Audit Management

GCTS Audit Management Policy

Supplemental to Global Transformation Services Security Standard (GTS SS)

© 2017, 2018 IBM. All Rights Reserved.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| version | Date | APPROVED BY | Description of the Change |
| 1.0 | 15-Jul-2013 | Art Griffin | First Approved version under new Document Management System |
| 2.0 | 13-Mar-2014 | Marc Verstraeten | Updates to reflect Pre-sales audit policies. Updated Revision history table to reflect document mg SOP adjustments. (Only approved versions will be in revision history) |
| 2.1 | 20-Nov-2015 |  | Updated template |
| 2.2 | 08-Sep-2016 |  | Policy Management Review, edit, and template refresh |
| 2.3 | 02-Mar-2017 | Jeremy Dick | Annual update to content Added Section 2 (all) |
| 2.4 | 09-Mar-2017 |  | Minor style/formatting changes (cosmetic) and |
| 2.5 | 13-Mar-2017 |  | Policy Management Review – Analysed against CPI-810 10 and Data Classification |
| 2.6 | 14-Mar-2017 |  | Policy Management Added applicable Control Standards to Purpose and DMS Registry. TCC Review scheduled 3/20/2017 |
| 2.7 | 20-Mar-2017 | TCC | TCC Majority Approval for CISC Review |
| 2.8 | 21-Mar-2017 |  | Policy Management Control Standards Gap Analysis |
| 2.9 | 24-Mar-2017 |  | CISC No Vote – Suggested Changes:  No Vote – Change PCI 12.6 to 12.1.1 and 12.8.4  Purpose and Scope need to be reworked  Program Audit also needs to be reworked |
| 2.10 | 07-Dec-2017 |  | Template updated |
| 2.11 | 08-Dec-2017 |  | IN PROGRESS Policy Management review and changes associated with IBM branding  **NOTE: After this review, the SME would need to make the changes requested by CISC per document history entry 2.9** |
| 2.12 | 2-Jul-2018 | Jeremy Dick | Updates throughout document to update overall policy changes. |
| 2.13 | 2-Jul-2018 |  | Policy Management Review and Update – Ready for Final SME Review |
| 2.14 | 9-Jul-2018 | TCC | TCC Review and Approved for GRCQ |
| 2.15 | 16-Ju-2018 |  | GRCQ Review |

Table of Contents

[1 Overview 1](#_Toc500426920)

[1.1 Purpose 1](#_Toc500426921)

[1.2 Scope 2](#_Toc500426922)

[1.2.1 Personnel Covered 2](#_Toc500426923)

[1.2.2 Alignment with Corporate Policies 2](#_Toc500426924)

[1.2.3 Environments Covered 2](#_Toc500426925)

[2 Request for Information and Audit Policy 3](#_Toc500426926)

[2.1 Ad hoc Email Questions 3](#_Toc500426927)

[2.2 Questionnaire / Security Questionnaire 3](#_Toc500426928)

[2.3 Customer Audit 4](#_Toc500426929)

[2.4 Program Audit 5](#_Toc500426930)

[2.5 Definitions 5](#_Toc500426931)

[3 Audit Evidence Policy 7](#_Toc500426932)

[3.1 Purpose 7](#_Toc500426933)

[3.2 Scope of the Audit Evidence Policy 7](#_Toc500426934)

[4 Third-Party Compliance Reports 8](#_Toc500426935)

[5 Audit Evidence Distribution Policy 9](#_Toc500426936)

[5.1 Restrictions 9](#_Toc500426937)

[5.2 Distribution Matrix 9](#_Toc500426938)

[6 Responsibility 11](#_Toc500426939)

[6.1 Compliance Responsibility 11](#_Toc500426940)

[6.2 Management Commitment 11](#_Toc500426941)

[7 Exceptions 12](#_Toc500426942)

[8 Expiration 12](#_Toc500426943)

[9 Enforcement 12](#_Toc500426944)

[10 Appendices 13](#_Toc500426945)

[Appendix A - Terms and Definitions 14](#_Toc500426946)

[Appendix B - References 16](#_Toc500426947)

[Appendix C - Distribution 17](#_Toc500426948)

List of Tables

[Table 4‑1: IBMThird-party Compliance Reports 8](#_Toc500426949)

[Table 5‑1: Audit Evidence Distribution Matrix 9](#_Toc500426950)

[Table A‑1: Terms and Definitions 14](#_Toc500426951)

[Table B‑1: References 16](#_Toc500426952)

[Table C‑1: Distribution Contacts 17](#_Toc500426953)

List of Figures

**No table of figures entries found.**

# Overview

## Purpose

This policy documents the addendum policy statements supplemental to Information Global Transformation Services Security Standard (GTS SS), addressing requirements specific to IBM Global Technology Servers (GTS) Cloud Transformation Services (formerly Verizon), hereinafter referred to as “GCTS.” This Audit Policy is developed for internal use only to set the policy regarding of all audit related activities within GCTS. Although designed for internal use, this document can serve as evidence where applicable for audit related information requests.

* FedRAMP: based on NIST SP 800-53, Rev4: AU-1
* ISO 2700:2013: A12.7, A.12.7.1
* PCI DSS 3.2: 12.1.1 and 12.8.4

This Audit Policy requires renewal on an annual basis and updates as needed to reflect changes to business objectives or the risk environment in accordance **PCI DSS 3.2: 12. 1.1**. The updates and annual renewal changes are documented Revision History Table located on page (i).

The purpose of this Policy document is to outline the guidelines and requirements for the engagement and management of a Request for Information (RFI) of the Cloud Operations organization. An RFI represents any request from an internal or external individual or organization requesting information about internal policies and processes with regards to Cloud’ operational framework.

RFI’s exist on a continuum of complexity and depth and in multiple formats:

* Security Questionnaires
* Ad hoc questions via email
* Audit requests (customer, program, quality and internal)
* Etc.

This policy is in place to help mitigate the risk to IBM by outlining the overall policy and controls by which IBM will provide information in the event of an RFI.

RFI’s for the Operations team in GCTS are managed by the Governance, Risk, Compliance, and Quality team (GRCQ) with the mission to deliver on requirements of the Operations organization to provide qualified responses, project management, and oversight to all types of requests for information to the organization with respect to GCTS products and services.

Qualified responses are defined as responses that have a degree of rigor around them that are typically provided by a subject matter expert, reviewed by stakeholders and Legal and approved as a vetted response. Conversely, unqualified responses are responses that are not fully vetted by stakeholders or subject matter experts. Unqualified responses to any request for information must be identified as such in communications back to the requestor.

## Scope

### Personnel Covered

This policy applies to all IBM full and part-time employees, temporary workers, volunteers, contractors, or any other agents employed to perform work and who have been granted access to GCTS information systems and information assets. Hereinafter, the covered personnel described above will be referred to as “personnel.”

### Alignment with Corporate Policies

This document is a supplemental guideline that specifies certain requirements related to GCTS products and services. All documents considered for approval by the IBM GCTS Technical Coordination Committee (TCC) and the Governance, Risk, Compliance, and Quality (GRCQ) Council are sub-ordinate to, and supplements of, IBM Corporate Policy GTS SS, as well as the Business Conduct Guiltiness and the Worldwide Records Management.

### Environments Covered

Unless otherwise noted, the controls outlined within this policy apply to all equipment and associated services that the GTCS business unit owns, manages, or leases.

# Request for Information and Audit Policy

As stated above, there is a full spectrum of RFI types that the GRCQ teams are engaged to manage. The GRCQ team is the primary funnel for all RFI’s into the Cloud Operations organization. As described in subsequent sections, the GTS audit team shall only be engaged in an audit related activity (to include all types of RFIs) via the following email address: [GTS\_PCI\_AUDIT\_TEAM@wwpdl.vnet.ibm.com](mailto:GTS_PCI_AUDIT_TEAM@wwpdl.vnet.ibm.com).

GTS PCI Audit Team (Note: in order to engage the audit team, the email can only be initiated to this email distro from an IBM workstation connected to the IBM network.

The contents of the request shall include the following information at a minimum:

* Scope of the request (i.e. audit, questionnaire, ad hoc question, etc.)
* Definition of services in scope (i.e. Managed Hosting, Cloud, ECME, RAM, IPAH, etc.)
* Location of services
* Specifics of the request
* If an audit, please provide customer audit rights outlined in the customer contract.
* Target timeframe requested for information

The following are the high level RFI Categories and associated policies.

## Ad hoc Email Questions

These types of questions are generally based on internal questions. In general, responses to ad hoc email questions will be in the form of non-qualified responses, and must be reflected as such in the response. If the requestor needs a formalized response, the exact verbiage from an already approved response (i.e. qualified) must be leveraged if available. If there is not already an approved response available for the question, a Subject Matter Expert (SME) must be consulted for the control area and the answer must be vetted prior to submitting the response as a qualified response.

Once an unqualified response is vetted and approved, it then becomes a qualified response for use at a later date for an identical request. Qualified responses shall be stored for use in a controlled environment.

## Questionnaire / Security Questionnaire

The following policy statements are applicable for all Questionnaires:

1. All Sales and RFP related questionnaires shall be directed to Sales and Account teams.
2. Questionnaires must be submitted to the GRCQ team via the RFI email, as described above.
3. The customer must be provided the applicable certifications, audit reports and pre-approved questionnaires prior to submitting the Questionnaire request to the GRCQ team.
4. It is the responsibility of the requester to populate the questionnaire to the best of their ability prior to requesting assistance from the GRCQ team. This involves reviewing applicable certifications, Consensus Assessments Initiative Questionnaire (CAIQ) and other knowledge tools to populate answers.
5. Once the GRCQ team is engaged to assist with a questionnaire, the completed questionnaire will be submitted back to the requester. It is the responsibility of the requester to submit back to the end customer.
6. Prior to submitting the fully responded questionnaire, it is the responsibility of the internal requester to ensure Legal approval, if required, prior to sending responses to the customer.
7. Questionnaires vary in depth and complexity, therefore, the amount of time to complete varies. Completion time of the questionnaire will be negotiated with the requester at the time of submission.
8. The scope of responses that the GRCQ team can respond to are limited to questions around the GCTS Operations organization. The requester is responsible for all other non-Operations related questions (ex. Human Resources (HR), Sourcing, etc.).

## Customer Audit

Prior to agreeing to conduct a customer audit, policy dictates the following criteria must be met:

1. The scope of audit facilitation that the GRCQ team can provide is limited to the business functions pertaining to Cloud Operations organization. The requester is responsible for all other non-Operations related questions (ex. HR, Sourcing, BCEM etc.).
2. Sales and request for proposal (RFP) related audit requests shall be directed to the Proposal team for vetted responses. In the event a supplier qualification is required in a pre-contract scenario, the requester may request approval to facilitate the audit from the Cloud Operations Vice President (VP).
3. The GRCQ team is the primary funnel into the Operations organization with regards to all types of RFIs.
4. The internal requestor of the customer audit must validate the audit rights the customer has in the contract. At a minimum, IBM must deliver on any contractual obligations. Lack of a right to audit clause in the contract requires approval from the VP of Operations and Legal before agreeing to the audit. In some cases, regulatory conditions may exist to give customers the right to audit regardless of their contractual right (ex. GDPR). In such cases, the requestor must identify the regulatory right to audit as part of the initial request.
5. The GRCQ team remains as an internal resource and all communications with the customer are the responsibility of the internal requester.
6. The requestor shall provide the customer with all applicable certification and compliance reports in accordance with the customer’s Non-Disclosure Agreement (NDA).
7. A minimum of 30 days notification of a customer audit is required before the proposed start date. Ultimately, IBM and the customer must agree mutually on an audit date, which is based on resource availability within Verizon. In some cases, the contract with the customer may state different terms for notification of an audit. In those scenarios, the contract takes precedence over this policy.
8. Prior to conducting an audit, a scoping session must be held, at a minimum of 2 weeks prior to the start of the audit and must include the GRCQ team, account team, the customer and their auditor (if a 3rd party auditor is involved).
9. The requestor must validate who will conduct and participate in the audit: 3rd party auditor, customer, subsidiary, customer of a customer. In all cases, Verizon’s customer MUST be present for the duration of the audit. Unless specified in the customer contract or through executive leadership, IBM does not agree to facilitate an audit conducted by a customer of a customer.
10. The requester is responsible for ensuring all participants, including related affiliates in the audit, are covered by applicable NDA’s.
11. Policies and Procedures are only available for review on-site or via WebEx (or similar tool), with agreement that screen shots will not be taken by customer (auditor).
12. Existing reports and certifications shall be provided to the customer by the internal requester and are expected to be valid evidence as needed. For example, if a customer requests an audit to support their ISO27001 certification, IBM expects the IBM ISO27001 certificate to suffice as evidence for their own certification endeavors. The same applies to other certifications that IBM holds and maintains.
13. Prior to commencement of an audit, the customer shall review all applicable compliance reports and other publicly available knowledge sources regarding Cloud control (ex. CAIQ).
14. The redacted customer facing version of the ISO27001 Statement of Applicability (SOA) is available for distribution only if specifically requested by the customer and must follow all applicable rules for NDA.
15. Non-customer records and records for shared environments will not be shared.

## Program Audit

1. Program Audits are owned and managed by the Security and Compliance team in most cases. These include programs such as (but not limited to) SSAE16, ISO27001, FedRAMP, PCI. There are other Program Level audits that are handled by other teams, such as HIPAA.
2. The GRCQ team fulfills a support role for Program Level audits and is the first point of contact for Operations by the Program Audit Owner. The GRCQ team will assist in collection of resources and evidence related to the audit as well as issue tracking and audit management during the execution phase of the audit.
3. Program Level audits require deeper records review by 3rd party auditors and assessors. These auditors are considered privileged auditors and are covered by confidentiality agreements to view detailed records, files and evidence that contains information about the underlying shared infrastructure within the bounds and scope of the audit. In the case of program audits, which are in place to support our own 3rd party compliance initiatives, review and analysis of these artifacts are required for successful certification.

## Definitions

* **Internal Requestor:** IBM resources initiating an audit request on behalf of a customer. This is usually a:
  + Service Manager
  + Account Representative
* **Pre-contract Audit:** A vendor risk assessment performed by prospective IBM customers on the IBM Quality Systems and Security Controls.
* **Production Audit:** A vendor risk assessment performed by existing and contracted IBM customers on the IBM Quality Systems and Security Controls according to the terms and frequency stipulated in their contract.
* **GRCQ –** Governance, Risk, Compliance, and Quality
* **Qualified response –** Responses prepared for a request for information that have been provided by the SME and fully vetted through the appropriate approval channels, such as Legal.

# Audit Evidence Policy

## Purpose

The purpose of the Audit Evidence Policy is to define the IBM evidence distribution guidelines.

## Scope of the Audit Evidence Policy

The scope of this policy defines the auditability of policies, procedures, and records in the following areas:

* Physical security
* Environmental security
* Logical access control
* System software maintenance
* Change Management
* Infrastructure systems monitoring and support
* Computer operations production support
* Data backup
* Internal audits
* Business Continuity (BC) and Disaster Recovery (DR)

# Third-Party Compliance Reports

External, third-party auditors and assessors audit IBM on annually to maintain compliance with many industry-wide standards. The output of these audits and assessments provides detailed information about GCTS operations. In most cases, questions that customer auditors have can be addressed by reviewing these third-party reports.

Table 4‑1: IBM Third-party Compliance Reports

| **Payment Card Industry** | |
| --- | --- |
| **Attestation Report** | **Description** |
| IBM Payment Card Industry Data Security Standard Attestation on Compliance (PCI DSS AOC) | Attestation from an independent PCI assessor confirming IBM compliance to the PCI DSS |
| PCI DSS v3.2 | The PCI standard under which IBM has exhibited compliance. The PCI DSS AOC (above) evidences compliance with this standard. |
| **SSAE 16/SOC 1 Reports** | |
| **Audit Report** | **Description** |
| SOC 1 Report | Independent Service Auditor’s Report on Controls Placed in Operation and Tests on Operating Effectiveness for in scope colocation sites. |
| **AT 101 (Attestation Engagements Standard) with Trust Services Criteria** | |
| **Audit Report** | **Description** |
| SOC 2 Report | Independent Service Auditor’s Report on Controls Placed in Operation and Tests on Operating Effectiveness for in scope colocation sites. |
| **ISO/ISE 27001:2005 Certification** | |
| **Certificate** | **Description** |
| ISO 27001 Certificate | Certification provided by an accredited certification body that IBM has demonstrated compliance with this standard. |
| ISO27001 Customer Facing Statement of Applicability (SOA) | Matrix noting control applicability to in-scope services. This is a redacted, customer facing version of the SOA. |

# Audit Evidence Distribution Policy

## Restrictions

IBM GTS SS is the governing policy for classification of data. In addition to these corporate directives, IBM– in a subordinate policy – implements the following restrictions on the distribution of information to protect its copyrights;

1. Infrastructure details (system names, functions, IP addresses, locations, vulnerabilities, configuration details) are not allowed to leave IBM control – even under NDA.
2. For procedures involving design, product implementation and documents that are labelled **Confidential** only the table of contents will be available for audit.

## Distribution Matrix

For all audits, the control owner must approve evidence that is provided to an auditor.

Table 5‑1: Audit Evidence Distribution Matrix

| **Evidence Type** | **Commercial Customer** | **Federal Customer** | **IBM Third-party Auditors** | **GxP Customer**  **Pre-Contract** |
| --- | --- | --- | --- | --- |
| Policy | Show | Show \*\* | Distribute (Note) | Show |
| Process | Show | Show \*\* | Distribute (Note) | Show |
| Procedures | Show onsite | Show onsite \*\* | Distribute (Note) | Show |
| Records | Show onsite\*\*\* | Interview \*\* | Distribute (Note) | Interview |
| **Note:** The following distribution “Methods” apply:  **Interview:** Cannot be distributed or shown to the auditor in any form. Evidence is provided by interview only. Redacted screenshots and presentations are allowed to support the interview  **Show onsite**: Can be shown via remote collaboration to an auditor on-site (at a IBM location) (inclusive of Distribution Methods above)  **Show**: Can be shown to the auditor:   * On-site (that is, at a IBM location * Via remote collaboration. (inclusive of Distribution Methods above)   **Distribute**: Can be distributed to an auditor as a soft copy. Client names and IP addresses must be scrubbed. Inclusive of Distribution Methods above  **\*\* FedRAMP Secure Distribution**: For Federal customers of a FedRAMP accredited platform, distribution of policy, process, procedures and records within a secure FedRAMP portal for access by agencies leveraging it. Exclusive of distribution methods above  \*\*\* Commercial customer can view records pertaining to their own transactions. No records from shared environments or multitenant platforms can be shown | | | | |

# Responsibility

It is the responsibility of all personnel to know, understand, and conform to the policies set in IBM Corporate GTS SS, and others as they apply to all IBM employees.

## Compliance Responsibility

Compliance with security standards and practices addressed in this document are subject to applicable law. Conflicts with local legislation or regulation shall be brought to the attention of IBM Counsel and coordinated with the responsible security executive for resolution.

***Important****: Nothing in this document should be taken as justification to circumvent existing IBM Corporate policies, standards, or management direction.*

## Management Commitment

IBM has established the GRCQ to serve as a forum for all stakeholders with responsibility for maintaining the security of the IBM information technology environment, both internal and customer serving.

This policy has been managed by [SECM-00089 Policy Management Process](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00089%20Policy%20Management%20Process.pdf) and approved by IBM GTS GRCQ Council.

# Exceptions

Exceptions to this policy must be approved by the governing/serving by the GTS GRCQ Council.

# Expiration

Unless readopted, this Policy expires three (1) years from the date of approval.

# Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Appendices

Appendix A - Terms and Definitions 14

Appendix B - References 16

Appendix C - Distribution 17

Appendix - Terms and Definitions

Table A‑1: Terms and Definitions

| Term | Definition |
| --- | --- |
| BC | Business Continuity |
| BO | Business Owner |
| CAIQ | Consensus Assessments Initiative Questionnaire |
| DC | Disaster Recovery |
| GRCQ | Governance, Risk, Compliance, and Quality |
| HIPAA | Health Insurance Portability and Accountability Act |
| HR | Human Resources |
| IRC | Information Resource Custodian |
| NDA | Non-Disclosure Agreement |
| PCI | Payment Card Industry |
| Personnel | All IBM full and part-time employees, temporary workers, volunteers, contractors, or any other agents employed to perform work and who have been granted access to IBM Cloud and Data Center Services information systems and information assets. |
| RFI | Request for Information |
| RFP | Request for Proposal |
| SOA | Statement of Applicability |
| SME | Subject Matter Expert |
| SSAE 16 | Statements on Standards for Attestation Engagements |
| TCC | IBM Technical Coordination Committee |
| VP | Vice President |

Appendix - References

Table B‑1: References

| Document Number | Document Title |
| --- | --- |
| SECM-00089 | [SECM 00089 Policy Management Process](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00089%20Policy%20Management%20Process.pdf) |
|  |  |
|  |  |
|  |  |

Appendix - Distribution

Table C‑1: Distribution Contacts

| Name/Role | Contact Information |
| --- | --- |
| GTS PCI Audit Team | [GTS\_PCI\_AUDIT\_TEAM@wwpdl.vnet.ibm.com](mailto:GTS_PCI_AUDIT_TEAM@wwpdl.vent.ibm.com) |
| GCTS Governance and Compliance | [GCTS-Governance&Compliance@wwpdl.vnet.ibm.com](mailto:GCTS-Governance&Compliance@wwpdl.vnet.ibm.com) |
| GTS Risk and Compliance RFI Request Group | GTS Risk and Compliance RFI [Requests@wwpdl.vnet.ibm.com](mailto:Requests@wwpdl.vnet.ibm.com) |