Ahmed Tawfik & Co. CPA

MAZARS

Cyber Security Assessment and Penetration Testing Services

June 2016

WHY MAZARS?

Cyber security risks are dramatically increasing in the gulf region with international events planned to take place like Dubai Expo 2020 and Qatar 2022 World Cup, which expose Qatari organisations especially the financial ones to more cyber security threats, evident lately with number of high profile incidents. Mazars is responding to this risk with number of services including cyber security review and penetration testing. This document contains a detailed explanation of our experience, our methodology, approach, our team and Mazars' values of integrity and independence

We believe we are an excellent fit to provide cyber security review and penetration testing to Qatari companies for the following reasons:

Expertise

- We have been providing cyber security and IT security services as part of a number of consulting and internal audit (both outsourced and co-sourced) engagements to a significant number of financial, manufacturing and distribution companies.
- The team is composed of individuals carrying the most recognised information security certifications such as CISSP, GPEN, CEH, CISA, CISM, CRISC, ITIL, ISO 27001 lead auditor, CE, CE+ and IASME Gold assessors.

Leadership by a strong partner-led team

This is where we really excel. We genuinely provide a partner-led team with partners 'on the ground' giving you the best senior input and added value recommendations at a cost which is extremely competitive. This level of senior input is unique amongst firms who provide internal audit services, as demonstrated by your central point of contact.

Rigorous standard based approach

We employ various standards and framework such as ISO 27001, NIST 800 series and SANS/CPMI critical controls. In addition we would refer to ISACA (COBIT) and Prince 2 (project management) for specific matters. As members of the ISACA and certified cyber security assessors, these standards form a core part of our methodology. We understand how to apply these standards in practice rather than just in theory.

Meeting your requirements (client centric)

We are confident that Mazars develop cyber security solution that is customised to meet our clients requirements for a trusted and highly skilled cyber security review and penetration testing. This is demonstrated within this document.

Credibility

As a leading global audit and consulting firm, we are a credible partner to Qatari companies and a recognised and trusted audit brand internationally. We act as auditors/ advisors to over 15% of European companies and to over 400 companies listed on 20 different stock exchanges internationally.

Our partner-led team has the right combination of skills, experience and credibility required to satisfy your cyber security review needs. The team has built up a strong reputation in the marketplace for the delivery of cyber security services, built upon its breadth and depth of specialist knowledge and experience.

Independence and objectivity

Should Mazars be appointed to provide cyber security review services for Qatari companies, we do not anticipate any conflicts of interests which would compromise our ability to deliver our services with on-going independence and objectivity. None of our partners or staff members sit on the Boards of, or are employed by, any of the organisations we are engaged with and we act independently for each of our clients. We would manage any potential conflicts of interest in line with our standard practices, which are as follows:

- We have policies and procedures in place which are designed to ensure that we carry out our work with integrity, objectivity and independence, and that our clients' best interests are safeguarded.
- We respect our confidentiality agreements with our clients. We will not disclose any information we acquire which is confidential to Qatari companies or its clients. We will not disclose this information to third parties except where prior written consent has been obtained from the owner of the confidential information or where there is a legal right or duty to make disclosure.
- If, at any time, you have concerns or questions about our integrity, objectivity or independence, the engagement partner will discuss these with you.

OUR METHODOLOGY

Methodology

Mazars proposes several cyber security assessment options that cover a broad risk spectrum. These assessments and their coverage are presented here.

Mazars has a global methodology for performing cyber security reviews. Our methodology is a risk based approach focusing on clients' strategic objectives and the risks and uncertainties which may affect their ability to achieve them. Our approach is based on globally recognised standards, guidelines and framework such as ISO 27001, NIST 800 series and SANS/CPMI

Cyber Security Assessment

Our assessment offers a level of assurance around five areas:

1. **Firewalls and internet gateways:** Enumeration of external network, identification of running services and vulnerabilities and ensure firewall is secure.
2. **Secure configuration:** Assess internal host, identify running services and vulnerabilities.
3. **Access control:** Existence of generic accounts, end-users with privileged access, password protection
4. **Malware protection:** Malware injection through emails or from electronic media (USB sticks)
5. **Patch management:** Patch installation against baseline (vendor patch list).

Part of these tests will be run using internationally recognised tools such as Nessus scanner, nmap, MBSA, Burp Suite, OWASP WAP or Titania.

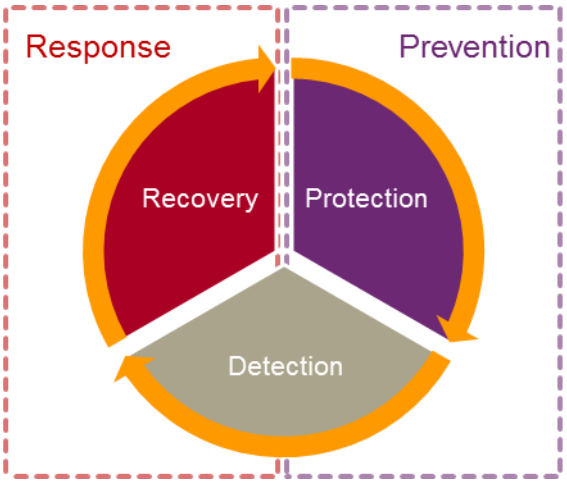
Advanced Cyber Security Assessment

Full assessment will complement the Cyber Security Assessment five domains with:

- Risk management
- Governance (Information Security)
- Training (security awareness)
- Policies & Procedures;
- Security Incident management
- Business continuity aspects

Cyber security control categories

There are three main categories of activities needed to respond to cyber threats.



There is a common set of factors to be considered when assessing the effectiveness of an organisation's business, which are summarised below. These are much the same as those for cyber security, which is most cost effective when considered to be part of the business.

Protection

- Organisation
- Assessing the risk
- Policy and compliance
- Assets
- People
- Physical and environmental protection
- Operations and management
- Access control

Detection

- Malware and technical intrusion
- Monitoring

Recovery

- Backup and restore
- Incident management
- Disaster recovery / business continuity

OUR APPROACH

Scope

Cyber security risks are dramatically increasing in the gulf region with international events planned to take place like Dubai Expo 2020 and World Cup in 2022, which expose Qatari organisations to more cyber security threats, evident lately with number of high profile incidents. Mazars is responding to this risk with Cyber Security review services including:

- The assessment of its cyber security posture as compared to global international standards and baseline
- A penetration testing of its public IP addresses and two websites/ web platforms.

Per each assessment levels, the scope of the review will include the components illustrated in the graphic below.

Approach

Our approach for proposed engagement will be as follows:

Planning

In the context of the proposed assignment:

- Mazars will, at commencement of the assignment conduct a planning meeting with the relevant stakeholders including IT contractors to gain a better understanding of the environment, review the self-assessment performed by the company, refine the scope and obtain relevant supporting information.
- Prepare a detailed work programme in advance of the commencement of the review on site
- Prepare the details of the penetration testing.
- Send out an information request to the nominated Business/ IT contact for the review following the preliminary meeting and in advance of the commencement of the fieldwork setting out the meetings required, the information (such as copies of policies etc.) that we will require in the course of the review, contact details etc.

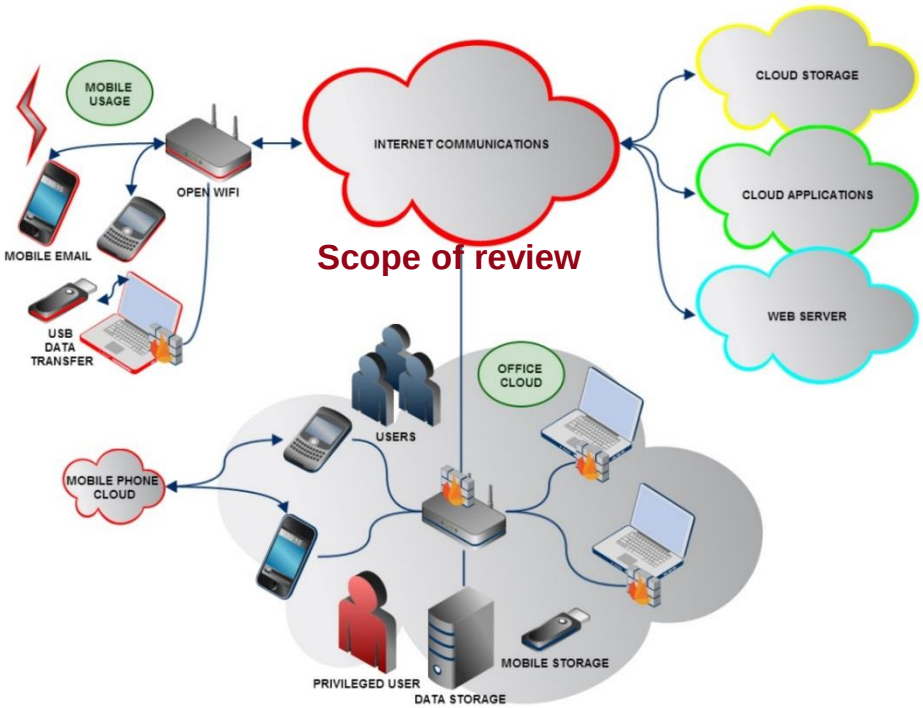
Fieldwork

The field work will be divided into two distinct streams:

1. Review of the current IT environment:

During this stream, our team that will be based on site in Doha for the duration of the fieldwork, and will work to a detailed work programme presented below:

- **Risk assessment** – i.e. the determination of the risks which exist in the areas covered in the scope of the review and required in the IASME standard.



- **Controls assessment -** existence of business/ IT operations controls in place. The team will examine what controls and practices exist and also whether these controls are adequate in nature to manage the risks of the organisation.
- **Substantive testing** – this phase of the fieldwork will involve the detailed testing of a number of aspects of the business/ IT operations controls in place to determine the extent to which they are operating effectively. The testing might include technical tests such as penetration testing and vulnerability assessment.

In practical terms, the team will review the existing documentation (policies and procedures, technical documentation), conduct interviews with the IT consultant and perform tests.

2. Penetration testing

Mazars' international security team based in UK, will perform an external ethical hacking/ penetration testing approach which will involve the exploitation of any vulnerabilities found. The test will focus on the public IP address provided by Qatari companies.

We acknowledge and agree it is important to ensure that a Denial of Service (DoS) type attack is excluded as these types of reviews can potentially interfere with and disrupt the live operation of other systems; as such, the approach which we have set out does not include such an attack and will not exploit any vulnerability detected.

Mazars' security team will attempt to penetrate from the internet, and will include the following activities:

- Foot printing
- Port scanning
- Enumeration
- Vulnerability scanning
- Penetration testing

Our testing will focus on passive and active testing; that is, during our testing:

- Vulnerabilities found will be exploited, a proof of the successful penetration will be provided.
- Use of active and passive testing will gather information only.

In addition, a detailed review of the routers and firewall configuration will be done in order to make sure configurations are achieving the highest protection for the company's environment.

* * *

At completion of our fieldwork, we will facilitate a meeting with management to ensure correct interpretation of findings and results (i.e. factual accuracy of our observations), and to give management an opportunity to comment on our findings prior to a report being drafted. This meeting will be conducted by members of the team.

Reporting

At the completion of the fieldwork of the review, results from our meeting will be collated, analysed and evaluated by the team and a draft report prepared.

At this stage and if applicable, document templates (e.g. policies, guidelines or procedures) can be provided to facilitate addressing the recommendations.

OUR TEAM - MEET THE EXPERTS

Hatem Elsafty, Partner, Governance, Risk and Internal with more than 15 years experience in IT security, information security governance, is the cyber security service in Qatar is managing the relationships with our clients. He is a Certified Information System Auditor (CISA) and Certified Internal Auditor (CIA)

Francisco Sanches, is a cyber security Senior Manager that has been working within information security and IT audit for over 14 years. He is a certified Information Security Professional (CISSP), a Certified Information Security Manager (CISM) and Certified Information System Auditor (CISA)

Whilst Hatem will be leading the team in Qatar, and available to Qatari companies as needed. Francisco will be leading the UK professional team of ethical hacking and penetration testing team.

We have the resources and capacity within our team to ensure that your needs and expectations are met.

The delivery of our services will be led by our IT security specialists based in Qatar while the technical penetration testing will be lead by our specialists in London, supplemented by local resources where possible and in order to keep costs down.

The team members are eager to undertake the work and to be proactively involved with your assignments. The team members included within this proposal will be those that actually provide the services – this is something that we believe makes us stand out from the competition.

As previously mentioned, we believe that the time invested by the senior members of the team is unparalleled. Our partners contribute to all stages of the process, including input into planning, scoping and opening meetings through to reporting and presentation to management.

Hatem Elsafty

Qatari Cyber Security Service Leader

Francisco Sanches

UK, IT audit and IT security Senior Manager

ABOUT MAZARS?

International, integrated, independent

Mazars is unique. We are an international, integrated and independent organisation specialising in audit, advisory, accounting and tax services, covering 77 countries and drawing on the expertise of 17,000 professionals to assist businesses, major international groups, SMEs, entrepreneurs and public bodies at every stage in their development.

Unlike our competitors, we are neither a network nor an association. We are a truly integrated, international partnership. We believe our structure, our client base and service delivery position us as a truly global firm. But what does that mean, in practice?

It means we operate as one united team, across national boundaries. We have one management structure which allows us to think, decide, and act collectively, sharing our knowledge and expertise. This fundamental principle has helped us to better serve our global clients, and think progressively, ahead of other firms who are only just beginning to move in this direction.

Ahmed Tawfik & Co. CPA

MAZARS

Please get in touch…

Should you require any further information,
please do not hesitate to contact:

Hatem Elsafty
Partner: Governance Risk & Internal Control Service Leader
T: +974 4444 1132
M: +974 6696 8065
E: hatem.elsafty@mazars.qa