Information Security Controls for Website Development and Hosting

Version: 1.0

Author: ictQATAR

Classification: Internal

Date of Issue: 18th August 2011

Contents

Overview:

A website is like any other information processing system. In order to ensure confidentiality, integrity and availability of the website it is of paramount importance that information security is part of the overall project / development cycle. It should be embedded in each stage of project management and software development cycle and not used as a cosmetic makeover.

Publishing a website for an agency includes the following major activities:

1. Website Development
2. Website Hosting

Each of the above activity may be done in-house by an agency or outsourced to a vendor.

This document focuses on identifying controls to be used in case the activities are outsourced to a vendor.

Controls:

An outsourced activity (in the scope of this document website development and / or website hosting) will be typically executed as a project in an agency. To simplify things we will use the project management strategy to identify the controls relevant at each stage.

Project Initiation

The following controls should be included:

1. The first step is to do a self-assessment to assess the criticality of website that is being developed or hosted by the agency and assessment of local laws and regulations. This will be a guiding factor in the later stages to objectively choose information security controls. Appendix A provides guidance on categorizing your website.
2. In case of multiple stakeholders, a consensus should be there amongst the stakeholders to implement and comply with the relevant information security controls. This may be included in the Project Initiation Document or a Memorandum of Understanding as may be applicable.
3. Ensure that the RFP / RFQ include information security compliance as part of the scope of work. Ensure that proposal evaluation takes into account the vendor's capability and willingness to comply with the necessary information security controls. An example of the proposed clauses that can be used in such documents is provided in Appendix B.
4. Ensure that vendors chosen for the project meet the vendor qualification requirements as prescribed in Appendix C.

Project Planning

1. The Final agreement signed with the vendor shall reinforce the vendor's obligation to comply and implement the necessary information security controls. An example of the proposed clause that can be used in such contract is provided in Appendix D.

Project Execution

1. Evaluate the proposed design, security controls and methodology. Ensure that the design integrates with the principles of information security. Information security should be considered in all aspects of software development life cycle.
2. The application and the information that the website will provide and process shall be classified using the Government Information Classification Policy.
3. Ensure compliance to GIA policies and any other policies / legislations as may be applicable.
4. Assess the effectiveness of security controls.
5. A detailed checklist of controls is available in Appendix E

Project Closure

1. The vendor shall provide a Compliance certificate attesting that he has complied with the necessary security controls as prescribed in the GIA Policies and the applicable policies / legislations, as mandated in the RFP and the final technical proposal of the vendor. In case of non-compliance the vendor shall state the reasons for the same, the associated risk and the stakeholder acceptance for the same.
2. The agency on its part shall ensure that GIA Policies compliance is part of the final acceptance test plan.
3. In case of websites categorized as level 3 and above it is strongly recommended to have the website audited by a third party prior to going live.
4. As a minimum this audit shall include compliance to the prescribed policies / legislations as described above and a vulnerability assessment.
5. For websites categorized as Level 4 and above and developed by external vendors, a code review shall also be included in the audit.

Appendix A: Website Categorization and Self-Assessment

Website Categorization

Website Type	Categorization Level
Static Website (Mainly for information sharing)	1
Transaction Website (Provides queries etc but no financial / official transactions)	2
Static Website (Information Sharing but high stakes on Reputation)	3
Transaction Website (Provides financial / official transactions)	4
Transaction Website (Provides financial / official transactions and is linked to multiple agencies)	5

Self-Assessment

S. Nos	Description	Website Hosting	Website Development	GIA Policy Mapping
1	Has the agency done a Risk assessment to assess the risks (pros / cons) of using an outsourced services	Applicable	Not Applicable	RM, TM2
2	Are there any Local laws / regulations that restrict you from moving your data to outside your organization locally / internationally	Applicable	Not Applicable	TM2
3	Are there any data laws / regulations in the vendors country of operation that contradict laws or regulation in your country or that may endanger the privacy / confidentiality of your data	Applicable	Not Applicable	TM2
4	Does the choice of your vendor / solution restrict your mobility and independence? Can you move your data or change your service provider if you wanted?	Applicable	Applicable	

Appendix B: Project Initiation Document / MoU and RFP

Project Initiation Document / MoU

Compliance:

The project shall comply with the following policies and standards which are in line with international recommended standards and best practice.

1. Government Information Assurance Policies (ictQATAR)
2. Architecture and Standards (ictQATAR)

<<Agency>> shall endeavor to ensure that the relevant policies and standards are made available to the <<stake holders>> and provide assistance in their interpretation. The project management methodology in use by <<Agency>> shall ensure compliance with these policies and standards during the project term.

The <<stakeholder>> shall endeavor to ensure compliance to the above policies and standards, specifically the GIA policies, during the operational phase of the project in addition to the availability of the necessary resources to achieve this compliance.

RFP

Compliance Requirements:

One of the factors for a successful project is to ensure compliance to established best practices and standards. <<Agency>> shall use the following policies and standards developed by ictQATAR, based upon internationally recognized best practices.

1. Government Information Assurance Policies (ictQATAR)
2. Architecture and Standards (ictQATAR)

All vendors / consortiums bidding for this project shall ensure compliance with the above policies and standards. Further they will also ensure compliance with the relevant Qatari laws that may be in force at the time of submitting their bids.

Copies of the detailed policies and standards shall be made available on request.

Vendors are hereby notified that compliance to these policies and standards and laws shall be part of the evaluation criterion during the bid evaluation phase. Furthermore the vendor will be required to submit a compliance certificate as part of the acceptance test during project closure.

<<Agency>> shall have the right to assess and verify the compliance status internally or through a third party auditor within a period of one (1) year starting from the date of project acceptance. The cost of such an assessment shall be borne by <<Agency>>. However, any non-conformance highlighted in the assessment will have to be fixed by the vendor at no extra cost to <<Agency>>.

Appendix C: Vendor Qualification

Vendor Qualification

S. Nos	Description	Website Hosting	Website Development	GIA Policy Mapping
1	Vendor Assessment in terms of the organization, ownership and financial strength	Yes	Yes	PR3
2	Vendor's Information Security Governance. Do they comply to international standards	Yes	Desired	PR8
3	Does the company provide desired service levels tied to a Service Level agreement	Yes	Desired	TM3, TM8

Appendix D: Contract with Vendor

Contract with Vendor

"Vendor" warrants that the proposed solution complies with the policies and standards mentioned in the RFP. This includes ictQATAR's "Government Information Assurance Policies" and "Architecture and Standards". The vendor further warrants that:

1. They shall comply with the provisions of these policies and standards throughout the project term.
2. They shall provide a compliance certificate as part of the acceptance test during the project closure phase.
3. Failure to achieve compliance shall amount to a default and may lead to invocation of "Default Clause" as per this agreement.

Appendix E: Technical Controls

Technical Controls

S. Nos	Description	Website Hosting	Website Development	GIA Policy Mapping
Infrastructure				
	Are the proposed infrastructure / technology up-to-date?	DESIRABLE	MUST	PR4
	Does the vendor provide commitment to stay abreast of technology?	MUST	MUST	PR8, PR9
Information Security Governance				
	What is the vendor's policy on Information Security (C-I-A)	MUST	DESIRABLE	
	Do they comply with any known standards?	MUST	DESIRABLE	
	What is the vendor's policy on Data Privacy	MUST	DESIRABLE	PS3, SS24
	Do they comply with any known standards?	MUST	DESIRABLE	
	Does it meet Qatar's Privacy Law requirement?	MUST	DESIRABLE	
	What is the vendor's policy on Incident Handling	MUST	MUST	IM
	Does the vendor have an Incident Handling Process?	MUST	MUST	
	Any major incidents in the last 2 years of operation?	MUST	MUST	
	What is the vendor's policy on Business Continuity	MUST	MUST	BC
	Does the vendor have a business continuity plan?	MUST	MUST	
	Is the BCP extended to its supply chain?	MUST	DESIRABLE	
Processes				
	Does the vendor have a Change Management process in place?	MUST	MUST	CM
	Does the vendor have a Patch Management process in place?	MUST	MUST	PR9
	Does the vendor have an Information Life Cycle Management in process? What	MUST	MUST	MS, SS1

	happens to the data when you have terminated the contract?			
	Does the vendor have a process for Service Level Management?	MUST	Not Applicable	
	Does the vendor have a process to track project / development progress?	Not Applicable	MUST	
	Does the vendor have a process for controlling Access to your data?	MUST	MUST	AM
	Do you as "Data Owner" have full access to your data and the associated system logs on the host system?	MUST	Not Applicable	
	Does the vendor provide suitable controls for physically securing the information systems where your website is hosted?	MUST	Not Applicable	PH
	Does the vendor have a process for logging and monitoring system performance, availability, threats	MUST	Not Applicable	SM
Technical Controls				
	The Network is designed to limit opportunities of unauthorized access.	MUST	Not Applicable	NS5, GS1, GS2, GS6
	There is separation in case of multi-tenant operations	MUST	Not Applicable	NS7
	Does Data resides on Physically separate servers (Recommended)	DESIRABLE	Not Applicable	
	In case of Virtualized environments or in a multi-tenant environment review in details the security controls for shared resources	MUST	Not Applicable	
	Public DNS Information should be hosted on a secured local server and /or the Government DNS (part of GN)	MUST	Not Applicable	NS20
	Ensure necessary agreements exist prior to establishing information exchange	MUST	MUST	IE3
	Proper testing and effective matching between vendor's	MUST	MUST	PR4

	claim and functionality			
	Dedicated test and development platform	Not Applicable	MUST	PR5, SS4
	The website is made live (production) only after suitable quality and security assurance tests have been made.	MUST	MUST	SS5
	Software developers use secure coding practices	Not Applicable	MUST	SS6
	The active content on the website shall adhere to OWASP guidelines for building secure application	Not Applicable	MUST	SS22
	Hard coded IP addresses should not be used in the program code	Not Applicable	MUST	
	Authentication information should not be stored / transmitted in clear text. Authentication information should not be hard coded into the application.	Not Applicable	MUST	AM17, AM18, CY6
	All Personal and confidential information shall be encrypted whilst in storage and transit	MUST	MUST	CY3, SS24
	Servers should be hardened to minimize opportunities of misuse	MUST	MUST	SS12, SS13, SS14
	Certain combinations of services are not permitted. For eg: AD servers should not function as any other server, webservers should not be used to hold data. High risk servers e.g. Web, email, file and Internet Protocol telephony servers, etc. having connectivity to uncontrolled public networks: a. maintain effective functional separation between servers allowing them to operate independently b. minimise communications between servers at both the network and file system level,	MUST	MUST	SS15

	as appropriate c. limit system users and programs to the minimum access needed to perform their duties.			
	In case of software development a code review should be done	Not Applicable	MUST	SS7
	System / software / solution meets all legal requirements including license, copyrights, IPR etc	Not Applicable	MUST	SS8
	Suitable documentation is provided	MUST	MUST	NS4, SS9
	Source code is provided by the vendor (websites categorized at level 3 and above)	Not Applicable	MUST	SS10
	Suitable Authentication mechanism is in place to provide access to applications. May include strong passwords, dual factor authentication, cryptography etc..	MUST	MUST	AM12, AM19, AM24, SS25
	Check the integrity of all servers whose functions are critical to the State Agency, and those identified as being at a high risk of compromise. Wherever possible these checks SHOULD be performed from a trusted environment rather than the system itself.	MUST	Not Applicable	SS16
	Store the integrity information securely off the server in a manner that maintains integrity	MUST	Not Applicable	SS17
	Update the integrity information after every legitimate change to a system	MUST	Not Applicable	SS18
	As part of the State Agency's ongoing maintenance schedule, compare the stored integrity information against current integrity information to determine whether a compromise, or a legitimate but incorrectly completed	MUST	Not Applicable	SS19

	system modification, has occurred			