



cutting through complexity™

First regional survey on information security in Kazakhstan and Kyrgyzstan

February 2012



KPMG Tax and Advisory LLC
180, Dostyk Avenue
Almaty, Kazakhstan, 050051

Ph: +7 (727) 298 08 98
Fax: + 7 (727) 298 07 08
E-mail company@kpmg.kz

Dear Ladies and Gentlemen,

We are pleased for taking an opportunity to present you our first regional information security survey in Kazakhstan and Kyrgyzstan.

This survey purpose is identify the common issues, threats, risks and trends in the information security area and assess of impact thereof on the entities' operations in Kazakhstan and Kyrgystan. Based on the survey results each participant shall be able to compare its own estimates with the average estimates of the respondents regarding the industry and region.

We believe that the survey will help identify areas for development and improvement of information security in your organization.

All questions in the survey are generic, and usually not require you to disclose any confidential information.

If you have any questions or comments related to information provided, please do not hesitate to contact coordinator in Kazakhstan: Vladimir Remyga by phone +7(727) 2980898 ext. 62 500 or e-mail VRemyga@kpmg.kz.

Respectfully yours,

David Alun Bowen

Managing Partner in Kazakhstan and Central Asia
KPMG Tax and Advisory LLC

Survey

General questions about the organization

Name of organization

Industry

Does your organization have the Department of Information Security?

How many people are in this Department?

Part 1. Information Security Management

1. Who in your organization responsible for security issues? (Choose one)

CEO

CIO

CISO

Compliance Director

CSO

CTO

Information Security Specialist

Information Technology Specialist

Internal audit Director

Personal data protection director

Risk Management Director

System Administrator

Other:

2. Who is accountable to that person in your organization? (Choose one)

The Board of Directors

CEO

CIO

CTO

Risk Management Director

Other:

3. Which of the following areas are included in the area of responsibility of information security department in your organization? (Select all applicable answers)

Application/system development

Asset Management

Business continuity/remedial recovery

Fraud management

IT Compliance (for example, Bazel II, SOX, HIPAA, PCI DSS, FISMA, etc.)

IT Risk Management

Office-work

Personal data protection

Physical security

Projects and programs implementation

Protection of intellectual property/commercial secrets

Supplier Relationship Risk Management

4. Which of the following activities in the area of information security are submitted to the subcontract, or the possibility of submit is considered? (Select all applicable answers)

Submitted to a subcontract in the present	Under evaluation / Plan to submit to the subcontract	Plan to submit to sub-contract is absent.
---	--	--

- Information security audit/assessment
- Penetration testing performance
- Firewall and other security tools administration (for example: IDS, IPS)
- Application testing
- Help Desk (Access Administration)
- Vulnerability/update management
- IT Security trainings and awareness raising
- Business continuity/remedial recovery management
- Incident investigation/counter measures for illegitimate actions
- IT Security Incident management

5. Choose three main security priorities for the next 12 months from the list below. (Please mark the most important answer with the number "1", the second most important – the number "2", and the third most important – the number "3")

Three priorities

- Implementation or improvement of technologies and processes to prevent data leakage
- Implementation or improvement of technologies and processes of access administration
- Implementation of virtualization technologies
- Implementation of other technologies (please list):

- Compliance
- Create and performed internal security-awareness training
- Implementing or improvement of internal software development processes (for example, the process of secure coding, quality control process)
- Implementing of standards (example, ISO/IEC 27002:2005)
- Implementing of mechanism for incident investigation/counter measures for illegitimate actions
- Improving of information security risk management system (including monitoring of compliance with regulatory requirements)
- Staffing (for example, from internal staff)
- Risk management
- Testing the information security function (such as penetration testing)
- Transfer information security functions to outsource

6. Check the statements which describes the annual investment in information security in your organization in the best way. (Choose one answer)

- Increase of share in total expenditure of the organization
- Decrease of share in total expenditure of the organization
- Relatively constant of share in total expenditure of the organization

7. Choose the statement which describes current situation in your organization for each of the following prospects of information security development.

Increase expense Decrease expense No changes

Implementation or improvement of technologies and processes to prevent data leakage

Implementation or improvement of technologies and processes of access administration

Implementation of virtualization technologies

Implementation of other technologies (please list):

Compliance

Create and performed internal security-awareness training

Implementing or improvement of internal software development processes (for example, the process of secure coding, quality control process)

Implementing of standards (example, ISO/IEC 27002:2005)

Implementing of mechanism for incident investigation/counter measures for illegitimate actions

Implementing or improvement of internal software development processes (for example, the process of secure coding, quality control process)

Staffing (for example, from internal staff)

Risk management

Testing the information security function (such as penetration testing)

Transfer information security functions to outsource

8. Does your organization have documented information security strategy for the next 1-3 years?

Yes – please, refer to question 9.

No – please, refer to question 10.

9. Please select all answers, applicable to your information security strategy:

Information security strategy includes security plan for the next 12 months

It has been reviewed and updated for the last 12 month

It is designed in accordance with the IT strategy of your organization

It is designed in accordance with the overall business strategy of your organization

10. Does your organization have approved information security policy?

Yes – follow to question 11.

No – follow to question 12.

11. Please select all response options, applicable to your information security policy:

It has been reviewed and updated for the last 12 month

It was formally approved by senior management

Policy communicated to all relevant staff (including staff, contractors, temporary employees and third parties)

The policy contains a definition of the organizational structure of information security

The policy covers the legal aspects of security

The policy regulates the role and duties of employees

12. Which of the following parts are covered by information security policy or several normative documents in the IS area? (Select all applicable answers)

- Data/information classification
- Data/information storage/destruction
- Data privacy/protection of personal data
- Passwords requirements
- Rules for clean desk/desktop
- Using mobile and portable devices (tablet, Smartphone, flash-drive and etc.)
- Using of Internet and e-mail

13. Evaluate the following factors affecting on implementation of information security initiatives in your organization (rating scale from 1 to 5, where 1 - "not difficult", 5 - "significant difficulty")

Not difficult		Significant difficulty		
1	2	3	4	5
				Availability of resources
				Appropriate budget
				Changes or lack of clarity in regulations and legislation
				Knowledge of new technologies
				Identification / assessment of new threats and vulnerabilities
				Improving staff awareness
				Organizational changes (eg, as a result of mergers and acquisitions)
				Support from management
				The uncertainty in the business (for example, due to market conditions)

14. How does your organization evaluate the quality and effectiveness of information security? (Select all applicable answer)

- Assessment by internal audit department
- Assessment is not conducted
- Assessment of the external audit of financial statements
- Assessment of an independent contractor
- Comparison with similar/competing organizations
- Official certification in accordance with industry standards, (eg., Payment Card Industry Data Security Standard – PCI DSS)
- Official certification in accordance with international standards (eg., ISO/IEC 27001:2005)
- Self-assessment by staff of IT or IS department

15. Is the information security management system (ISMS) implemented in your organization? (Choose one)

- Yes, implemented and officially certified (for ex., ISO/IEC 27001:2005)
- Yes, implemented, but the certification task is not set
- Yes, in the implementation process
- No, but this possibility is considered
- No, and this possibility is not considered

16. Which of the following standards/best practices for information security management is used in your organization? (Check the main standards/best practices with the number "1", and any others used in conjunction with them - the number "2")

- Capability Maturity Model Integration (CMMI)
- CobiT
- COSO
- Generally Accepted Privacy Principles
- Information Security Forum's (ISF) Standard of Good Practice
- Information Technology Infrastructure Library (ITIL)
- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- PCI DSS
- Webtrust
- Another industry standard:
- Other:

17. Has the amount of the following types of penetration testing, performed in your organization, changed for the last 12 months?

The amount of testing has	The amount of testing has	The amount of testing has not	Testing is not performed
---------------------------	---------------------------	-------------------------------	--------------------------

- Performing the analysis of the source code
- Testing of possibility of external attacks from the Internet
- Security testing of the internal IT infrastructure (operation systems, databases, networks)
- Security testing of the wireless networks
- Security testing of the remote access (modem pools, VPN)
- Security testing of organization's employees using social engineering methods
- Testing the physical penetration in the protected perimeters and buildings
- Security testing of VoIP service
- Other:

18. How often do IS Department employees hold meetings with the key individual or groups to discuss needs/activities in the area of information security?

Monthly	Quarterly	Twice a year	Annually	Never
---------	-----------	--------------	----------	-------

- Board of Directors
- Top Management (eg., CEO, CFO)
- The Audit Committee
- Head of operating units
- IT Department
- Internal Audit Department
- Legislation compliance Department
- Legal Department / General Counsel
- Risk management Department
- Human Resources Department
- Responsible for protection of personal data
- Operation and maintenance of building Department
- Other:

Part 2. Technical measures for Information Security

19. What measures does your organization take to increase the efficiency of information security management? (Select all applicable answers)

- Implementation of additional security tools
- Implementation of automated access control and account management
- Implementation of continuous monitoring of controls
- Implementation of the balanced indicators system (BSC or KPI)
- Outsourcing of selected activities in the area of security
- Standardization based on a unified system of control procedures

20. Which of the following measures of access and user accounts administration are implemented or planned to be implemented in your organization? (Select all applicable answers)

Implemented at the moment	Planned during the year	Implementation isn't planned
---------------------------	-------------------------	------------------------------

- Access management to Web application
- Automation procedures for access (request, approval, providing)
- Centralized logging and monitoring
- Centralized storage accounts
- Enterprise single sign-on
- Entitlement management
- Federated access to data
- Multifactor authentication
- Network access control/networks using the user account
- Password management
- Public Key Infrastructure – PKI
- Secure password storage/management of privileged access
- User accounts management
- User roles management

21. Which of the following measures are implemented in your organization to control the leakage of confidential information? (Select all applicable answers)

- Access to confidential data limited by time
- Additional security mechanisms to protect information (eg. encryption)
- Audit tools
- Developed special policy of classification information and how to work with her
- Identified special requirements for sending/remote access to confidential data
- Limited/restricted using of instant messaging or e-mail for transferring confidential systems
- Blocking/limitation use of certain hardware components(USB/FireWire ports)
- Restricted using devices with build-in camera in restricted area
- Tools for analysis of event logs
- Tools of content monitoring and filtration

22. Has the inventory and classification of information resources been carried out in your organization? (Choose one answer)

- Yes, for all critical resources
- Yes, for some critical resources, work is in progress
- No

23. How do you check whether your partner, suppliers or contractors provide necessary level of security for your information? (Select all applicable answers)

Analysis of assessments and other certifications results held by partners, suppliers or contractors (e.g. ISO/IEC 27001, BS 25999)

Analysis of the results of independent assessments performed by partners, suppliers or contractors, conducted by external organization (e.g. SAS 70, ISAE 3402)

Assessment by information security department or internal audit department (eg. site visits, testing security systems)

Analysis or assessment is not performed

Other:

24. Which or the following statements regarding the protection of the personal data could your organization make? (Select all applicable answers)

We have clear understanding of the laws and regulations to protect personal data, which may have an impact on your organization

We conducted an inventory of information assets which are regulated by requirements of the personal data protection

We evaluated the life cycle of personal data (collection, use, storage, transfer and disposal)

We introduced a special control procedures for protection of personal data

We implemented a process to monitor and maintenance of control procedures related to the protection of personal data

We implemented response procedures and incident management related to the protection of personal data

We included requirements for the protection of personal data into contracts with independent partners, suppliers and contractors

25. Are specific requirements for information security included into the contracts signed by your organization with partners, suppliers or contractors? (Choose one)

Yes, all agreements include specific requirements for information security

Yes, some agreements include specific requirements for information security

No agreements include specific requirements for information security

26. Which of the following items are included into the program of business continuity in your organization? (Choose all applicable answer)

Agreed credentials and responsibilities of all team members to recover in case of incident or crisis situation

Established relationships with local emergency services (fire, police, ambulance)

Identification and assessment of major threats and risks affecting the business continuity

Plans of awareness program and training for staff on business continuity

Prioritizing the restoration of critical business process

Procedures for incident management or crisis situation (including the order of escalating the crisis, and internal and external communication)

Procedures for recovery of business processes

Recovery plan after the failure of IT infrastructure (DRP)

Strategy of business continuity, aimed at restoring the IT and telecommunications, related infrastructure and mission-critical business processes in an emergency situation

Testing plan for business continuity management system, including a review of the exercises and tests

27. How does your organization evaluate the program to ensure business continuity? (Select all applicable answers)

- Carrying out a simulation test recovery of business units after failures
- Carrying out a simulation test recovery of the IT infrastructure after failures
- Complete simulation testing lack of continuity in the organization (simulation of emergency)
- Complete simulation testing of IT recovery from failures
- Modeling of Crisis Management (for manager of operation units and senior management)
- Parallel testing (conducted on reserve areas)
- Testing of complete breach of the organization activity and IT infrastructure functioning (testing the actual failure rate)
- Testing using the checklists
- Assessment is not conducted

28. How is interaction of your organization with the key counterparts organized in the context of business continuity? (Select all applicable answers)

- Distribution of the questionnaire with questions to ensure the continuity of activities
- Request for copies of the testing of business continuity plans reports
- Executing the audit program to ensure continuity of operations
- The nomination of the requirements to the counterparty about the passing of the official certification in the field of business continuity (eg. BS25999)
- No action taken. No requests to the business continuity counterparty are not sent

29. What issues are considered in the program to improve information security awareness approved in your organization? (Choose all applicable answers)

- Distribution of information bulletins on new relevant topics
- Distribution of visual and regular news/alerts about current threats of your organization
- Evaluating the effectiveness of activities to improve awareness and existing program based on the result of this assessment
- Executing special events or training in the information security for users in high-risk groups
- Raising information security awareness in general
- Verification, approval and compliance with the current policies and standards in the area of security
- Other:

30. Which of the following technologies does your organization use or plan to use? (Select all applicable answers)

Is used in the present time	Is planned to use during the year	The evaluation process
-----------------------------	-----------------------------------	------------------------

- Access and user accounts management systems
- Cloud computing
- Combination of physical and logical security (e.g., association of parameters of physical and logical access)
- Distributed computing
- E-mail encryption
- Encryption of data on the hard drives of desktop computers
- Encryption of data on the hard drives of laptops
- Encryption of removable media
- Multifactor authentication (802.1x, tokens)
- Radio Frequency Identifiers (RFID)
- Server virtualization
- Software tools of corporate governance, risk management and compliance

The growth of fraudulent activities within the company
 Changes are not assumed

34. How much your organization is concerned about the possibility of malicious actions from employees who have left the organization in the recent time? (Choose one)

- Very concerned and take measures to minimize risks
- Very concerned, but we have not evaluated the potential risks
- Have some concerns and try to get an idea of the potential risks
- Not concerned
- Not applicable

35. What measures has your organization taken to minimize potential risks arising as a result of staff reduction? (Select all applicable answers)

- Develop a program to keep knowledge, ensuring keeping of knowledge in case of dismissal of key staff
- Evaluation and improvement of access and user accounts administration
- Evaluation and improvement of monitoring of changes in information systems
- Implementation of programs to prevent data leak
- Measures haven't been taken
- Not applicable
- Other:

36. What effect does regulatory compliance have on the value of annual costs of information security in your organization?

For the previous 3 years	For the current year
--------------------------------	-------------------------

- A significant increase in the costs of providing of information security
- A moderate increase in the costs
- The cost is not changed
- Costs decreased

37. What effect does regulatory compliance have on the effectiveness of information security in your organization?

For the previous 3 years	For the current year
--------------------------------	-------------------------

- Significant increase of the effectiveness of information security as a result of compliance with regulatory requirements
- A moderate increase in the efficiency
- Without changes
- The effectiveness of information security decreased as a result of compliance with regulatory requirements

Contact us

Alun Bowen

Managing Partner

T +7 727 2980898

E ABowen@kpmg.kz

Vladimir Remyga

Senior Manager

T +7 727 2980898

E VRemyga@kpmg.kz

Aleksey Kan

Senior Consultant

T +996 312 623380

E AKan@kpmg.kg

www.kpmg.kz

www.kpmg.kg

© 2012 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan, a subsidiary of KPMG Europe LLP, and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name, logo and 'cutting through complexity' are registered trademarks or trademarks of KPMG International.

