Statement of Exception

GIA Policies Implementation

End of Audit Year: 2010 - 11

<State Agency Name & Logo>

WHAT IT IS?

This template is used to report business functions, process or assets that should be considered as exceptions for GIA policies compliance audit. It helps State Agencies to identify and report audit exceptions.

WHY IS IT IMPORTANT?

The Government Information Assurance Policy is proposed to secure information assets of State Agencies in the State of Qatar. It is mandatory for all State Agencies to comply with the GIA Policy. However, it may not be possible for a State Agency to comply with all requirements specified in the GIA policy document. There may be some exceptions that should be taken into account before planning for GIA policies compliance audit. Hence to report audit exceptions, State Agency should develop a Statement of Exception prior to GIA policies compliance audit.

Upon ABQ's approval, the agency's exceptions (functions, departments and/or processes) will be excluded from GIA Policy Compliance audit. ABQ will carry out GIA Policy compliance audit on State Agency by excluding approved exceptions. This template will allow State Agencies to define its exceptions for GIA Policy compliance audit.

WHO SHOULD USE?

State Agency Security Manager

HOW TO USE IT?

This document must be labeled as 'RESTRICTED' since as per Documentation [DC] of GIAM all ICT documentation should be given highest confidentiality rating (C3). The objective of this template is to identify, document and report State Agency audit exceptions that should be excluded from GIA policies compliance audit. Consider the template as a form and then

1. Start identifying business areas such as functions, departments, processes, sections and/or assets which are not ready for the GIA Policies audit.
2. For each exception, provide details such as
   a. Describe audit exception with adequate explanation
   b. Explain rationale for requesting exception
   c. Identify and list risks involved for not implementing GIA Policy controls
   d. Provide mitigation measures in place for minimizing risk impact
3. Identify the State Agency officer/staff person who is responsible for ensuring compliance for requesting exceptions after the audit and provide his/her contact details.
4. Obtain approval of the State Agency Head & Security Manager and submit the document to ABQ.

Internal

DECLARATION

(User should print/write this page on his/her official letterhead/stationery. This section should briefly outline what this document is about, its contents and brief on why it should be reported. This section may also mention names of individuals who contributed to the analysis and document preparation.)

On behalf of <The State Agency Name>, we hereby confirm that the functions, department, processes, sections or systems listed in this document (please refer to previous page) should be excluded from the GIA Policy Compliance Audit.

_____ _____

Signature of State Agency Head

Date:

Signature of Security Manager

Date:

Official Seal

Exceptions to be considered

(Identify, list and provide areas to which exception is being requested.)

1. **Description**	[Example] Agency Courier/Transport service is not in compliance with GIA Policies particularly with IE7 baseline control of GIAM.
Rationale	[Example] Due to the impact of the recent global recession, A State Agency had to look for various ways to minimize its operational costs. As a part of minimizing costs, the agency cancelled existing service agreement with well known courier agency and entered in to a 5-year contract with a newly setup courier agency. The contract was given only after vendor agreed to • implement appropriate information security controls and • periodic checks to improve service
Risks Involved	[Example] Loss, damage, unauthorized access, mis-delivery, delay
Mitigation Plan	[Example] These risks are common to all couriers. However, State Agency can minimize impact of these risks by • use of HSMs with appropriate encryption levels • insuring high-valued information assets • ensuring regular reporting, monthly checks etc.

2. **Description**	
Rationale	
Risks Involved	
Mitigation Plan	

3. **Description**	
Rationale	
Risks Involved	
Mitigation Plan	

4. **Description**	
Rationale	
Risks Involved	
Mitigation Plan	

Compliance Contact

Name	[Example] Mr. Hameed
Designation	Security Manage
Phone Number	XXXX – XXXXX extn. XXXXXXXX
Fax	XXXXXXXXXX
Email	XXXXXXXXX