, 2006. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specific controls at Pinnacle Group Worldwide, Inc. is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected.

Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by management of Pinnacle Group Worldwide, Inc., its user organizations, and the independent auditors of its user organizations.

A handwritten signature in cursive script that reads "Schramm & Company P.C.".

May 17, 2006

## ***Objectives and Scope of the Review***

The purpose of this report is to communicate to the customers of Pinnacle Group Worldwide, Inc. (Pinnacle) the design effectiveness of general controls in place that affect the support of their services. The review of controls was limited only to those procedures and activities performed by Pinnacle.

Pinnacle Group Worldwide, Inc. internal controls and procedures, as understood by Schramm & Company P.C., were obtained from personal interviews, written documentation, and direct observation. Results of testing were compiled as a result of a combination of examination of evidence generated during the review period, interviews and observation. Due to certain limitations, errors or irregularities may go undetected. In addition, future changes in conditions or personnel may render current procedures useless or outdated.

## ***Approach Utilized***

Our approach to performing the Third Party Review follows the American Institute of Certified Public Accountant's (AICPA) Statement of Auditing Standards Number 70: Reports on the Processing of Transactions by Service Organizations.

The specific control objectives reviewed were selected by Pinnacle Group Worldwide, Inc. management. Pinnacle Group Worldwide, Inc. management feels that the selected control objectives address concerns in the market place for independent assurance of the reliability of computer information systems.

Pinnacle Group Worldwide, Inc. selected a subset of the ISO 17799 controls for this audit. ISO 17799 is a globally recognized security standard that provides a comprehensive set of security best practices controls to guide organizations on effectively protecting the confidentiality, integrity and availability of their critical data. It consists of 11 different sections, each covering a different security area, ranging from risk assessment to security policy compliance to business continuity. The burden for many organizations is finding the resources and internal expertise to apply these standards to their business needs.

The ISO 17779:2005 standard is a collection of controls that are detailed under 11 major headings.

These headings are:

1. Security Policy;
2. Organization of Information Security;
3. Asset Management;
4. Human Resources Security;
5. Physical and Environmental Security;
6. Communications and Operations Management;
7. Access Control;
8. Information Systems Acquisition, Development and Maintenance;
9. Information Security Incident Management;
10. Business Continuity Management;
11. Compliance.

For each control objective reviewed, we have provided an assessment as to whether or not Pinnacle Group Worldwide has achieved the requirements of the control objective. Additionally, we have provided a summary of the relevant Pinnacle Group Worldwide, Inc. policies and procedures that led to the assessment.

The summary of observations was based on the full complement of services provided by Pinnacle Group Worldwide, Inc. within the scope of the previously identified service areas.

**Pinnacle Group Worldwide, Inc.**

## **Section 2**

### ***Pinnacle Group Worldwide, Inc. Description of Controls***

## **Description of Controls**

The following ISO 17799:2005 controls were selected for this audit:

- 5.1.1 Information security policy document
- 5.1.2 Review of the information security policy
- 6.1.3 Allocation of information security responsibilities
- 6.1.5 Confidentiality agreements
- 6.1.8 Independent review of information security
- 6.2.2 Addressing security when dealing with customers
- 6.2.3 Addressing security in third party agreements
- 7.2.1 Classification guidelines
- 8.1.1 Roles and responsibilities
- 8.1.2 Screening
- 8.1.3 Terms and conditions of employment
- 8.2.2 Information security awareness, education, and training
- 8.2.3 Disciplinary process
- 8.3.3 Removal of access rights
- 9.1.1 Physical security perimeter
- 9.1.2 Physical entry controls
- 9.1.4 Protecting against external and environmental threats
- 9.1.5 Working in secure areas
- 9.1.6 Public access, delivery, and loading areas
- 9.2.2 Supporting utilities
- 10.1.1 Documented operating procedures
- 10.1.2 Change management
- 10.1.3 Segregation of duties
- 10.1.4 Separation of development, test, and operational facilities
- 10.3.1 Capacity management
- 10.4.1 Controls against malicious code
- 10.5.1 Information back-up
- 10.7.2 Disposal of media
- 10.8.3 Physical media in transit
- 10.10.1 Audit logging
- 10.10.5 Fault logging
- 11.1.1 Access control policy
- 11.2.1 User registration
- 11.2.3 User password management
- 11.2.4 Review of user access rights
- 11.3.1 Password use
- 11.3.3 Clear desk and clear screen policy
- 11.4.4 Remote diagnostic and configuration port protection
- 11.4.5 Segregation in networks
- 11.5.2 User identification and authentication
- 11.5.3 Password management system
- 11.5.5 Session time-out
- 11.7.1 Mobile computing and communications
- 12.5.1 Change control procedures
- 13.1.1 Reporting information security events
- 13.1.2 Reporting security weaknesses

## Pinnacle Group Worldwide, Inc. Overview

Pinnacle Group Worldwide is a preferred Hyperion reseller and services provider. The company has been working with Hyperion products for over a decade, and focuses on delivering financial consolidation and analytical reporting solutions to Fortune 1000 companies.

Founded in 1995, Pinnacle Group Worldwide is a global consulting firm focusing on business analysis and financial systems solutions. They were proudly selected in 2002 (#338 as Lindin Group) as one of Inc. Magazine's 500 fastest growing companies in the United States.

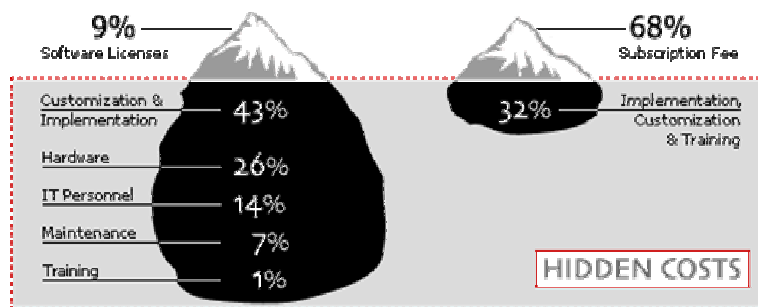
Pinnacle consultants have years of experience in both financial analysis and information systems (IS), and many hold advanced degrees. Their programmers are skilled at rapidly developing custom solutions that integrate, automate, and deliver financial information.

Pinnacle provides a unique opportunity to sell Hyperion Solutions Applications+ more competitively by offering an on-demand solution for prospects and customers. This service provider model gives prospects a low total cost of ownership (TCO) solution for meeting financial consolidation, planning and forecasting, and business analytics needs.

K2Analytics.com is the domain for a web-based hosted solution for Hyperion products such as Hyperion Planning, Hyperion Financial Management, Hyperion Essbase, and even Hyperion Enterprise 6.4. In addition, web-based extraction, transformation and load data (ETL) tools such as Upstream and Hyperion Application Link (HAL) can be hosted.

The hosted solution has been branded separately to allow other partners and Hyperion services to be able to offer this solution to their customers and prospects. Pinnacle branding has been removed completely from the offering so it will be as transparent as implementing within a customer's data center.

### What is the Value Proposition to my customers and prospects?



The savings come in what is known as “the iceberg effect” - the costs that occur after the sale; implementation, hardware, technology staff costs, administration, and training. Pinnacle has bundled these services together in an affordable and easily budgeted monthly fee. When you look at total cost of ownership, these expenses quickly add up, and hosting becomes a very price competitive solution.

The hosted solution really shows off how far ahead of the competition Hyperion's technology is. Hyperion's superior N-tier architecture and AJAX (Asynchronous Java and XML) deployment allows for a very robust and scalable solution. It offers a stark contrast to other solutions in the marketplace that rely on Excel or heavy-client front ends such as Business Objects, Cognos, or Outlooksoft.

The solution can be demonstrated over the web from just about anywhere in the world. In fact, Pinnacle's consultants can provide value add during the pre-sales cycle by creating prototypes, test drives, and proof of concepts for your prospects. Pinnacle has been doing this for customers and prospects since 2004.

The core difference is in the licensing of the software. An MSP is a Managed Service Provider, which houses the customer's licensed software. The customer is free to move the solution in-house or to another hosting provider. A prospect will purchase licenses to Hyperion software as normal, and the sales process and compensation structure is exactly the same. An ASP is an Application Service Provider,

where the software cost is bundled in to that monthly fee. In this model, a customer is not free to move the software and application to wherever they want. *This is not a subscription service like Salesforce.com.*

The K2Analytics Data Center is a state-of-the-art facility located in Towson, MD. The facility has fully redundant systems, contains backup generators, waterless fire suppression systems, and thumbprint security room access. We operate under very strict SAS 70 data center conditions, so you can be assured that the facility and data are safe and secure.

Pinnacle's servers and applications are continuously monitored from an outside source. In 2005, the servers in Pinnacle's data center had an independently documented 99.4% uptime. That *includes* a move from the previous facility in Ellicott City, Maryland to the brand new K2Analytics data center in Towson. Without the move 20 miles north, the uptime would have been very close to 100%.

Backup and offsite archival are provided by Iron Mountain, the premiere name in data archival and storage. Data will be stored in an offsite location for seven years in accordance with Sarbanes-Oxley requirements. Iron Mountain's facilities and offering is also SAS 70 and Sarbanes-Oxley compliant.

Pinnacle has contracted with L3-Communications to provide a hot site located in Denver, Colorado. In case of any catastrophic disaster we can have customers up and running in that facility in a matter of hours. This geographically distinct site is a state-of-the art SAS 70 compliant facility that will keep our customers going should the unthinkable ever happen.

Every customer gets their own domain with primary and backup domain controllers. Security is controlled using Active Directory and the System 9 user provisioning. Each customer gets dedicated top of the line 64-bit HP/Compaq servers with fully redundant power systems, data lines, and disk storage. The segregated N-Tier architecture is ideal for applications that can be accessed globally. Customers will be able to apply upgrades and patches to meet their needs and not impact any other customer's environments.

### **What kinds of services are included in the offering?**

- ✓ Hardware Procurement and Configuration – each customer gets an environment suited to their solution needs.
- ✓ Software Installation / Configuration – all operating systems, firewall, and antivirus software are provided.
- ✓ Application and Data Integration – we configure and securitize all interaction between data and application.
- ✓ System and Service Management – all servers and services are monitored and administered by our staff.
- ✓ Performance Monitoring and Tuning – servers are independently monitored for uptime and tuned for performance.
- ✓ All Server and Database Administration – log archival and database tuning are all performed by our staff.
- ✓ Fully Managed 3-Layer Security – all SAS 70 compliant security is directed by the customer, but managed by staff.
- ✓ 24/7 Live Technical Support – for any issues or requests that arise for global customers.
- ✓ Network-based Intrusion Detection System – to ensure against hacking and even “social engineering.”

### **What kinds of customers would be interested in this offering?**

A hosted solution is NOT for everyone. Many larger companies have their own data centers and do not need this type of service. *(You can still use this service for a quick way to provide demos, prototypes and proof of concepts for these prospects!)* An ideal customer for a hosted solution fits into one or more of the following categories;

- Is outsourcing business services or hosts other software applications
- Does not have internal infrastructure or a data center of their own
- The solution requires a third party for distribution or joint venture purposes
- Concerned about the ongoing cost of maintaining a Hyperion Solution
- Has an unconstructive relationship with their company IT department
- Uses a legacy Hyperion product (Pillar, Enterprise) and needs added TLC
- Needs a quick win or strategic implementation in order to promote a larger sale

Pinnacle Group Worldwide is a Hyperion preferred select reseller and consulting partner. They've been around since 1995 and continuously profitable every quarter. Unlike other partners, Pinnacle Group Worldwide does not sell products that compete with Hyperion, therefore their goal is aligned with their client's: mutually successful sales and implementations of Hyperion software.

Pinnacle consultants have been responsible for hundreds of implementations of Hyperion products, including some breathtaking sale-to-implementation times of Hyperion Enterprise (3 weeks) and Hyperion Financial Management (15 weeks). Quick wins like this deliver some incredible ROI to their customer. Pinnacle has a highly referenced customer base that crosses many verticals including financial services, manufacturing, consumer products, telecommunications, and pharmaceuticals / healthcare.

Pinnacle is a reseller in the small-midsize business (SMB) market, and they experience firsthand the price pressure and feature competitiveness with Hyperion's competitors. Hosting was developed to create an affordable solution and expand the versatility of Hyperion's offerings to fit the needs of the marketplace.

Pinnacle has been a "thought leader" in this space for over two years now, first approaching upper management of Hyperion with the idea in early 2004. Conceptually it was possible, but it wasn't until the new 'tadpole' product look and feel, and the release of Smartview for this to be practical. The foundation services within System 9 have also added to the prudence and robustness of this offering.

Pinnacle has been hosting demos, prototypes, proof of concepts, and product trial runs on a limited basis since 2004, adding tremendous value to the pre-sales process. On some projects, Pinnacle has also used the data center as a development environment while their customers order and install their own hardware, then a transfer of the application to the customer site takes place.

Customers have also asked if Pinnacle can provide alternative services in the K2Analytics Data Center such as acting as a customer's disaster recovery hot-site or the ability to conduct performance and load testing on applications. Pinnacle will gladly help with any of these additional services should a customer request them from Pinnacle's clients!

Pinnacle has made a significant financial investment to bring this opportunity to market. The management of Pinnacle strongly believes that the broader market is moving toward lower cost solutions and this initiative will help Hyperion penetrate opportunities in new customers as well as other business areas such as marketing, human resources, and operations within existing customers.

If for any reason a customer wishes to move out of the hosted environment, they are free to do so. The software, application, and data are all customer owned property for them to do with as they wish. That is one of the benefits of the managed service provider (MSP) model.

## **Section 3**

### ***Information Provided by the Service Auditor***

**5.1.1 Information security policy document  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

**Implementation guidance**

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

- 1) compliance with legislative, regulatory, and contractual requirements;
- 2) security education, training, and awareness requirements;
- 3) business continuity management;
- 4) consequences of information security policy violations;

e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;

f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

**Other information**

The information security policy might be a part of a general policy document. If the information security policy is distributed outside the organization, care should be taken not to disclose sensitive information. Further information can be found in the ISO/IEC 13335-1:2004.

---

**5.1.2 Review of the information security policy  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

## Implementation guidance

The information security policy should have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. The review should include assessing opportunities for improvement of the organization's information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.

The review of the information security policy should take account of the results of management reviews. There should be defined management review procedures, including a schedule or period of the review.

The input to the management review should include information on:

- a) feedback from interested parties;
- b) results of independent reviews (see 6.1.8);
- c) status of preventive and corrective actions (see 6.1.8 and refer to 15.2.1);
- d) results of previous management reviews;
- e) process performance and information security policy compliance;
- f) changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment;
- g) trends related to threats and vulnerabilities;
- h) reported information security incidents (see 13.1);
- i) recommendations provided by relevant authorities (refer to 6.1.6).

The output from the management review should include any decisions and actions related to:

- a) improvement of the organization's approach to managing information security and its processes;
- b) improvement of control objectives and controls;
- c) improvement in the allocation of resources and/or responsibilities.

A record of the management review should be maintained.

Management approval for the revised policy should be obtained.

---

### 6.1.3 Allocation of information security responsibilities

#### Design Effectiveness

#### No Deficiencies Noted

#### Description

All information security responsibilities should be clearly defined.

### **Implementation guidance**

Allocation of information security responsibilities should be done in accordance with the information security policy (refer to clause 4). Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly identified. This responsibility should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes, such as business continuity planning, should be clearly defined.

Individuals with allocated security responsibilities may delegate security tasks to others. Nevertheless they remain responsible and should determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible should be clearly stated; in particular the following should take place:

- a) the assets and security processes associated with each particular system should be identified and clearly defined;
- b) the entity responsible for each asset or security process should be assigned and the details of this responsibility should be documented (refer to 7.1.2);
- c) authorization levels should be clearly defined and documented.

### **Other information**

In many organizations an information security manager will be appointed to take overall responsibility for the development and implementation of security and to support the identification of controls.

However, responsibility for implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

---

#### **6.1.5 Confidentiality agreements Design Effectiveness**

#### **No Deficiencies Noted**

##### **Description**

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.

##### **Implementation guidance**

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. To identify requirements for confidentiality or nondisclosure agreements, the following elements should be considered:

- a) a definition of the information to be protected, e.g. confidential information;
- b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;
- c) required actions when an agreement is terminated;

- d) responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know');
- e) ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;
- f) the permitted use of confidential information, and rights of the signatory to use information;
- g) the right to audit and monitor activities that involve confidential information;
- h) process for notification and reporting of unauthorized disclosure or confidential information breaches;
- i) terms for information to be returned or destroyed at agreement cessation; and
- j) expected actions to be taken in case of a breach of this agreement.

Based on an organization's security requirements, other elements may be needed in a confidentiality or non-disclosure agreement.

Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which it applies (refer to 15.1.1).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

#### **Other Information**

Confidentiality and non-disclosure agreements protect organizational information and inform signatories of their responsibility to protect, use, and disclose information in a responsible and authorized manner.

There may be a need for an organization to use different forms of confidentiality or non-disclose agreements in different circumstances.

### **6.1.8 Independent review of information security**

#### **Design Effectiveness**

#### **No Deficiencies Noted**

#### **Description**

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

#### **Implementation guidance**

The independent review should be initiated by management. Such an independent review is necessary to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

Such a review should be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or a third party organization specializing in such reviews. Individuals carrying out these reviews

should have the appropriate skills and experience.

The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained. If the independent review identifies that the organization's approach and implementation to managing information security is inadequate or not compliant with

the direction for information security stated in the information security policy document (see 5.1.1), management should consider corrective actions.

#### **Other information**

The area, which managers should regularly review (refer to 15.2.1), may also be reviewed independently. Review techniques may include interviews of management, checking records or review of security policy documents. ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing, may also provide helpful guidance for carrying out the independent review, including establishment and implementation of a review program. Section 15.3 specifies controls relevant to the independent review of operational information systems and the use of system audit tools.

---

### **6.2.2 Addressing security when dealing with customers**

#### **Design Effectiveness**

#### **No Deficiencies Noted**

##### **Description**

All identified security requirements should be addressed before giving customers access to the organization's information or assets.

##### **Implementation guidance**

The following terms should be considered to address security prior to giving customers access to any of the organization's assets (depending on the type and extent of access given, not all of them might apply):

a) asset protection, including:

- 1) procedures to protect the organization's assets, including information and software, and management of known vulnerabilities;
- 2) procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred;
- 3) integrity;
- 4) restrictions on copying and disclosing information;

b) description of the product or service to be provided;

c) the different reasons, requirements, and benefits for customer access;

d) access control policy, covering:

- 1) permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
- 2) an authorization process for user access and privileges;
- 3) a statement that all access that is not explicitly authorized is forbidden;
- 4) a process for revoking access rights or interrupting the connection between systems;

e) arrangements for reporting, notification, and investigation of information

inaccuracies, e.g. of personal details, information security incidents and security breaches;

f) a description of each service to be made available;

g) the target level of service and unacceptable levels of service;

h) the right to monitor, and revoke, any activity related to the organization's assets;

i) the respective liabilities of the organization and the customer;

j) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries (refer to 15.1);

k) intellectual property rights (IPRs) and copyright assignment (refer to 15.1.2) and protection of any collaborative work (refer to 6.1.5).

#### **Other information**

The security requirements related to customers accessing organizational assets can vary considerably depending on the information processing facilities and information being accessed. These security requirements can be addressed using customer agreements, which contain all identified risks and security requirements (refer to 6.2.1).

Agreements with external parties may also involve other parties. Agreements granting external party access should include allowance for designation of other eligible parties and conditions for their access and involvement.

---

### **6.2.3 Addressing security in third party agreements**

#### **Design Effectiveness**

#### **No Deficiencies Noted**

#### **Description**

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

#### **Implementation guidance**

The agreement should ensure that there is no misunderstanding between the organization and the third party. Organizations should satisfy themselves as to the indemnity of the third party.

The following terms should be considered for inclusion in the agreement in order to satisfy the identified security requirements (refer to 6.2.1):

a) the information security policy;

b) controls to ensure asset protection, including:

1) procedures to protect organizational assets, including information, software and hardware;

2) any required physical protection controls and mechanisms;

- 3) controls to ensure protection against malicious software (see 10.4.1);
  - 4) procedures to determine whether any compromise of the assets, e.g. loss or modification of information, software and hardware, has occurred;
  - 5) controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the agreement;
  - 6) confidentiality, integrity, availability, and any other relevant property (refer to 2.1.5) of the assets;
  - 7) restrictions on copying and disclosing information, and using confidentiality agreements (see 6.1.5);
- c) user and administrator training in methods, procedures, and security;
  - d) ensuring user awareness for information security responsibilities and issues;
  - e) provision for the transfer of personnel, where appropriate;
  - f) responsibilities regarding hardware and software installation and maintenance;
  - g) a clear reporting structure and agreed reporting formats;
  - h) a clear and specified process of change management;
  - i) access control policy, covering:
    - 1) the different reasons, requirements, and benefits that make the access by the third party necessary;
    - 2) permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
    - 3) an authorization process for user access and privileges;
    - 4) a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use;
    - 5) a statement that all access that is not explicitly authorized is forbidden;
    - 6) a process for revoking access rights or interrupting the connection between systems;
  - j) arrangements for reporting, notification, and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement;
  - k) a description of the product or service to be provided, and a description of the information to be made available along with its security classification (see 7.2.1);
  - l) the target level of service and unacceptable levels of service;
  - m) the definition of verifiable performance criteria, their monitoring and reporting;
  - n) the right to monitor, and revoke, any activity related to the organization's assets;
  - o) the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;
  - p) the establishment of an escalation process for problem resolution;
  - q) service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities;
  - r) the respective liabilities of the parties to the agreement;

s) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries (refer to 15.1);

t) intellectual property rights (IPRs) and copyright assignment (refer to 15.1.2) and protection of any collaborative work (see also 6.1.5);

u) involvement of the third party with subcontractors, and the security controls these subcontractors need to implement;

v) conditions for renegotiation/termination of agreements:

1) a contingency plan should be in place in case either party wishes to terminate the relation before the end of the agreements;

2) renegotiation of agreements if the security requirements of the organization change;

3) current documentation of asset lists, licenses, agreements or rights relating to them.

### **Other information**

The agreements can vary considerably for different organizations and among the different types of third parties. Therefore, care should be taken to include all identified risks and security requirements (refer to 6.2.1) in the agreements. Where necessary, the required controls and procedures can be expanded in a security management plan.

If information security management is outsourced, the agreements should address how the third party will guarantee that adequate security, as defined by the risk assessment, will be maintained, and how security will be adapted to identify and deal with changes to risks.

Some of the differences between outsourcing and the other forms of third party service provision include the question of liability, planning the transition period and potential disruption of operations during this period, contingency planning arrangements and due diligence reviews, and collection and management of information on security incidents. Therefore, it is important that the organization plans and manages the transition to an outsourced arrangement and has suitable processes in place to manage changes and the renegotiation/termination of agreements.

The procedures for continuing processing in the event that the third party becomes unable to supply its services need to be considered in the agreement to avoid any delay in arranging replacement services.

Agreements with third parties may also involve other parties. Agreements granting third party access should include allowance for designation of other eligible parties and conditions for their access and involvement.

Generally agreements are primarily developed by the organization. There may be occasions in some circumstances where an agreement may be developed and imposed upon an organization by a third party. The organization needs to ensure that its own security is not unnecessarily impacted by third party requirements stipulated in imposed agreements.

**7.2.1 Classification guidelines**  
**Design Effectiveness**

**No Deficiencies Noted**

**Description**

Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.

**Implementation guidance**

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information and the business impacts associated with such needs.

Classification guidelines should include conventions for initial classification and reclassification over time; in accordance with some predetermined access control policy (see 11.1.1).

It should be the responsibility of the asset owner (refer to 7.1.2) to define the classification of an asset, periodically review it, and ensure it is kept up to date and at the appropriate level. The classification should take account of the aggregation effect mentioned in 10.7.2.

Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic to use or prove impractical. Care should be taken in interpreting classification labels on documents from other organizations, which may have different definitions for the same or similarly named labels.

**Other Information**

The level of protection can be assessed by analyzing confidentiality, integrity and availability and any other requirements for the information considered.

Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense.

Considering documents with similar security requirements together when assigning classification levels might help to simplify the classification task.

In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected.

---

**8.1.1 Roles and responsibilities**  
**Design Effectiveness**

**No Deficiencies Noted**

**Description**

Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.

**Implementation guidance**

Security roles and responsibilities should include the requirement to:

a) implement and act in accordance with the organization's information security policies (see 5.1);

- b) protect assets from unauthorized access, disclosure, modification, destruction or interference;
- c) execute particular security processes or activities;
- d) ensure responsibility is assigned to the individual for actions taken;
- e) report security events or potential events or other security risks to the organization.

Security roles and responsibilities should be defined and clearly communicated to job candidates during the pre-employment process.

**Other Information**

Job descriptions can be used to document security roles and responsibilities. Security roles and responsibilities for individuals not engaged via the organization's employment process, e.g. engaged via a third party organization, should also be clearly defined and communicated.

**8.1.2 Screening  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Explanation: The word 'employment' is meant here to cover all of the following different situations:  
 employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.

**Implementation guidance**

Verification checks should take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following:

- a) availability of satisfactory character references, e.g. one business and one personal;
- b) a check (for completeness and accuracy) of the applicant's curriculum vitae;
- c) confirmation of claimed academic and professional qualifications;
- d) independent identity check (passport or similar document);
- e) more detailed checks, such as credit checks or checks of criminal records.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, e.g. financial information or highly confidential information, the organization should also consider further, more detailed checks.

Procedures should define criteria and limitations for verification checks, e.g. who is eligible to screen people, and how, when and why verification checks are carried out. A screening process should also be carried out for contractors, and third party users. Where contractors are provided through an agency the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third party (see also 6.2.3) should clearly specify all responsibilities and notification procedures for screening.

Information on all candidates being considered for positions within the organization should be collected and handled in accordance with any appropriate legislation

existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

---

**8.1.3 Terms and conditions of employment**  
**Design Effectiveness**

**No Deficiencies Noted**

**Description**

As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.

**Implementation guidance**

The terms and conditions of employment should reflect the organization's security policy in addition to clarifying and stating:

- a) that all employees, contractors and third party users who are given access to sensitive information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities;
- b) the employee's, contractor's and any other user's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation (refer to 15.1.1 and 15.1.2);
- c) responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third party user (refer to 7.2.1 and 10.7.3);
- d) responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties;
- e) responsibilities of the organization for the handling of personal information, including personal information created as a result of, or in the course of, employment with the organization (refer to 15.1.4);
- f) responsibilities that are extended outside the organization's premises and outside normal working hours, e.g. in the case of home-working (refer to 9.2.5 and 11.7.1);
- g) actions to be taken if the employee, contractor or third party user disregards the organization's security requirements (see also 8.2.3).

The organization should ensure that employees, contractors and third party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see also 8.3).

**Other Information**

A code of conduct may be used to cover the employee's, contractor's or third party user's responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. The contractor or third party users may be associated with an external organization that may in turn be required to enter in contractual arrangements on behalf of the contracted individual.

---

**8.2.2 Information security awareness, education, and training**

**Design Effectiveness**

**No Deficiencies Noted**

**Description**

All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

**Implementation guidance**

Awareness training should commence with a formal induction process designed to introduce the organization's security policies and expectations before access to information or services is granted.

Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities, e.g. log-on procedure, use of software packages and information on the disciplinary process (see 8.2.3).

**Other Information**

The security awareness, education, and training activities should be suitable and relevant to the person's role, responsibilities and skills, and should include information on known threats, who to contact for further security advice and the proper channels for reporting information security incidents (see also 13.1).

Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role.

---

**8.2.3 Disciplinary process**

**Design Effectiveness**

**No Deficiencies Noted**

**Description**

There should be a formal disciplinary process for employees who have committed a security breach.

**Implementation guidance**

The disciplinary process should not be commenced without prior verification that a security breach has occurred (refer to 13.2.3 for collection of evidence).

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of security. The formal

disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offense, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

#### **Other Information**

The disciplinary process should also be used as a deterrent to prevent employees, contractors and third party users in violating organizational security policies and procedures, and any other security breaches.

### **8.3.3 Removal of access rights Design Effectiveness**

#### **No Deficiencies Noted**

#### **Description**

The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

#### **Implementation guidance**

Upon termination, the access rights of an individual to assets associated with information systems and services should be reconsidered. This will determine whether it is necessary to remove access rights. Changes of an employment should be reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adapted include physical and logical access, keys, identification cards, information processing facilities (see also 11.2.4), subscriptions, and removal from any documentation that identifies them as a current member of the organization. If a departing employee, contractor or third party user has known passwords for accounts remaining active, these should be changed upon termination or change of employment, contract or agreement.

Access rights for information assets and information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

- a) whether the termination or change is initiated by the employee, contractor or third party user, or by management and the reason of termination;
- b) the current responsibilities of the employee, contractor or any other user;
- c) the value of the assets currently accessible.

#### **Other Information**

In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee, contractor or third party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees, contractors and third party users involved to no longer share this information with the person departing.

In cases of management-initiated termination, disgruntled employees, contractors or third party users may deliberately corrupt information or sabotage information

processing facilities. In cases of persons resigning, they may be tempted to collect information for future use.

**9.1.1 Physical security perimeter  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

**Implementation guidance**

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) security perimeters should be clearly defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

b) perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks, etc; doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;

c) a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only;

d) physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;

e) all fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards; they should operate in accordance with local fire code in a failsafe manner;

f) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;

g) information processing facilities managed by the organization should be physically separated from those managed by third parties.

**Other information**

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection, where the failure of a single barrier does not mean that security is immediately compromised.

A secure area may be a lockable office, or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical

access may be needed between areas with different security requirements inside the security perimeter.

Special consideration towards physical access security should be given to buildings where multiple organizations are housed.

---

### 9.1.2 Physical entry controls

#### Design Effectiveness

**No Deficiencies Noted**

#### Description

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

#### Implementation guidance

The following guidelines should be considered:

a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures;

b) access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only; authentication controls, e.g. access control card plus PIN, should be used to authorize and validate all access; an audit trail of all access should be securely maintained;

c) all employees, contractors and third party users and all visitors should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

d) third party support service personnel should be granted restricted access to secure areas or sensitive information processing facilities only when required; this access should be authorized and monitored;

e) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary (see 8.3.3).

---

### 9.1.4 Protecting against external and environmental threats

#### Design Effectiveness

**No Deficiencies Noted**

#### Description

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

#### Implementation guidance

Consideration should be given to any security threats presented by neighboring premises, e.g. a fire in a neighboring building, water leaking from the roof or in floors below ground level or an explosion in the street.

The following guidelines should be considered to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:

a) hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area;

b) fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster affecting the main site;

c) appropriate fire fighting equipment should be provided and suitably placed.

---

#### 9.1.5 Working in secure areas

##### Design Effectiveness

##### No Deficiencies Noted

##### Description

Physical protection and guidelines for working in secure areas should be designed and applied.

##### Implementation guidance

The following guidelines should be considered:

a) personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis;

b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;

c) vacant secure areas should be physically locked and periodically checked;

d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized.

The arrangements for working in secure areas include controls for the employees, contractors and third party users working in the secure area, as well as other third party activities taking place there.

---

#### 9.1.6 Public access, delivery, and loading areas

##### Design Effectiveness

##### No Deficiencies Noted

##### Description

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

##### Implementation guidance

The following guidelines should be considered:

a) access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel;

b) the delivery and loading area should be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;

c) the external doors of a delivery and loading area should be secured when the internal doors are opened;

d) incoming material should be inspected for potential threats (see 9.2.1d)) before this material is moved from the delivery and loading area to the point of use;

e) incoming material should be registered in accordance with asset management procedures (refer to 7.1.1) on entry to the site;

f) incoming and outgoing shipments should be physically segregated, where possible.

**9.2.2 Supporting utilities  
Design Effectiveness**

**No Deficiencies Noted**

**Description** Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

**Implementation guidance**

All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning should be adequate for the systems they are supporting. Support utilities should be regularly inspected and, as appropriate, tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply should be provided that conforms to the equipment manufacturer's specifications.

An uninterruptible power supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Power contingency plans should cover the action to be taken on failure of the UPS. A back-

up generator should be considered if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period. UPS equipment and generators should be regularly checked to ensure it has adequate capacity and is tested in accordance with the manufacturer's recommendations. In addition, consideration could be given to using multiple power sources or, if the site is large, a separate power substation.

Emergency power off switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided in case of main power failure.

The water supply should be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used). Malfunctions in the water supply system may damage equipment or prevent fire suppression from acting effectively. An alarm system to detect malfunctions in the supporting utilities should be evaluated and installed if required.

Telecommunications equipment should be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. Voice services should be adequate to meet local legal requirements for emergency communications.

**Other information**

Options to achieve continuity of power supplies include multiple feeds to avoid a single point of failure in the power supply.

**10.1.1 Documented operating procedures  
Design Effectiveness**

**No Deficiencies Noted**

**Description** Operating procedures should be documented, maintained, and made available to all users who need them.

**Implementation guidance**

Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety.

The operating procedures should specify the instructions for the detailed execution of each job including:

- a) processing and handling of information;
- b) backup (see 10.5);
- c) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
- d) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (refer to 11.5.4);
- e) support contacts in the event of unexpected operational or technical difficulties;
- f) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs (refer to 10.7.2 and 10.7.3);
- g) system restart and recovery procedures for use in the event of system failure;
- h) the management of audit-trail and system log information (see 10.10).

Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools, and utilities.

---

**10.1.2 Change management  
Design Effectiveness****No Deficiencies Noted****Description**

Changes to information processing facilities and systems should be controlled.

**Implementation guidance**

Operational systems and application software should be subject to strict change management control.

In particular, the following items should be considered:

- a) identification and recording of significant changes;
- b) planning and testing of changes;
- c) assessment of the potential impacts, including security impacts, of such changes;
- d) formal approval procedure for proposed changes;

e) communication of change details to all relevant persons;

f) fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. When changes are made, an audit log containing all relevant information should be retained.

#### **Other information**

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications (see also 12.5.1).

Changes to operational systems should only be made when there is a valid business reason to do so, such as an increase in the risk to the system. Updating systems with the latest versions of operating system or application is not always in the business interest as this could introduce more vulnerabilities and instability than the current version. There may also be a need for additional training, license costs, support, maintenance and administration overhead, and new hardware especially during migration.

---

### **10.1.3 Segregation of duties**

#### **Design Effectiveness**

#### **No Deficiencies Noted**

#### **Description**

Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

#### **Implementation guidance**

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent.

---

### **10.1.4 Separation of development, test, and operational facilities**

#### **Design Effectiveness**

#### **No Deficiencies Noted**

#### **Description**

Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.

#### **Implementation guidance**

The level of separation between operational, test, and development environments that is necessary to prevent operational problems should be identified and appropriate controls implemented.

The following items should be considered:

- a) rules for the transfer of software from development to operational status should be defined and documented;
- b) development and operational software should run on different systems or computer processors and in different domains or directories;
- c) compilers, editors, and other development tools or system utilities should not be accessible from operational systems when not required;
- d) the test system environment should emulate the operational system environment as closely as possible;
- e) users should use different user profiles for operational and test systems, and menus should display appropriate identification messages to reduce the risk of error;
- f) sensitive data should not be copied into the test system environment (refer to 12.4.2).

**Other information**

Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment, or system failure. In this case, there is a need to maintain a known and stable environment in which to perform meaningful

testing and to prevent inappropriate developer access.

Where development and test personnel have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code, which can cause serious operational problems.

Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, test, and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data (refer to 12.4.2 for the protection of test data).

---

**10.3.1 Capacity management**  
**Design Effectiveness**

**No Deficiencies Noted**

**Description**

The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

**Implementation guidance**

For each new and ongoing activity, capacity requirements should be identified. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore, managers should monitor the utilization of key system resources. They should identify trends in usage, particularly in relation to business applications or management information system tools.

Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

**10.4.1 Controls against malicious code  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

**Implementation guidance**

Protection against malicious code should be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls. The following guidance should be considered:

- a) establishing a formal policy prohibiting the use of unauthorized software (refer to 15.1.2);
- b) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken;
- c) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated;
- d) installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the checks carried out should include:
  - 1) checking any files on electronic or optical media, and files received over networks, for malicious code before use;
  - 2) checking electronic mail attachments and downloads for malicious code before use; this check should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;
  - 3) checking web pages for malicious code;
- e) defining management procedures and responsibilities to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks (refer to 13.1 and 13.2);
- f) preparing appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements (refer to clause 14);
- g) implementing procedures to regularly collect information, such as subscribing to mailing lists and/or checking web sites giving information about new malicious code;
- h) implementing procedures to verify information relating to malicious code, and

ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malicious code, are used to differentiate between hoaxes and real malicious code; all users should be made aware of the problem of hoaxes and what to do on receipt of them.

#### **Other information**

The use of two or more software products protecting against malicious code across the information processing environment from different vendors can improve the effectiveness of malicious code protection.

Software to protect against malicious code can be installed to provide automatic updates of definition files and scanning engines to ensure the protection is up to date. In addition, this software can be installed on every desktop to carry out automatic checks.

Care should be taken to protect against the introduction of malicious code during maintenance and emergency procedures, which may bypass normal malicious code protection controls.

---

#### **10.5.1 Information back-up**

##### **Design Effectiveness**

##### **No Deficiencies Noted**

##### **Description**

Backup copies of information and software should be taken and tested regularly in accordance with the agreed back-up policy.

##### **Implementation guidance**

Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information back-up should be considered:

- a) the necessary level of back-up information should be defined;
- b) accurate and complete records of the back-up copies and documented restoration procedures should be produced;
- c) the extent, e.g. full or differential backup, and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization;
- d) the back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;
- e) back-up information should be given an appropriate level of physical and environmental protection (refer to clause 9) consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the back-up site;
- f) back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary;
- g) restoration procedures should be regularly checked and tested to ensure that they

are effective and that they can be completed within the time allotted in the operational procedures for recovery;

h) in situations where confidentiality is of importance, back-ups should be protected by means of encryption.

Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans (refer to clause 14). For critical systems, the back-up arrangements should cover all systems information, applications, and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information, and also any requirement for archive copies to be permanently retained should be determined (refer to 15.1.3).

#### **Other information**

Back-up arrangements can be automated to ease the back-up and restore process. Such automated solutions should be sufficiently tested prior to implementation and at regular intervals.

---

### **10.7.2 Disposal of media**

#### **Design Effectiveness**

#### **No Deficiencies Noted**

##### **Description**

Media should be disposed of securely and safely when no longer required, using formal procedures.

##### **Implementation guidance**

Formal procedures for the secure disposal of media should minimize the risk of sensitive information leakage to unauthorized persons. The procedures for secure disposal of media containing sensitive information should be commensurate with the sensitivity of that information. The following items should be considered:

a) media containing sensitive information should be stored and disposed of securely and safely, e.g. by incineration or shredding, or erased of data for use by another application within the organization;

b) procedures should be in place to identify the items that might require secure disposal;

c) it may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items;

d) many organizations offer collection and disposal services for papers, equipment and media; care should be taken in selecting a suitable contractor with adequate controls and experience;

e) disposal of sensitive items should be logged where possible in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of non-sensitive information to become sensitive.

### Other information

Sensitive information could be disclosed through careless disposal of media (refer to 9.2.6 for information about disposal of equipment).

#### 10.8.3 Physical media in transit Design Effectiveness

**No Deficiencies Noted**

##### Description

Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

##### Implementation guidance

The following guidelines should be considered to protect information media being transported between sites:

- a) reliable transport or couriers should be used;
- b) a list of authorized couriers should be agreed with management;
- c) procedures to check the identification of couriers should be developed;
- d) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, e.g. for software, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;
- e) controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification; examples include:
  - 1) use of locked containers;
  - 2) delivery by hand;
  - 3) tamper-evident packaging (which reveals any attempt to gain access);
  - 4) in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

##### Other Information

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier.

#### 10.10.1 Audit logging Design Effectiveness

**No Deficiencies Noted**

##### Description

Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

##### Implementation guidance

Audit logs should include, when relevant:

- a) user IDs;
- b) dates, times, and details of key events, e.g. log-on and log-off;
- c) terminal identity or location if possible;
- d) records of successful and rejected system access attempts;
- e) records of successful and rejected data and other resource access attempts;
- f) changes to system configuration;
- g) use of privileges;
- h) use of system utilities and applications;
- i) files accessed and the kind of access;
- j) network addresses and protocols;
- k) alarms raised by the access control system;
- l) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

**Other information**

The audit logs may contain intrusive and confidential personal data. Appropriate privacy protection measures should be taken (refer to 15.1.4). Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (see 10.1.3).

**10.10.5 Fault logging  
Design Effectiveness**

**No Deficiencies Noted**

**Description**            Faults should be logged, analyzed, and appropriate action taken.

**Implementation guidance**

Faults reported by users or by system programs related to problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:

- a) review of fault logs to ensure that faults have been satisfactorily resolved;
- b) review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

It should be ensured that error logging is enabled, if this system function is available.

**Other information**

Logging of errors and faults can impact the performance of a system. Such logging should be enabled by competent personnel, and the level of logging required for individual systems should be determined by a risk assessment, taking performance degradation into account.

**11.1.1 Access control policy  
Design Effectiveness**

**No Deficiencies Noted**

**Description**            An access control policy should be established, documented, and reviewed based on business and security requirements for access.

**Implementation guidance**

Access control rules and rights for each user or group of users should be clearly

stated in an access control policy. Access controls are both logical and physical (refer to section 9) and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

- a) security requirements of individual business applications;
- b) identification of all information related to the business applications and the risks the information is facing;
- c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information (see 7.2);
- d) consistency between the access control and information classification policies of different systems and networks;
- e) relevant legislation and any contractual obligations regarding protection of access to data or services (refer to 15.1);
- f) standard user access profiles for common job roles in the organization;
- g) management of access rights in a distributed and networked environment which recognizes all types of connections available;
- h) segregation of access control roles, e.g. access request, access authorization, access administration;
- i) requirements for formal authorization of access requests (see 11.2.1);
- j) requirements for periodic review of access controls (see 11.2.4);
- k) removal of access rights (see 8.3.3).

#### **Other information**

Care should be taken when specifying access control rules to consider:

- a) differentiating between rules that must always be enforced and guidelines that are optional or conditional;
- b) establishing rules based on the premise, "Everything is generally forbidden unless expressly permitted," rather than the weaker rule, "Everything is generally permitted unless expressly forbidden";
- c) changes in information labels (see 7.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;
- d) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;
- e) rules which require specific approval before enactment and those which do not.

Access control rules should be supported by formal procedures and clearly defined responsibilities (for example refer to, 6.1.3, 11.3, 10.4.1, 11.6).

**11.2.1 User registration  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

**Implementation guidance**

The access control procedure for user registration and de-registration should include:

a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons, and should be approved and documented;

b) checking that the user has authorization from the system owner for the use of the information system or service; separate approval for access rights from management may also be appropriate;

c) checking that the level of access granted is appropriate to the business purpose (see 11.1) and is consistent with organizational security policy, e.g. it does not compromise segregation of duties (see 10.1.3);

d) giving users a written statement of their access rights;

e) requiring users to sign statements indicating that they understand the conditions of access;

f) ensuring service providers do not provide access until authorization procedures have been completed;

g) maintaining a formal record of all persons registered to use the service;

h) immediately removing or blocking access rights of users who have changed roles or jobs or left the organization;

i) periodically checking for, and removing or blocking, redundant user IDs and accounts (see 11.2.4);

j) ensuring that redundant user IDs are not issued to other users.

**Other information**

Consideration should be given to establish user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews (see 11.2.4) are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or service agents (see also 6.1.5, 8.1.3 and 8.2.3).

---

**11.2.3 User password management  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

The allocation of passwords should be controlled through a formal management process.

### **Implementation guidance**

The process should include the following requirements:

- a) users should be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group; this signed statement could be included in the terms and conditions of employment (see 8.1.3);
- b) when users are required to maintain their own passwords they should be provided initially with a secure temporary password (see 11.3.1), which they are forced to change immediately;
- c) establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;
- d) temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided;
- e) temporary passwords should be unique to an individual and should not be guessable;
- f) users should acknowledge receipt of passwords;
- g) passwords should never be stored on computer systems in an unprotected form;
- h) default vendor passwords should be altered following installation of systems or software.

### **Other information**

Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization. Other technologies for user identification and authentication, such as biometrics, e.g. fingerprint verification, signature verification, and use of hardware tokens, and smart cards, are available, and should be considered if appropriate.

---

#### **11.2.4 Review of user access rights Design Effectiveness**

#### **No Deficiencies Noted**

##### **Description**

Management should review users' access rights at regular intervals using a formal process.

##### **Implementation guidance**

The review of access rights should consider the following guidelines:

- a) users' access rights should be reviewed at regular intervals, e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment (see 11.2.1);
- b) user access rights should be reviewed and re-allocated when moving from one employment to another within the same organization;
- c) authorizations for special privileged access rights (refer to 11.2.2) should be

reviewed at more frequent intervals, e.g. at a period of 3 months;

d) privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;

e) changes to privileged accounts should be logged for periodic review.

#### **Other information**

It is necessary to regularly review users' access rights to maintain effective control over access to data and information services.

### **11.3.1 Password use Design Effectiveness**

#### **No Deficiencies Noted**

#### **Description**

Users should be required to follow good security practices in the selection and use of passwords.

#### **Implementation guidance**

All users should be advised to:

a) keep passwords confidential;

b) avoid keeping a record, e.g. paper, software file or hand-held device, of passwords, unless this can be stored securely and the method of storing has been approved;

c) change passwords whenever there is any indication of possible system or password compromise;

d) select quality passwords with sufficient minimum length which are:

1) easy to remember;

2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth, etc.;

3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);

4) free of consecutive identical, all-numeric or all-alphabetic characters;

e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;

f) change temporary passwords at the first log-on;

g) not include passwords in any automated log-on process, e.g. stored in a macro or function key;

h) not share individual user passwords;

i) not use the same password for business and non-business purposes.

If users need to access multiple services, systems or platforms, and are required to maintain multiple separate passwords, they should be advised that they may use a single, quality password (see d) above) for all services where the user is assured that

a reasonable level of protection has been established for the storage of the password within each service, system or platform.

**Other information**

Management of the help desk system dealing with lost or forgotten passwords needs special care as this may also be a means of attack to the password system.

---

**11.3.3 Clear desk and clear screen policy**

**Design Effectiveness**

**No Deficiencies Noted**

**Description**

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

**Implementation guidance**

The clear desk and clear screen policy should take into account the information classifications (see 7.2), legal and contractual requirements (refer to 15.1), and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:

a) sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;

b) computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

c) incoming and outgoing mail points and unattended facsimile machines should be protected;

d) unauthorized use of photocopiers and other reproduction technology, e.g., scanners, digital cameras, should be prevented;

e) documents containing sensitive or classified information should be removed from printers immediately.

**Other information**

A clear desk/clear screen policy reduces the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Consider the use of printers with pin code function, so the originators are the only ones who can get their printouts, and only when standing next to the printer.

---

**11.4.4 Remote diagnostic and configuration port protection**

**Design Effectiveness**

**No Deficiencies Noted**

**Description**

Physical and logical access to diagnostic and configuration ports should be controlled.

### **Implementation guidance**

Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port. An example for such a supporting procedure is to ensure that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.

Ports, services, and similar facilities installed on a computer or network facilities which are not specifically required for business functionality should be disabled or removed.

### **Other information**

Many computer systems, network systems, and communication systems are installed with a remote diagnostic or configuration facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access.

---

## **11.4.5 Segregation in networks**

### **Design Effectiveness**

### **No Deficiencies Noted**

#### **Description**

Groups of information services, users, and information systems should be segregated on networks.

#### **Implementation guidance**

One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. A graduated set of controls can be applied in different logical network domains to further segregate the network security environments, e.g. publicly accessible systems, internal networks, and critical assets. The domains should be defined based on a risk assessment and the different security requirements within each of the domains.

Such a network perimeter can be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains (refer to 11.4.6 and 11.4.7) and to block unauthorized access in accordance with the organization's access control policy (see 11.1). An example of this type of gateway is what is commonly referred to as a firewall. Another method of segregating separate logical domains is to restrict network access by using virtual private networks for user groups within the organization.

Networks can also be segregated using the network device functionality, e.g. IP switching. Separate domains can then be implemented by controlling the network data flows using the routing/switching capabilities, such as access control lists.

The criteria for segregation of networks into domains should be based on the access control policy and access requirements (see 10.1), and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology (refer to 11.4.6 and 11.4.7).

In addition, segregation of networks should be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

Consideration should be given to the segregation of wireless networks from internal

and private networks. As the perimeters of wireless networks are not well defined, a risk assessment should be carried out in such cases to identify controls, e.g. strong authentication, cryptographic methods, and frequency selection, to maintain network segregation.

#### **Other information**

Networks are increasingly being extended beyond traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorized access to existing information systems that use the network, some of which may require protection from other network users because of their sensitivity or criticality.

---

### **11.5.2 User identification and authentication Design Effectiveness**

#### **No Deficiencies Noted**

#### **Description**

All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

#### **Implementation guidance**

This control should be applied for all types of users (including technical support personnel, operators, network administrators, system programmers, and database administrators)

User IDs should be used to trace activities to the responsible individual. Regular user activities should not be performed from privileged accounts.

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented for such cases. Additional controls may be required to maintain accountability.

Generic IDs for use by an individual should only be allowed either where the functions accessible or actions carried out by the ID do not need to be traced, e.g. read only access, or where there are other controls in place, e.g. password for a generic ID only issued to one staff at a time and logging such instance.

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

#### **Other information**

Passwords (see also 11.3.1 and 11.5.3) are a very common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user identification and authentication should be suitable to the sensitivity of the information to be accessed.

Objects such as memory tokens or smart cards that users possess can also be used for identification and authentication. Biometric authentication technologies that use the unique characteristics or attributes of an individual can also be used to authenticate the person's identity. A combination of technologies and mechanisms securely linked will result in stronger authentication.

**11.5.3 Password management system  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

Systems for managing passwords should be interactive and should ensure quality passwords.

Implementation guidance

A password management system should:

- a) enforce the use of individual user IDs and passwords to maintain accountability;
- b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
  
- c) enforce a choice of quality passwords (see 11.3.1);
- d) enforce password changes (see 11.3.1);
- e) force users to change temporary passwords at the first log-on (see 11.2.3);
- f) maintain a record of previous user passwords and prevent re-use;
- g) not display passwords on the screen when being entered;
- h) store password files separately from application system data;
- i) store and transmit passwords in protected, e.g. encrypted or hashed, form.

**Other information**

Passwords are one of the principal means of validating a user's authority to access a computer service.

Some applications require user passwords to be assigned by an independent authority; in such cases, points b), d) and e) of the above guidance do not apply. In most cases the passwords are selected and maintained by users. See section 11.3.1 for guidance on the use of passwords.

---

**11.5.5 Session time-out  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

Inactive sessions should shut down after a defined period of inactivity.

**Implementation guidance**

A time-out facility should clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity. The time-out delay should reflect the security risks of the area, the classification of the information being handled and the applications being used, and the risks related to the users of the equipment.

A limited form of time-out facility can be provided for some systems which clear the screen and prevent unauthorized access, but does not close down the application or network sessions.

## Other information

This control is particularly important in high risk locations, which include public or external areas outside the organization's security management. The sessions should be shut down to prevent access by unauthorized persons and denial of service attacks.

### 11.7.1 Mobile computing and communications

#### Design Effectiveness

#### No Deficiencies Noted

#### Description

A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

#### Implementation guidance

When using mobile computing and communicating facilities, e.g. notebooks, palmtops, laptops, smart cards, and mobile phones, special care should be taken to ensure that business information is not compromised. The mobile computing policy should take into account the risks of working with mobile computing equipment in unprotected environments.

The mobile computing policy should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques (refer to 12.3).

Users of mobile computing facilities in public places should take care to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date (see 10.4).

Back-ups of critical business information should be taken regularly. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information.

Suitable protection should be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile

computing facilities should only take place after successful identification and authentication, and with suitable access control mechanisms in place (see 11.4).

Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers, and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization should be established for cases of theft or loss of the mobile computing facilities. Equipment carrying important, sensitive, and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment (refer to 9.2.5).

Training should be arranged for personnel using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that should be implemented.

**Other information**

Mobile network wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are:

- a) some wireless security protocols are immature and have known weaknesses;
- b) information stored on mobile computers may not be backed-up because of limited network bandwidth and/or because mobile equipment may not be connected at the times when backups are scheduled.

---

**12.5.1 Change control procedures  
Design Effectiveness**

**No Deficiencies Noted**

**Description**

The implementation of changes should be controlled by the use of formal change control procedures.

**Implementation guidance**

Formal change control procedures should be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control, and managed implementation.

This process should include a risk assessment, analysis of the impacts of changes, and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

Wherever practicable, application and operational change control procedures should be integrated (see also 10.1.2). The change procedures should include:

- a) maintaining a record of agreed authorization levels;
- b) ensuring changes are submitted by authorized users;
- c) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;
- d) identifying all software, information, database entities, and hardware that require amendment;
- e) obtaining formal approval for detailed proposals before work commences;
- f) ensuring authorized users accept changes prior to implementation;
- g) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

- h) maintaining a version control for all software updates;
- i) maintaining an audit trail of all change requests;
- j) ensuring that operating documentation (see 10.1.1) and user procedures are changed as necessary to remain appropriate;
- k) ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

**Other information**

Changing software can impact the operational environment.

Good practice includes the testing of new software in an environment segregated from both the production and development environments (see also 10.1.4). This provides a means of having control over new software and allowing additional

protection of operational information that is used for testing purposes. This should include patches, service packs, and other updates. Automated updates should not be used on critical systems as some updates may cause critical applications to fail (refer to 12.6).

**13.1.1 Reporting information security events**

**Design Effectiveness**

**No Deficiencies Noted**

**Description**

Information security events should be reported through appropriate management channels as quickly as possible.

**Implementation guidance**

A formal information security event reporting procedure should be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event. A point of contact should be established for the reporting of information security events. It should be ensured that this point of contact is known throughout the organization, is always available, and is able to provide adequate and timely response.

All employees, contractors and third party users should be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact. The reporting procedures should include:

- a) suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed;
- b) information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event;
- c) the correct behavior to be undertaken in case of an information security event:
  - 1) noting all important details, e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behavior, immediately;

2) not carrying out any own action, but immediately reporting to the point of contact;

d) reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches.

In high-risk environments, a duress alarm may be provided whereby a person under duress can indicate such problems. The procedures for responding to duress alarms should reflect the high risk situation such alarms are indicating.

NOTE: A duress alarm is a method for secretly indicating that an action is taking place 'under duress.'

### **Other Information**

Examples of information security events and incidents are:

- a) loss of service, equipment or facilities,
- b) system malfunctions or overloads,
- c) human errors,
- d) non-compliances with policies or guidelines,
- e) breaches of physical security arrangements,
- f) uncontrolled system changes,
- g) malfunctions of software or hardware,
- h) access violations.

With due care of confidentiality aspects, information security incidents can be used in user awareness training (see 8.2.2) as examples of what could happen, how to respond to such incidents, and how to avoid them in the future. To be able to address information security events and incidents properly it might be necessary to collect evidence as soon as possible after the occurrence (refer to 13.2.3).

Malfunctions or other anomalous system behavior may be an indicator of a security attack or actual security breach and should therefore always be reported as information security event.

More information about reporting of information security events and management of information security incidents can be found in ISO/IEC TR 18044.

---

### **13.1.2 Reporting security weaknesses**

#### **Design Effectiveness**

#### **No Deficiencies Noted**

#### **Description**

All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

#### **Implementation guidance**

All employees, contractors and third party users should report these matters either to their management or directly to their service provider as quickly as possible in order to

prevent information security incidents. The reporting mechanism should be as easy, accessible, and available as possible. They should be informed that they should not, in any circumstances, attempt to prove a suspected weakness.

**Other Information**

Employees, contractors and third party users should be advised not to attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.