

Opening Meeting | Internal Audit Cybersecurity Audit

September 30, 2021 2:00pm – 2:45pm



Introduction of Audit and Client Teams

Internal Audit Team Members

- · Hillel Judasin, First Vice President
- · Christian Soellner, Vice President
- · George He, Assistant Treasurer

Information Security Team Members

- Max Tumarinson, Senior Vice President, CISO
- · Jonathan Ruf, First Vice President, Information Security Officer
- · Edward Tsai, Vice President, Information Security Officer
- Joseph Martano, AVP Information Security
- Austin Muniz, AT Information Security

Current Events, Business Processes and Technology

Discussion of:

- Changes to the business processes since the last audit.
- New technologies that play a role in the business process.
- New procedure documents and controls.
- New processes
- Changes in personnel

Audit Process / Phases

Planning

- Discovery Build knowledge of organizational structure, business processes, current and emerging risks, systems
 - · Walkthrough processes
 - Review Documents
 - Research technologies
- Opening Meeting
- Provide initial request list for documents
- Finalize audit objectives and scope
- Audit Scoping Memo

Fieldwork

- Additional walkthroughs, substantive tests of key controls
- Status meetings discuss accomplishments, next steps, potential issues, roadblocks
- Prepare, review and QA work papers
- Issues are communicated as they are identified

Reporting

- Closing meeting
- Collaborate on background section, identify SMART corrective actions and realistic target dates
- Review draft report
- Discuss artifacts that will evidence completion of corrective action
- Final report

Post-Audit

- Audit Issue Tracker
- Ongoing collaboration with management team on progress of remediation
- Status of issues are reported to Audit Committee

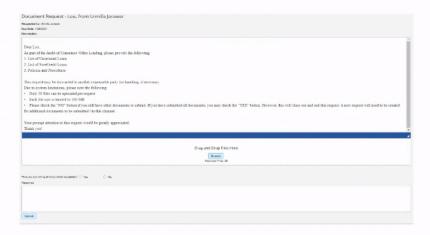
Audit Process Enhancement: TeamMate

Internal Audit recently implemented an electronic work paper solution called TeamMate.

This new application brings efficiency and consistency to the audit process, and will facilitate the full audit lifecycle from risk assessment through reporting.

In addition, TeamMate drives certain requests and alerts including audit documentation requests.

Below is an example of a documentation request email and the email contents once opened. The request can be fulfilled directly within the email received.



Anticipated Audit Timeline

| Milestone | Date |
|---------------------------------|--------------------|
| Intention to Audit Notification | May 20, 2021 |
| Planning | September 30, 2021 |
| Opening Meeting | September 30, 2021 |
| Audit Scoping Memo | October 21, 2021 |
| Closing Meeting | November 19, 2021 |
| Draft Report | November 26, 2021 |
| Final Report | December 9, 2021 |

Management-Identified and Repeat Issues

Management-Identified Issues

- As noted in the Intent to Audit Notification, these issues must be logged in the issue management component of the Bank's GRC tool, prior to the audit opening meeting in order for the issue to be considered Management-identified for this audit.
- These issues should have a defined action plan, applicable target date, status and owner.

Repeat Issues

- When an issue in a prior audit report was closed and the same control breakdown is identified, the issue will be reported again and noted as a REPEAT ISSUE.
- The auditor will determine if the risk level will be increased because the original corrective action was not sustainable.

Issue and Report Ratings

Issue Ratings

High The probability of errors occurring is highly likely or its impact is significant. Immediate attention is necessary

Medium The probability of errors occurring is likely or its impact is moderate. Prompt attention is necessary.

Low The probability of an error occurring is less likely or its impact is limited. Attention is necessary.

Control Environment Ratings

Satisfactory: The processes are designed with effectively operating key controls that facilitate the achievement of business objectives. Risks, if any, may be mitigated or managed and do not prevent the achievement of overall business objectives. Actions may still be required.

Improvement Required: The processes are designed with key controls that may not effectively mitigate risks. Significant control deficiencies were identified, and/or previously noted deficiencies remain open.

Unsatisfactory: The overall control framework is compromised. Key controls within the process do not exist or do not mitigate risks. Serious control deficiencies were identified, and/or previously noted deficiencies remain open.

Reporting, Issue Tracking and Audit Committee

Reporting

- Issues identified during audits are discussed with responsible officers to facilitate management's corrective
 actions and target dates.
- After review by responsible officers, audit reports are issued with background, scope, audit report rating, audit issues, management's corrective actions, corrective action owners and target dates.

Issue Tracking

- Audit issues are entered in the Audit Issue Tracker and distributed to corrective action owners and senior officers.
 - Auditor and corrective action owner should discuss the status of the remediation plan to determine
 whether it is on track or if the target date needs to be changed. The corrective action owner will need to
 provide the auditor with an explanation for the need to change the target date.
 - Corrective action owners need to notify Internal Audit when an audit issue is remediated and provide artifacts evidencing the implementation of the control. Internal Audit has 30 calendar days to validate the issue from the provision of artifacts.

Audit Committee

- Corrective action owners may be asked to attend the Audit Committee meeting when a report is rated Improvement Required or Unsatisfactory.
- Corrective action owners of high risk issues may be asked to attend the Audit Committee meeting when a target date is changed twice or is over due.

Communication and Interaction

- · Frequent communication of ideas and concerns
- Accessibility
- Timely responses
 - > Inquiries
 - Information Requests
 - Corrective Actions with target dates
- Transparency
- · Professional approach
- · Client liaison and contacts
- · Vacation schedules
- · Client upcoming deadlines
- Client feedback provided via Audit Client Survey

Scope not yet defined. CSF 500, Incident, Reporting from 2nd line, SLA, ServiceNow, Governance, Oversight, SIEM, Cloud (new) – INFOSEC only