# Mobile Devices Security Management under the Framework of ISO27001

**Zhao Lijun[1], He Jun[2]**

[1]Department of Information equipment, the Academy of Equipment, Beijing 101416, China
[2]Lab of Complex System Simulation, the Academy of Equipment, Beijing 101416, China
zlj0908@sina.com

**Abstract -** People are becoming more and more dependent on mobile devices in their work or life, and the security management issue of mobile devices is becoming much more serious than ever. ISO 27001 provides a practical framework for information security management which is based on risk assessment. However, it cannot be quite adaptable for mobile devices, because these developing mobile information devices lead to new challenges and security risks. This paper takes a thorough survey of mobile devices security issues, and then proposes a solution to these issues under ISO 27001 information security management system framework.

**Index Terms -** mobile devices, information security, ISO 27001, ISMS, PDCA.

## 1. Introduction

In recent years, the explosive growth of mobile devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a dramatic change in the computing and storing world: computing will not merely rely on the capability provided but the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer society [1]. Mobile devices are now playing more and more roles in our daily life and work, Mobile devices include smartphones, tablet computers, laptops, personal digital assistants (PDAs), storage devices (e.g. USB drives), scanners and connectivity devices (e.g. Wi-Fi, Bluetooth). These mobile devices provide significant value add to organizations but risks associated with their use need to be managed. Smartphones exceeded 55% of the mobile phone market [2]. For many people, smartphones can be used for Internet banking, browsing, taking and storing photos, scheduling one's daily work. This brings some risks. Smartphones can be infected with malicious software, and sensitive data can be stolen. Phishing attacks work just as effectively with smartphones as with any other device. Using a desktop or laptop PC without security software has become unthinkable. With mobile phones, this sense of responsibility has not yet reached the majority of users, even though important personal data, personal photos and even company data can be stored on smartphones.

## 2. Issues of Mobile Devices Security Management

Mobile Devices security management is every important for an organization. Therefore, issues and risks of mobile devices security management must be recognized. Due to the rapid development of mobile device technique, numerous new problems arise from the absence of management to the specific consideration of mobile device**s.**

### *A. Unauthorized Modification of mobile devices*

Unauthorized modification of mobile devices represents an additional level of risk. The terminology frequently applied to this practice is jail-breaking (Apple iOS devices) or rooting (Android devices) which removes vendor imposed limitations on the mobile devices. This leaves the device in an insecure state, making it more prone to malware and compromise. Unauthorized applications can be created to take advantage of the elevated privileges in these mobile devices to manipulate data, e.g. report false results to central management system (critical infrastructure) and other security tools that it is reporting to. Users of these modified devices can remove any centrally applied corporate policy controls on the device, making it more vulnerable to other security threats.

### *B. Powerful mobile devices*

Many mobile devices such as smartphones or PDAs are now equipped with fast processor and embedded operating system (OS). Many applications specific to embedded OS are developed and deployed. As a matter of fact, such mobile devices are powerful computers. Meantime, these devices are usually installed with multiple communication measures, such as Bluetooth, TCP/IP protocols, etc.

With these rich and powerful features, vulnerabilities are also exposed to potential adversary, who can exploit these vulnerabilities to attack mobile devices. Therefore, the mobile devices have become a prized target, where there are increased numbers of malware targeted at intercepting valuable data [3].

### *C. Vague security border*

End-to-end information assets always have limited boundary. A PC or server will always be in some place of a building, and so the security border can be easily recognized. But with mobile devices, it is hard to control the range of mobile devices. So, the security boundary is becoming vague under the existence of mobile devices.

### *D. Versatile function of mobile devices*

USB drives can now store much more software, and so it is quite easy to make a USB drive as a booting disk which can easily go into a PC disks but avoid the protection software of that PC. Therefore, mobile devices can play more functions, such as storing data, booting system, mp3 player, etc. It is

convenient for people to use mobile devices, but it is in high risk when using these versatile functions of mobile devices.

*E. Cross-border information Theft*

Mobile devices can be anywhere, as the inherent mobility (beginning from laptops) has always made it impossible to rely on a strong perimeter for adequate protection. The cloud computing revolution and the myriad of hosted application services that are not geographically fixed has made it easier for data to cross national borders [4]. With the increased use of mobile network, the applications and data stored in mobile devices lost locally and globally, may put critical infrastructure at risk. In addition, data travelling on the mobile devices is typically subject to laws and regulations that will vary from one jurisdiction to another.

*F. Data Disposal.*

The amount of data that can be stored and processed in mobile devices has been growing dramatically. Inappropriate device disposal procedures may bring the risk of sensitive information being retained on the device and unauthorized access. Organizational computing assets should be subject to company asset management procedures which should include secure disposal for assets containing sensitive data. However, the execution of these procedures can often be a grey area when dealing with personal devices in the workplace. This requires clear organizational policies in order to safeguard sensitive, confidential and highly valued information (including commercial intelligence).

## 3. ISO 27001 ISMS Framework

*A. Introduction to ISO27000 series*

ISO 27000 series includes multiple standards for building Information Security Management System (ISMS), as show in fig.1.

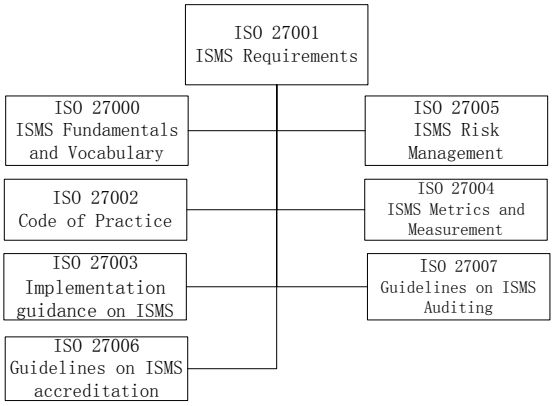


Figure 1. ISO 27000 information security standard series.

ISO 27001 is the only standard that can provide certification for an organization. It outlines the ISMS framework by which an organization can build its own ISMS based on PDCA (Plan-Do-Check-Action) model. The other standards provide profound support for an organization to build its ISMS. ISO 27002 provides choice from 133 concrete controls based on risk assessment. Though mobile devices covered, but it is not enough due to the ongoing technique limitations. ISO 27003 is ISMS Implementation guidance which implements PDCA in more detail, including identification of assets, threat identification, risk assessment, analysis and improvement of controls. ISO 27004 is ISMS Metrics and measurement which evaluates effectiveness of information security controls and objectives. ISO 27005 is ISMS Risk Management which is a new standard that is mainly concerned with risks. ISO 27006 is Guidelines on ISMS accreditation. ISO 27007 is Guidelines on ISMS Auditing.

*B. Plan-Do-Check-Action Process*

According to 27001, building ISMS is thorough a 4-phase process called PDCA (Plan-Do-Check-Action) process, as shown in fig. 2. In each phase, there are different activities. In PLAN phase, there is only one activity called "establish ISMS". In DO phase, there are two activities, called "Implement and operate the ISMS". In Check phase, there are two activities called "monitor and review ISMS". In ACT phase, there are also two activities called "maintain and improve".

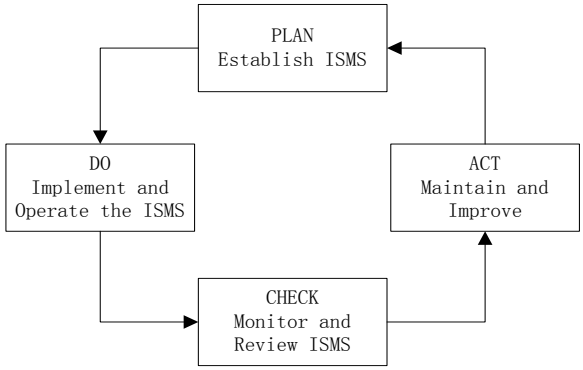


Figure 2. PDCA process.

*C. ISO 27001 Categories*

ISO 27001 provides 39 control objectives and 133 controls for information security. The ISO 27001 categories are shown in fig.3. The form is as shown in fig. 4.

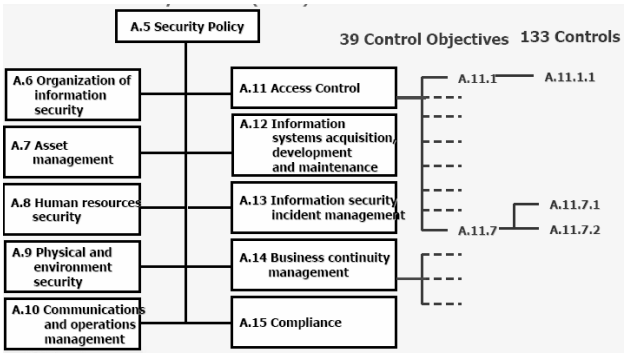


Figure 3. ISO 27001 categories.

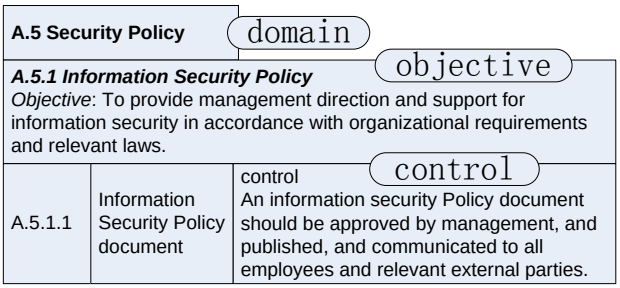


Figure 4. Form of ISO 27001 domain, objective and control.

However, these control objectives and controls are mostly too general, and for mobile devices information security it is not quite adaptable.

## 4. Mobile Devices Security under ISO 27001 Framework

### *A. Information Security Policy*

According to ISO 27001, the goal of information security policy is to set up management direction and support for information security. Information Security Policy is a directive and strategic file which includes the goal and strategy of information security. As the mobile devices security is particularly important, so it must be particularly shown and considered in Information Security Policy and. Information Security Policy should include the following aspects: information security view, objective, strategy, range, organizational structure, responsibility, assets, etc. Especially, policy relating to mobile devices should be effective, definite and complete. However, concrete and detail process should be concerned in policy.

Developing information security policy should obey to a flow: 1) determine the range of information security policy, 2) evaluate and analyze risk, and 3) check, approve and implement information security policy. While developing information security policy, advanced information security technique on mobile devices is the basic assurance. All related techniques should be collected and updated in time.

### *B. Organization of Information Security*

Information security will be managed within an organization. Management will approve information security policies, assign security roles, and coordinate and review the implementation of security across the organization. Information assets and information technology regarding to mobile devices must be recognized and updated in time.

### *C. Human Resources Security*

Mobile devices are always used by people, so human resources security is important. Everyone in an organization must understand his or her responsibilities and will know the manners to reduce the risk of theft, fraud or misuse of mobile devices. Thus, responsibilities should be divided into different layers. The top layer usually monitors and audits the information security activities of an organization. The second layer manages the routine information security activities. The third layer is mobile device owner who operates mobile devices according the policy, and is subject to upper layer's management.

### *D. Physical and Environmental Security*

Though mobile devices have not limited boundary, physical and environmental security must be considered in order to prevent unauthorized physical access, damage, theft, compromise, and interference to mobile information and facilities. Locations housing mobile devices will be secured with appropriate security barriers and entry controls. They will be physically protected from unauthorized access, damage and interference. Secure areas will be protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Security will be applied to off-site equipment. All equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal in compliance with statewide policies.

### *E. Communications and Operations Management*

There are much more communications and operations for mobile devices than for other devices. Responsibilities and procedures for administrating mobile devices must be established according to information security policy. Virus and malicious code for mobile devices should be detected protect the integrity of software and information in mobile devices. Exchange of sensitive data with other organizations must be done based on a formal exchange policy. Mobile devices containing sensitive data will be protected against unauthorized access, misuse.

### *F. Access Control*

For an organization with mobile devices, access control includes two aspects: one is access to organizational information systems from mobile devices; the other is access to outer information facilities from mobile devices. Both these two aspects of access control for mobile devices should be controlled on the basis of business and security requirements. Formal procedures should be established for the mobile devices to control access rights to both inner and outer information facilities, to prevent unauthorized access.

## 5. Conclusion

Information security management with mobile devices always meets new challenges with the rapid development of mobile technique. This paper analyses the issues of information security with mobile devices. It is a good practice with ISO 27000 information security series standards. The design, operation, use, and management of mobile information assets are subject to statutory, regulatory, and contractual security requirements in order to avoid breaches of any law.

The following controls are a good reference for Information Security Management system under ISO 27001 framework.

- Never set the login dialog box to remember the password;
- Keep antivirus protection up-to-date, as well as the operating system and application security patches;

- Password-protect all devices, such as removable drives and compact disks (CDs);
- Do not store unencrypted sensitive information on mobile devices;
- Incorporate a time-out function that requires re-authentication after 30 minutes of inactivity;
- Back up your data to a location separately from the device;
- Include both hardware/device-based authorization and application-based authorization for access control mechanisms;
- Do not keep mobile devices online when not in use. Either shut them off or physically disconnect them from the Internet connection; Lost or misplaced government-issued devices must be immediately reported to management.

## References


[1] Marco Conti, Body, *Personal and Local Ad Hoc Wireless Networks*, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2] http://www.comscore.com/ger/Insights/Presentations_and_Whitepapers/2013/The_Mobile_Shift

[3] Kao, I, *Securing Mobile Devices in The Business Environment, IBM Global Technology Services – Thought Leadership* White Paper, October 2011

[4] Ernst & Young, *Data Loss Prevention: Keeping Your Sensitive Data Out of The Public Domain*, Insights on IT Risk Business Briefing, 2012

[5] ISO/IEC 27000:2009, *Information* Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary, ISO/IEC, Geneva, 2009.

[6] ISO/IEC 27001:2005, Information Technology—Security Techniques—Information *Security* Management Systems—Requirements, ISO/IEC, Geneva, 2005.

[7] ISO/IEC 27002:2005, Information Technology—Security Techniques—Information Security Management Systems—Code of Practice for Information Security Management, ISO/IEC, Geneva, 2005.

[8] ISO/IEC 27003:2010, *Information* Technology—Security Techniques—Information Security Management System Implementation Guidance, ISO/IEC, Geneva, 2010.

[9] ISO/IEC 27004:2009, *Information* Technology—Security Techniques—Information Security Management—Measurement, ISO/IEC, Geneva, 2009.

[10] ISO/IEC 27005:2008, *Information* Technology—Security Techniques—Information Security Risk Management, ISO/IEC, Geneva, 2008