



Development of Information Security Policies and related standards

Real Estate Cadaster Committee of Armenia

—

August 2019

KPMG Armenia LLC

8th floor, Erebuni Plaza Business Center,
26/1 Vazgen Sargsyan Street
Yerevan 0010, Armenia

Tel + 374 (10) 59 59 99

www.kpmg.am

Private and confidential

August 21, 2019

Real Estate Cadaster Committee of Armenia

Dear colleagues!

We are pleased to announce our proposal for development of Information Security Policies and related standards for Real Estate Cadaster Committee of Armenia (hereinafter referred to as the 'Committee').

Taking into account the needs and expectations of the Committee, in this proposal we present our approach to the project implementation and cost of our services. In addition, the proposal includes a description of the project scope, based on our understanding of the requirements of the Committee and our experience on similar projects.

We would like to emphasize that our estimate of the cost of services depends not only on the alleged time-consuming, but also on the scope, complexity and quality of information to analyze.

We look forward to working with the Committee and we believe that KPMG has all the necessary knowledge and experience to perform the proposed work as efficiently as possible.

Should you need clarification on any of the points raised in this proposal, please contact:

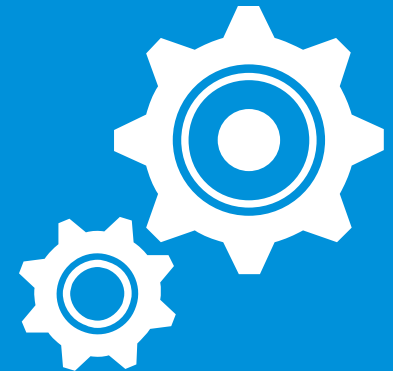
- Tigran Torosyan(phone : +374 (99) 051020, e-mail: ttorosyan@kpmg.com).

Yours sincerely,

Zaruhi Furunjyan
Head of Advisory



KPMG approach



KPMG approach

We propose the following stages of the project:

01

Conduct diagnostic audit to measure the compliance of the Information Security Management System (ISMS) of the Committee with the requirements of ISO/IEC 27001:2013 (Gap Analysis)

02

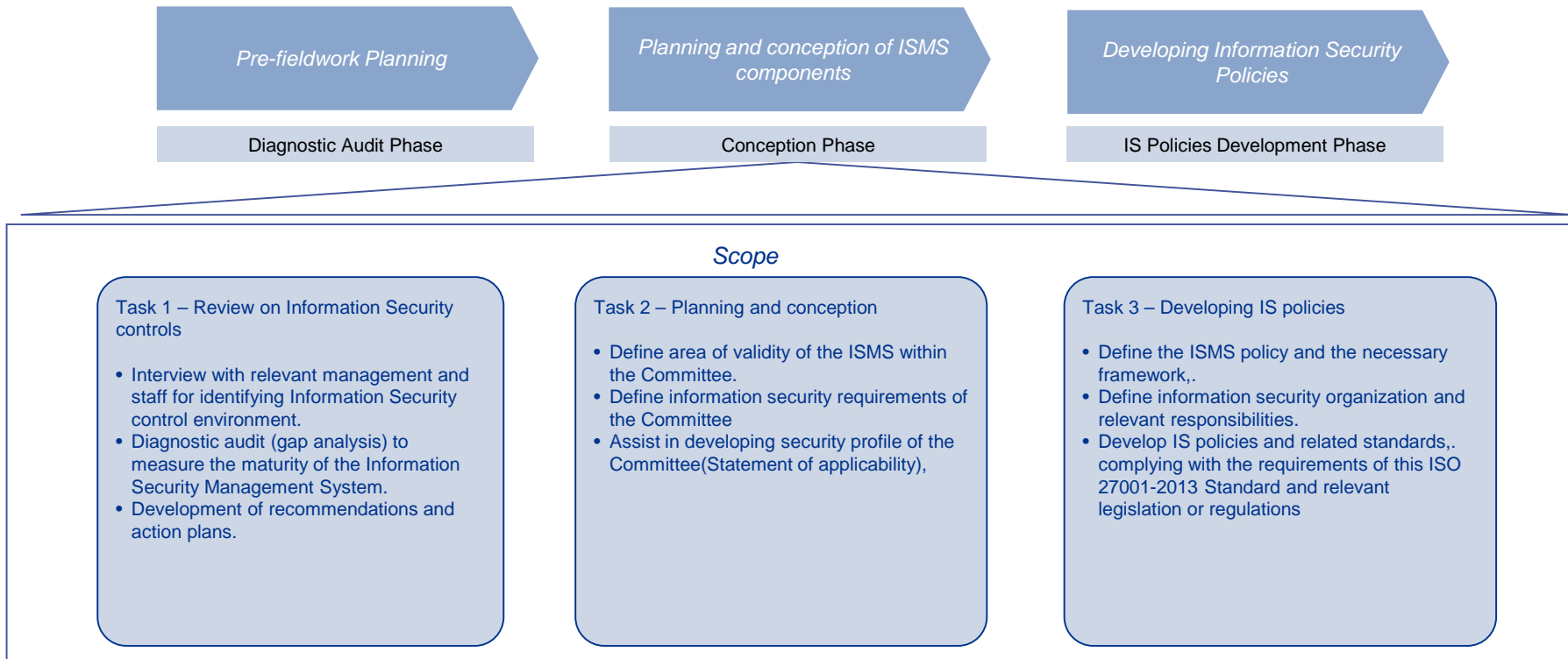
Assist in planning and defining conception of ISMS components of ISO/IEC 27001:2013 according to chapters 4 to 8 of the standard (ISMS - Conception phase).

03

Assist in developing Information Security Policies and related Standards, various records required by ISMS documentation according to ISO/IEC 27001:2013 Standard

Detailed approach

We will perform our work in accordance with the KPMG methodology following the three key phases of Diagnostic Audit, Planning and Conception and developing IS policies. We will perform our work in these phases, to increase efficiency and reduce the impact on the processes. The aim of this section is to provide you with more details of our tailored approach in the Analysis phase.



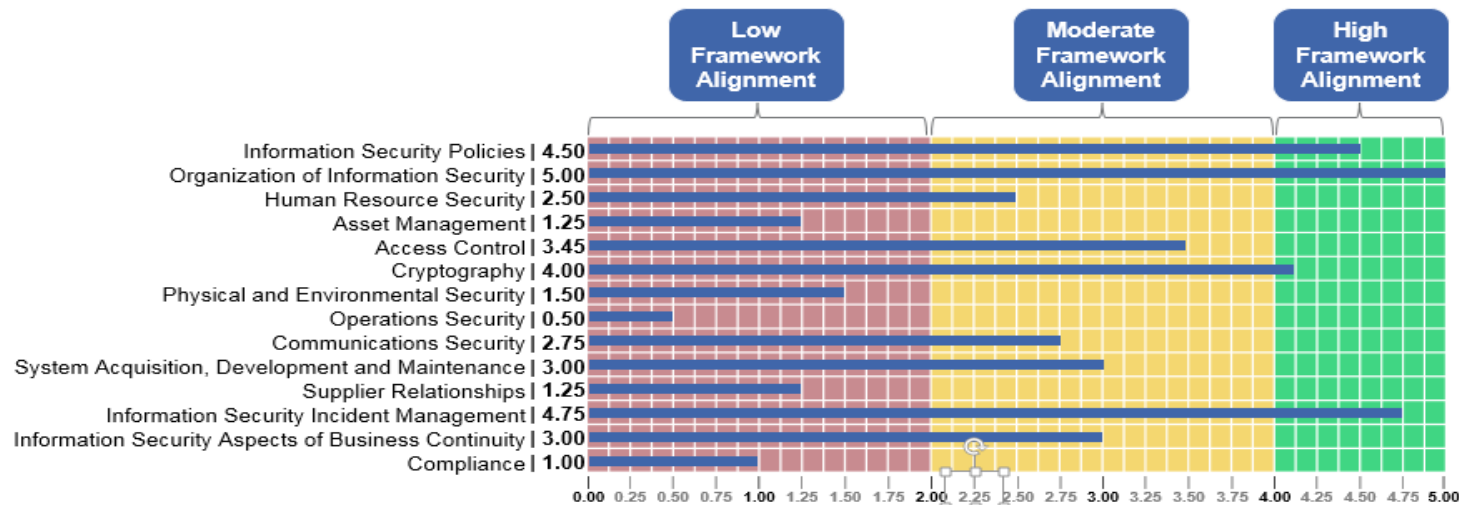
Task 1 – Diagnostic Audit Phase

Diagnostic audit (gap analysis) to measure the maturity of the Information Security Management System of the Committee:

Works:

Based on the agreed ISMS Scope Statement, a combination of documentation review, workshops and interviews will take place in the Gap Analysis phase.

KPMG will analyze the maturity of information security controls and processes of the Company and identify deviations from the ISO/IEC 27001:2013 standards. The Committee will identify and assign employees who will coordinate the elimination of issues within the processes identified by KPMG. The adjustment of weaknesses will be done by employees of the Committee. KPMG will accompany the removal of weaknesses by giving recommendations for improvement (based on the leading practice).



Results and deliverables:

Gaps identified and recommendations on the ways to close the gaps to achieve compliance with ISO/IEC 27001:2013 requirements. In particular gaps within the process descriptions will be highlighted

Task 2- Planning and Conception of ISMS components

Define information security requirements of the Committee and develop security profile of the Committee.

Works:

In the Conception phase the area of validity of the ISMS within the organization will be defined. The scope and conception will be set up by assessing information about the security requirements of the Committee and its 'Customers' as well as legal requirements and documents necessary for achieving ISO27001 certification. At least following domains are taken into account for ISMS:

- Scope of the ISMS
- Information security policy and objectives
- Risk assessment and risk treatment methodology
- Statement of Applicability
- Risk treatment plan
- Risk assessment report
- Definition of security roles and responsibilities
- Inventory of assets
- Acceptable use of assets
- Access control policy
- Operating procedures for IT management
- Secure system engineering principles
- Supplier security policy
- Incident management procedure
- Business continuity procedures
- Legal, regulatory, and contractual requirements

Non-security relevant areas will be excluded. Taking this scope as a basis it can be determined if Operation's specific security requirements have to be assessed separately as they necessitate a modification of the management system. The information will be obtained through interviews with the Committee management.

Results and deliverables:

Security profile of the Committee(Statement of applicability),

Task 3- Developing Information Security Policies

Support the Committee to develop Information Security Policies and related standards

Works:

Based on the results of the Gap Analysis phase and Planning and Conception phase we will assist the Committee to develop IS policies and related standards in accordance with ISO 27001-2013 Standard, including following topics:

Assist in defining the ISMS policy and the necessary framework,

Assist in defining information security organization and relevant responsibilities,

Assist in developing Information Security policies and related standards, at least covering topics:

- Scope of the ISMS
- Information security policy and objectives
- Risk assessment and risk treatment methodology
- Statement of Applicability
- Risk treatment plan
- Risk assessment report
- Definition of security roles and responsibilities
- Inventory of assets
- Acceptable use of assets
- Access control policy
- Operating procedures for IT management
- Secure system engineering principles
- Supplier security policy
- Incident management procedure
- Business continuity procedures
- Legal, regulatory, and contractual requirements

Results and deliverables:

IS policies and related standards, complying with the requirements of this ISO 27001-2013 Standard and relevant legislation or regulations



Fee & Timeline



Fee arrangement



Commercial terms and conditions

Scope of work	Time	Fee excl. VAT, AMD
Stage 1. Diagnostic Audit	8 days	1,600,000
Stage 2. Palming and conception	8 days	1,600,000
Stage 3. Developing IS policies	12 days	2,800,000
Total	30-50days	6,000,000

Our fees are based on the time spent and the experience and skills required to perform the work. The hourly rates of our professionals vary according to the respective degree of responsibility and level of experience

The fees stated above do not include VAT and reasonable out-of-pocket expenses. Out-of-pocket expenses, if any, will be calculated based on the expenses actually incurred related to the visits of KPMG employees, and will be reimbursed separately

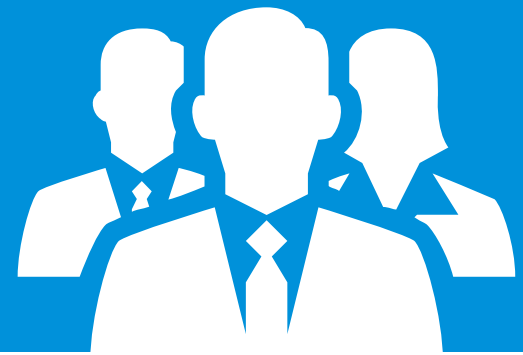
If you are interested we can provide a separate proposal for additional services not covered by this document

Approximate project duration – up to 50 working days

This proposal is valid for a period of two month and its conditions are dependent on the successful completion of our risk management procedures, including client and engagement acceptance, as well as conflict of interest checks. Its conditions are also subject to the negotiation and signing of an agreement containing standard KPMG conditions for the services rendered. The quality of the information provided can lead to changes in the fee for the Services



KPMG team



KPMG Engagement Team



Ilya Shalnikov

Director, Information
Protection and
Cybersecurity, KPMG
in Russia & CIS



Ilya is an expert in the field of information security, IT controls and IT audit. Ilya leads the Information Protection and Cybersecurity service line in KPMG in Russia.



Engineer, Automated Information Processing and Control Systems, Moscow State Technical University named after N. E. Bauman

Economist-Manager, Economics and Management at the Enterprise, Moscow State Technical University named after N. E. Bauman



CISA – Certified information systems auditor / Information Systems Audit and Control Association (ISACA).

CRISC – Certified in Risk and Information Systems Control / Information Systems Audit and Control Association (ISACA).

BS ISO/IEC 27001:2013 Lead Auditor – Lead auditor of Information Security Management Systems / The British Standards Institution.

> 10 years

Ilya has been working in the field of IT, IT auditing and information security, and more than 6 years – in the Moscow office of KPMG.



Sector experience: Information, Communication, & Media, Transport, Consumer Markets , Financial Services, Industrial Markets

KPMG Engagement Team



Andrey
Drozdov

Senior Manager,
Information Risk
Management Group,
KPMG in Russia & CIS



Andrey is a recognized international expert in the field of information technology and information security. He is vice president of the Moscow branch of the Association of Information Systems Auditors (ISACA). Participates in the preparation of regulatory documents of the Central Bank of the Russian Federation in the field of information security for the financial sector. Engaged in teaching.



Moscow State University named after M.V. Lomonosov, qualification "Mathematician" in the specialty "Applied Mathematics".



CISA – Certified information systems auditor / Information Systems Audit and Control Association (ISACA).

CISM – Certified Information Security Manager / Information Systems Audit and Control Association (ISACA).

CGEIT – Certified in the Governance of Enterprise IT / Information Systems Audit and Control Association (ISACA).

BS ISO/IEC 27001:2013 Lead Auditor – Lead auditor of Information Security Management Systems / The British Standards Institution.

Auditor 'СТО БР ИББС 1.0' (Central Bank of the Russian Federation)

Cobit 5 Foundation (ISACA/APMG)

> 30 years

Andrey has been working in the field of IT, IT auditing and information security, and more than 20 years – in the Moscow office of KPMG.

KPMG Engagement Team



Mark Gordeev

Senior Manager
Information Protection
and Cybersecurity,
KPMG in Russia & CIS



Mark is an expert in the field of information security, IT controls and IT audit. Ilya leads the Information Protection and Cybersecurity service line in KPMG in Russia. Mark's competencies include auditing of information security in compliance with international and corporate standards, and development of internal information security policies.



Moscow State Technical University named after N. E. Bauman, qualification "Information Security Specialist", specialty "Integrated information security of automated systems."



CISA – Certified information systems auditor / Information Systems Audit and Control Association (ISACA).

BS ISO/IEC 27001:2013 Lead Auditor – Lead auditor of Information Security Management Systems / The British Standards Institution.

> 9 years

Ilya has been working in the field of IT, IT auditing and information security, and more than 6 years – in the Moscow office of KPMG.



Sector experience: Information, Communication, & Media, Transport, Consumer Markets , Financial Services, Industrial Markets

KPMG Engagement Team



Artem
Kobets

Senior Consultant,
Information Protection
and Cybersecurity,
KPMG in Russia & CIS



Artem is a specialist in the area of practical information security vulnerability assessment and penetration testing. He is experienced in web-based application and network infrastructure penetration testing, has solid understanding of attack scenarios and common vulnerabilities. Artem is familiar with OSINT, OWASP, PTES, CEH methodologies and has extensive technical knowledge of both Unix and Windows platforms and related infrastructure



National Aviation University (Kiev, Ukraine), Information security in networks and computer systems, Specialist's degree.



Core skills includes:

- Penetration testing skills: OSINT (utilizing tools like Maltego, Recon-ng etc.); Vulnerabilities assessment (nmap, Nessus, Openvas); Exploiting (Metasploit); MITM, sniffing, packets inspection (Wireshark, ettercap, etherape); Web-based applications pentesting (Burp, ZAP, nikto, sqlmap, BeeF); Wireless network testing (aircrack-ng); Passwords cracking (hydra, john, l0phtcrack, medusa); Social engineering (SET).
- Understanding of networking and security technologies: TCP/IP, firewalls, VLAN, DMZ, proxy, NAT, IPS/IDS, patch management, backups, log analysis, VPN, antivirus software etc.
- Knowledge of programming languages: PHP, assembly language, shell/powershell, C/C++, SQL, JavaScript
- Unix family and Windows family systems administration and security: Access control (ACL), firewalls (ipfw, iptables), web servers (Apache, nginx), IPS/IDS (snort), integrity check (tripwire), patch management (portaudit), malware search (rkhunter), other network services and features (NTP, NAT, squid, syslog, NFS, MySQL, Bind, chroot, jail, hast, ZFS, Postfix); Active directory, group policies, WSUS, IIS, Terminal services, MS SQL Server.

KPMG Engagement Team



Tigran
Torosyan

Senior Consultant,
Information Risk
Management Group,
KPMG, Armenia



Tigran is an expert in the field of information security, IT/IS audits, information risk management and implementation of Information Security Management Systems.



– Applied Physics, Yerevan State University
Master degree



CISA – Certified information systems auditor / Information Systems Audit and Control Association (ISACA).

> 10 years

Tigran has been working in the field of IT, IT auditing and information security, and more than 5 years – in the Yerevan office of KPMG.



Sector experience: Financial Services(Bank, Insurance, Credit organization), Telecom, Retail, Utility Services.



Selected experience

Selected projects

Our experts have experience of successful projects in the field of the analysis of compliance with the requirements of ISO27001 and 27002, as well as in the field of the information protection and cybersecurity and the development of the required documentation. Relevant to the topic projects are:

Client	Brief description of provided services
Large international bank	Assessment of compliance of IT and IS processes with internal information security policies (based on ISO27002 requirements).
Large European pharmacology company	Risk analysis and risk assessment in IT governance. Development of recommendations for IS risk treatment.
Large Russian mining company	Information security function analysis including analysis of ISMS conformance with ISO/IEC 27001:2013 requirements
Large Russian mining company	Analysis of chosen ISMS controls for conformance with ISO/IEC 27001:2013 requirements.
Japan automotive concern factory in Russia	IT and IS risk assessment for consequent identification of key business-processes interruption risks.
Large bank	Assessment of web applications security, including Internet banking and partner's portal.
International oil and gas company	Penetration testing of the internal corporate network.



Why KPMG



Why KPMG?

Our advantages

We have the following advantages that distinguish us from other players in the market:



We have complex approach to information security issues, taking into consideration both organizational and technical aspects



We have world champions of "ethical hacking" in our team. They are the winners of various hacker competitions



Results of our work are clear not only to technical specialists, but to business leaders as well



We have been licensed by FSTEC (Federal Service for Technical and Export Control) to provide confidential information technical protection services



We have access to the global KPMG base of knowledge and have the opportunity to engage international experts



We have a comprehensive approach to the issues of information security and IT management function and are focused on both organizational and technical issues



KPMG International has been named a leader in information security consulting services in 2015 according to Forrester Research Inc.

Our certificates

Qualified professionals with international certificates are in our team:



CISA – Certified Information Systems Auditor / Information Systems Audit and Control Association (ISACA)

CISM – Certified Information Security Manager / Information Systems Audit and Control Association (ISACA)

ITIL Expert – Certification in IT Service Management / EXIN

OSCP – Offensive Security Certified Professional

CRISC – Certified Professional in Risk and Information Systems Control / Information Systems Audit and Control Association (ISACA)

CISSP – Certified Information Systems Security Professional / International Information Systems Security Certification Consortium (ISC2)

CGEIT -Certified in the Governance of Enterprise IT / Information Systems Audit and Control Association (ISACA)

BSI ISO/IEC 27001:2013 Lead Auditor – Lead Auditor of the information security management systems in conformance with ISO/IEC 27001:2013 (applicant) / British Standards Institute (BSI)

CEH – Certified Ethical Hacker / International Council of Electronic Commerce Consultants (EC-Council)

Cobit 5 Approved Trainer Foundation / Information Systems Audit and Control Association (ISACA)

Why KPMG?

About KPMG

KPMG is a “Big Four” firm, a global network of independent member firms providing Audit, Tax, and Advisory services.



We operate

in **154** countries and have

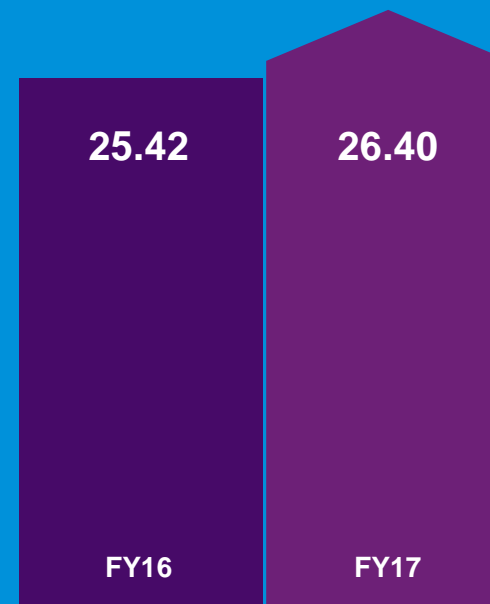


>200,000 people working in member firms around the world



Our purpose and aspiration is to turn knowledge into value for the benefit of our clients, our people, and the world’s capital markets.

Revenue KPMG International



US\$ in billions



Why KPMG?

KPMG in Russia and the CIS



* RAEX (Expert Rating Agency), Largest Audit Groups by Audit Revenue in 2009 – 2017



kpmg.am



kpmg.com/app

This proposal is in all respects subject to the negotiation, agreement, and signing of a specific engagement letter or contract. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

This proposal is subject to: 1 Completion of our normal client/ engagement acceptance procedures and checking for conflicts of interest; 2 Negotiation, agreement and signing of a specific engagement contract which incorporates our general terms of business.

Personal data contained in this proposal will be processed in accordance with the legislation of Armenia.

© 2019 KPMG Armenia LLC a company incorporated under the Laws of the Republic of Armenia, 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 KPMG name and logo are registered trademarks or trademarks of KPMG International.