Risk/control framework related to the security of mobile business applications

Jolien Démoed MSc
is Senior Consultant at KPMG Advisory.
demoed.jolien@kpmg.nl

Karima Siamari MSc
is Senior Consultant at KPMG Advisory.
siamari.karima@kpmg.nl

There is an increasing number of business applications on corporate mobile phones these days. There are threats to consider and risks involved when releasing corporate financial or other types of sensitive information on the go. Enterprises are responsible for mobile application and device security in their day-to-day business. In case of a loss of sensitive organizational data, management is held accountable. This article explores the risks surrounding the use of mobile business applications by employees and the measures organizations can take in order to become and stay in control.

INTRODUCTION

Organizations across the globe are developing or using mobile applications in order to increase employee productivity. Mobile technology fulfils an increasingly important role within business processes. Users have been familiar with mobile access and apps for a while to retrieve real-time information anywhere at any time. It is therefore no surprise that more organizations are providing access to financial and customer information via mobile devices.

As a relatively new way of working, this may pose additional challenges (e.g. lost/stolen mobile devices, mobile security) and consequently, result in security risks. In addition, already existing challenges such as malware, employee security awareness are also still applicable and cannot be neglected. Therefore, a strong focus on mobile application security and the accountability of management for the underlying risks is required. When identified risks are not addressed sufficiently through detailed risk assessments and implementation of a coherent set of security measures, sensitive financial data may become compromised. Using mobile applications in organizations raises the question whether additional measures – in comparison to regular online business applications – are needed to cover the security risks related to mobile business applications.

Recognizing these risks, organizations will become more aware of their responsibility for mobile application and device security. A risk/control framework will help organizations to guide their approach to control all risks involved and to be able to continuously test and update the security posture. This article focuses on securing mobile business solutions by determining which risks exist and how these could be controlled.

RELEVANCE OF SECURING MOBILE BUSINESS APPLICATIONS

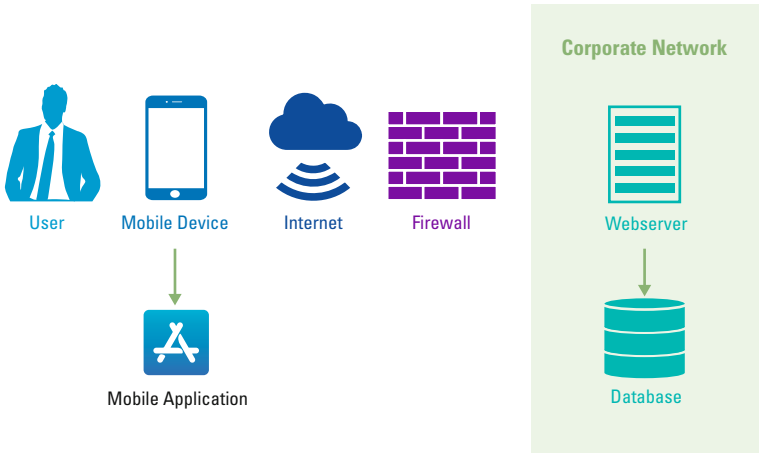
Mobile devices have evolved from merely providing access to enterprise e-mail to removing logistical process delays and tracking business transactions at any time through the use of mobile business applications. For example, these applications provide the organization the ability to review, approve or reject purchase requisitions and supplier invoices, continuously follow their order backlog and keep track of their Order-to-Cash and Purchase-to-Pay process performance trends in real-time. Mobile applications are rapidly becoming the primary – and maybe even single – communication channel for customers and employees and therefore the applications are expected to be secure and to protect privacy ([Ham17]). Despite numerous positive and useful features/benefits, the use of mobile applications in organizations also poses certain threats. In the context of this article, we ought to identify the (f)actors involved when using mobile business applications to identify potential threats. The actors identified are shown in Figure 1: the user, the mobile device, mobile application, the internet, firewall, the corporate network, webserver, and database.

The main threats taking the involved actors into account are discussed next.

Unprotected applications or networks

When network gateways are placed at easily accessible locations and include unpatched vulnerabilities, it may enable hackers to control the network gateways and intercept communications ([Enis17]). If so, it could lead to severe data privacy violations associated with the applicable GDPR legislation. Incidents may occur where sensitive organizational data is lost, which would have a significant negative impact on an organization's repu-

Figure 1. Actors mobile business applications in a highly simplified figure.



tation leading to financial damage. The implementation of the bring your own device (BYOD) policy at organizations acts as a complicating factor, as personal devices have diverse interfering applications installed.

Mobile security unawareness
Employees are considered to be the weakest link in information security ([Line07]). When there is limited awareness among employees regarding the security of mobile devices and the classification of data that is stored on devised and in the applications, this could bring about security incidents. For example, when sensitive organizational data is sent to personal non-managed devices by employees trying to meet a deadline. Most employees view security as a hindrance to their productivity. In case a way is found to work around security measures, there is a high chance that it will be used.

(Un)intended employee behavior
Employee behavior can have a substantial detrimental impact on the security of mobile business applications. When employees are insufficiently aware of the risks involved, their mobile activities could undermine the technical controls that organizations have in place to protect their data, such as incidents to consider, cases of malicious employees that have terminated, but that still have access to corporate applications on their mobile devices or cases where the mobile device is lost or stolen, etc. ([ISAC10]).

Access by external parties
External parties who have access to the network and systems of the organization are difficult to manage and monitor. Third parties are a known source of significant security breaches and are a target for hackers (as a steppingstone). This introduces more vulnerabilities and an increased risk to the corporate environment. These external parties usually require high privileged access to infrastructure and systems and therefore impose a high impact if those privileges are misused or compromised.

RISKS RELATED TO THE SECURITY OF MOBILE BUSINESS APPLICATIONS

The growing use of mobile devices within organizations has increased the threat level of IT security breaches, misuse of sensitive data and – as a result – reputational damage. Therefore, it is imperative that mobile business applications are subject to periodic audits performed by IT auditors.

In order to effectively perform such an IT audit, it is important to start with a risk assessment and to leverage a control framework designated for mobile business applications. To perform an IT audit effectively, the scope should only include the most relevant actors where organizations are able to influence and mitigate the risks involved. This leads to the following audit objects which are in scope for the designed risk/control framework:

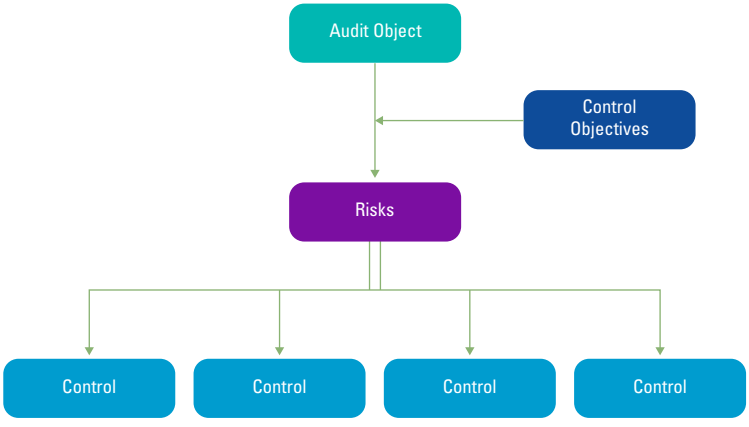
- User
- Mobile device
- Mobile (business) application
- Corporate network

Considering the objects in scope and the threats identified in the previous section, a risk assessment is performed in which risks are evaluated which are deemed relevant to the subject of mobile business applications. These risks should be controlled by organizations when using mobile business applications as part of their operational processes and will serve as a basis for identifying related mitigating controls. The audit objects, the risks and the controls are combined in a risk/control framework which is included in this article.

RISK/CONTROL FRAMEWORK MOBILE BUSINESS APPLICATIONS

The risk/control framework has been established by analyzing theory, identifying relevant objects and performing a risk assessment. The interlinkage of the appropriate controls, the risks, the control objectives and the relevant audit objects is depicted in Figure 2. The control objectives are desired conditions for an audit object which, if achieved, minimize the potential that the identified risk will occur. Hence, the control objectives are linked to the identified audit objects and are subject to the risks that threaten the effectiveness of the control objectives. The controls should mitigate the security risks to which mobile business applications are exposed.

Figure 2. Establishing the risk/control framework.



Resulting from the aforementioned described process of setting up a risk/control framework, Table 1 on the next page shows the risk/control framework that has been established.

CONTROL OBJECTIVES OF THE RISK/ CONTROL FRAMEWORK EXPLAINED

The risk/control framework can be used by organizations in order to continuously test and update technical measures related to the usage of mobile business applications in order to safeguard the organization and its sensitive data.

Controls related to the technical setup of the mobile business application and a secure application life cycle management, control objective 1, are vital and need to be taken into account. These controls focus on tracking the risk of an application as it moves through the development lifecycle. Binary hardening, input validation and encryption complement a secure development environment to prevent vulnerabilities and unintended leakage of data from unprotected applications. These controls are even more relevant for mobile business applications as mobile devices are taken everywhere and most likely contain sensitive business data.

Securing the mobile business application by means of sufficient authentication and authorization configuration, control objective 2, 3 and 4, is relevant for the mobile business applications, but is highly dependent on how the IT infrastructure and the mobile environment has been set up. Even though it could be that part of the authentication logic is performed by the back-end server, it is important to consider this as integral part of the mobile architecture. Plainly, authentication and authorization problems are prevalent security vulnerabilities and rank second highest in the OWASP Top 10 ([OWAS17]) and are therefore included in the established risk/control framework.

In order to prevent unauthorized access and unintended leakage of corporate data, it is also vital to incorporate the right technical security measures to protect the mobile device (e.g. anti-virus, patch and vulnerabilities, separate corporate and private environment and data sharing). The controls, control objectives 6, 7 and 10, that are related to these technical measure are a very important part of the risk/control framework: it would trigger organizations to rethink their mobile architecture strategy, to be continuously aware of potential vulnerabilities and to implement and monitor the security measures.

In order to steer organizations in their strategy to control their mobile environment, controls related to MDM solutions are also incorporated. An MDM solution, control objective 8, will provide input to secure, manage and monitor corporate owned devices that access sensitive corporate data.

> People are the most important link in the cyber security chain

Cryptographic controls on mobile devices are almost inevitable. As mobile devices may contain sensitive corporate data, a secure manner of protecting data using cryptographic techniques is required; control objective 9. Cryptographic controls will provide added value to organizations for protecting their mobile data.

Mobile devices should be safeguarded from external threats. Therefore, when connecting to the corporate network, stringent security standards should be applied to protect corporate data; control objective 5 and 11. Controls related to these security standards will guide the organization in how to continuously monitor and test connectivity security between mobile devices and the corporate network.

A well-known saying in the world of IT security is that people are the weakest link in cyber security. We would like to reframe that as: people are the most important link in the cyber security chain. The risk/control framework incorporates "soft controls" – control objective 12 and 13 – related to users (people aspect) of mobile devices.

In conclusion, the risk/control framework consists of several sections that relate to:

- secure development
- technical setup
- authentication & authorizations
- cryptography
- sessions handling
- using MDM
- data security
- connections with corporate network
- user awareness and
- device / asset management.

Table 1. Risk/control framework mobile business applications.

Audit Object	Control Objective	CO / Risk ID	Risk	Control ID	Control Description
Mobile business application	Controls provide reasonable amount of assurance that the mobile application is technical sufficiently secured	1	The technical security setup of the mobile business application is insufficient leading to increased vulnerability or unintended leakage of data	1.1	A secure (mobile) application lifecycle management policy is in place and includes a specification of the design, development and testing of mobile applications. The security officer is responsible for a yearly sign-off of this policy.
				1.2	The release of mobile applications to the app store and modification of future releases follows the process as described in the mobile application lifecycle management policy.
				1.3	Binary hardening techniques are standard protocol in application development and enforced at the time of application coding and maintenance.
				1.4	User/application-supplied data is subject to input validation prior to further processing.
				1.5	The mobile business application source code is encrypted according to good practice market standards to ensure that the code is kept secret
				1.6	Common leakage points/ vulnerabilities are monitored by the IT organization on a regular basis by means of specialized tooling and resolved accordingly.
	Controls provide reasonable amount of assurance that authentication to the mobile business application is sufficiently secure	2	Authentication to the mobile business application is insufficiently secure	2.1	Multi (2 or 3-) factor authentication is enforced when logging into the mobile business application by the user and system administrator.
				2.2	Login to the mobile business application is limited to the online mode.
	Controls provide reasonable amount of assurance that session handling is appropriately configured	3	Improper configuration of session handling leading to malicious session hijacking/ unauthorized access	3.1	When the user has exited the application, the current session will be terminated. It is impossible to continue with the same session.
				3.2	Users are required to re-authenticate or to sign electronically when performing critical actions (such as providing approval on invoices via mobile devices).
	Controls provide reasonable amount of assurance that authorizations with respect to the mobile business application are sufficiently accurate	4	User authorizations are inaccurate leading to authorizations being too wide and / or SoD conflicts	4.1	The mobile device access controls are in line with the generic Information/IT security policy and data classification policy.
				4.2	Access to mobile business applications follows the regular joiner approval process of the organization.
				4.3	Authentication to mobile business applications is (automatically) revoked when the employee leaves the organization and follows the regular leaver process.
				4.4	Authorizations within the mobile business application are periodically reviewed by the system owner in line with the established authorization procedures.
	Controls provide reasonable assurance that automated data processing within the mobile business applications works as intended.	5	Data is not processed correctly leading to false output	5.1	As part of the change management processes, specific testing is performed to verify that the mobile business application produces the expected results and is working as designed (i.e. the logic).
Mobile device	Controls provide reasonable amount of assurance that corporate data is stored appropriately secured	6	Data is stored in an insecure way making it more easily accessible	6.1	When corporate data is stored on the device it is protected in accordance with the information classification policy and the requirements from the IT organizations.
				6.2	Mobile device encryption settings are in line with the IT security as well as data classification policy.
				6.3	Data stored on the device is backed up on a separate and secure location accessible to the organization and/or employee.
	Controls provide reasonable amount of assurance that the mobile device is sufficiently secured	7	The technical security of the mobile devices insufficient leading to unauthorized access or unintended leakage of data	7.1	Mobile device antivirus software is updated regularly to prevent perpetuation of malware.
				7.2	Patch and Vulnerability management processes are established within the organization. Mobile devices are subject to these processes and its software is regularly updated/patched.
				7.3	Common leakage points/vulnerabilities are monitored by the IT organization on a regular basis by means of specialized tooling, and resolved accordingly.
				7.4	The corporate and personal environment are separated on the mobile device (Chinese wall).
				7.5	Mobile device management (MDM) technically enforces that unsigned third-party apps, which may carry malware or provide a gateway for malicious outsiders to enter the corporate network, cannot be installed on the mobile device.
				7.6	MDM technically enforces that sharing possibilities of data between the mobile business application and third-party applications is restricted according to the data classification policy.

Audit Object	Control Objective	CO / Risk ID	Risk	Con-trol ID	Control Description
	Controls provide reasonable amount of assurance that mobile devices are managed in a controlled way	8	Mobile devices are not managed in a controlled way leading to unauthorized access or unintended leakage of data	8.1	An MDM solution is used by the company in order to manage and secure mobile devices provided to employees. Any attempt to bypass the MDM solution results in immediate disconnection from all corporate resources.
				8.2	Mobile devices are required to register for the MDM solution of the organization when provisioned to employees.
				8.3	The technical security measures enforced by the MDM solution are periodically reviewed and updated by the security officer / security responsible.
				8.4	The organization has established procedures in order to safely destroy, replace or reuse mobile devices which may contain corporate data, ensuring that corporate data is not disclosed.
				8.5	An MDM solution is used to enable the organization to remotely wipe data stored on lost or stolen devices.
	Controls provide reasonable amount of assurance that corporate data is securely encrypted	9	The cryptography used to ensure corporate data is encrypted, is broken	9.1	Secure key management system (KMS) procedures are established and documented, including key generation, key distribution, key storage and key destruction. The role of key custodians, operators, key owners and KMS users are also defined in the policy.
				9.2	KMS procedures are periodically tested / dry run by the IT organization, to ensure that the procedures work effectively.
				9.3	Cryptography keys are stored in not easily accessible locations or are hard coded.
				9.4	The use of strong encryption protocols (i.e. not generally known to be easily broken within a certain timeframe) is standard in the mobile business application life cycle.
Corporate network	Controls provide reasonable amount of assurance that the connection between the mobile device and corporate network is appropriately secured	10	Connections between the mobile devices and corporate network are insufficiently secure leading to unauthorized access and exposure of corporate data	10.1	Mobile access to shared files or network drives that contain corporate data is only provided to employees in accordance with the data classification policy and done so in a secure manner in accordance the technical requirements determined by the IT organization.
				10.2	Mobile device users are connecting to the enterprise network via a secure and encrypted connection, using VPN, IP Security (IPsec), Transport Layer Security (TLS 2) or comparable secure protocols that adhere to good practice standards.
	Controls provide reasonable amount of assurance that mobile devices are appropriately used by employees.	11	Employees are not aware of guidelines/ procedures to be followed related to corporate network security.	11.1	An IT Security policy exist and includes guidelines and procedures with regards to securing the corporate network related to connection to mobile devices which is enforced by management.
				11.2	The IT security policy is periodically reviewed by the IT organization/ security officer and updated accordingly.
User	Controls provide reasonable amount of assurance that mobile devices are appropriately used by employees	12	Employees are not using the mobile devices appropriately and securely	12.1	An Acceptable Usage policy for mobile devices exist and includes rules for appropriate physical and logical handling, addresses mobile device use and specifies the type of information and services that may be accessible through the devices.
				12.2	Employees are required to sign a statement that they have read, understood and will comply with the Acceptable Usage policy for mobile devices including the rules for appropriate physical and logical handling.
				12.3	An awareness program is in place that addresses the importance of physically and logically securing the mobile devices. The training includes the types of information that can and cannot be stored on mobile devices.
				12.4	Employees are trained on a regular basis to be aware of the potential mobile security risks to enable them to recognize and properly respond to these risks in accordance with the IT security policy.
	Controls provide reasonable amount of assurance that mobile devices and security incidents are appropriately managed by employees	13	Device is lost or stolen leading to data stored on the device being disclosed	13.1	All employees are informed how to report on lost or stolen devices by means of a process description which is accessible to everyone in the organization (e.g. via Intranet).
				13.2	Mobile device (security) incidents are handled through established regular incident management processes in the organization and monitored on a regular basis.
				13.3	An asset management procedure is in place for registering mobile devices including the attributes that should be captured (e.g. basic software aspects, installed business applications, corporate data access) and is in line with the information classification policy.
				13.4	A Configuration Management Database (CMDB) is used within the organization for registering mobile devices and is updated periodically. This CMDB is part of the asset management procedure and a CMDB owner has been appointed to manage all assets.

RELEVANCE OF IMPLEMENTING A MOBILE SECURITY RISK/CONTROL FRAMEWORK

In today's world full of IT business transformations, it is important to implement controls for securing corporate data on mobile devices. Mobile business applications will continue to gather momentum in the coming years – despite the fact that the technical security level achieved will remain a concern. The risk/control framework as developed can be used in practice as a reference framework. As the mobile environment is rapidly evolving, there is a need to continuously test the security level and control the risks identified. Although there is an abundance of literature detailing specific technical security measures to be configured or implemented, these measures are usually not incorporated in (existing) risk/control frameworks. This framework is keeping abreast of new technology trends.

The aim of this article is to trigger organizations to think about these controls and how they can adjust this framework to make it applicable to their IT (mobile) environment and to incorporate these controls in their existing control framework that are most likely focused on regular ERP systems or IT General Controls. Since businesses and IT information chains have grown more sophisticated and complex, mobile applications become more prevalent at numerous large organizations.

LOOKING FORWARD

As the Dutch National Cyber Security Centre ([NCSC18]) states in their mobile applications research; organizations are using these applications more and more in their daily business activities. The differences between the backend of mobile phones, tablets, laptops and desktops are diminishing, however. In the near future, the IT auditor needs to focus on end-to-end device and mobile security, which is not yet fully integrated in risk/control or audit frameworks or taught at post-master IT auditing studies.

CONCLUSION

This article is aimed at showing the need for and providing a risk/control framework. The risk/control framework we developed and validated can be used by organizations to continuously test and update technical measures in and around mobile business applications. This will safeguard their organization and its sensitive data. There is a number of significant controls an organization should have in place in order to securely use mobile business applications. This article demonstrates that several mobile application areas need to be addressed using security controls. These areas are secure development, technical setup, authentication & authorizations, cryptography, sessions handling, using MDM, data security, corporate network connectivity, user awareness and device / asset management. We do emphasize that how organizations control their mobile environment is also dependent on several factors. It is critical to perform an extensive risk assessment that addresses the business as well as technical aspects to identify the IT maturity of the organization, risk appetite and how the mobile infrastructure has been designed and configured. The risk/control framework can be adjusted according to this assessment, by verifying the controls that are applicable to the organization.

References

[Enis17] Enisa (2017). *Privacy and data protection in mobile applications.* Retrieved on June 22, 2018, from: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications

[Ham17] Ham, D. van, Iterson, P. van & Galen, R. van (2017). *Mobile Landscape Security, Addressing security and privacy challenges in your mobile landscape.* KPMG.

[ISAC10] ISACA (2010). *Securing Mobile Devices.*

[Line07] Lineberry, S. (2007). The Human Element: The Weakest Link in Information Security. *Journal of Accountancy*, *24*(5), 44-46, 49.

[NCSC18] National Cyber Security Center (NCSC-NL) (2018). *IT Security Guidelines for Mobile Apps.* Den Haag.

[OWAS17] OWASP (2017). OWASP Top Ten. Retrieved on June 2018, from: https://owasp.org/www-project-top-ten/

About the authors

Jolien Démoed MSc is Senior Consultant at KPMG Advisory. Jolien is part of the GRC team as part of KPMG's Enterprise Solutions division. As an IT Auditor and Consultant, Jolien provides Advisory and Assurance services to national and multinational companies related to IT Auditing, (SOX) ERP implementations, implementing risk/control framework, risk assessments, IT security, implementation of authorization concepts.

Karima Siamari MSc is Senior Consultant at KPMG Advisory. Karima works in the GRC team part of KPMG's Enterprise Solutions division. As an IT Auditor and Consultant, Karima provides Advisory and Assurance services to national and multinational companies related to IT Auditing, SOX/ICoFR, ERP implementations, business process/risk analysis, design and implementation of risk/control framework, Segregation of Duties (SoD) monitoring, GRC tooling, continuous control monitoring.