AUDIT OF CAPITAL JONES

Office of Chief Audit Executive, Johnson Yang

APRIL 2, 2016

201, CONSUMERS RD SUITE, NEW YORK, USA
Email: johnsonyang@hotmail.com

Table of Contents

Executive Summary

We are pleased to serve Capital Jones as its independent auditors and look forward to our continued relationship. We provide information on the following pages and to assist you in performing your oversight responsibilities. This information is intended solely for the Board and management and is not intended to be and should not be used by anyone other than these specified parties

The report has been compiled by Executive members of Johnson Yang based on the analysis of the progress from the work streams and endorsed by the Audit and Risk Committee.

Our audit covered a review of the management control framework in place to ensure compliance with any government policies as well as with all parties and vendors; also compliance with company's own policies and procedures. Review was done to also make sure that departmental procedures are effective, efficient and provide value for money and ensure financial integrity in accordance with all memorandums signed.

In summary, we found deficiencies in complying with contracting policies as well as areas where improvements are warranted. This documented explains the following observations in detail:

- A proper segregation of duties (SoD) should be implemented
- Disaster recovery plans should be defined properly, tested and maintained
- IT service recovery should be provided after office hours as well
- IT disaster recovery plans should be completed with its invocation and mobilization processes
- A full ITDR needs to be performed
- Better Service Level Agreements should be implemented with the clients
- Service desk needs to be more prompt when issues and incidents are reported

Background

Capital Jones has been going through organizational and structural changes in the past couple of years.

Information Management and Technology have been going through internal transformation. Initially, changes were in response to poorly functioning internal structures causing problematic information service delivery.

The Assistant Director of Capital Jones, Eddard Stark, has provided a functional overview of all the systems in the company.

Internal audit is part of the ongoing monitoring of the bank's system of internal controls and of its internal capital assessment procedure. Internal audit provides an independent assessment of the adequacy of, and compliance with, the bank’s established policies and procedures. As such, the internal audit function assists senior management and the board of directors in the efficient and effective discharge of their responsibilities.

Audit Objective

The objective of this audit was to determine whether Capital Jones has developed and implemented policies and procedures and internal controls for effective and timely performance of IT examinations as required by the state and federal guidelines.

Audit Scope

The scope of this audit was Full Scope IT examinations (IT examinations) performed independently by Capital Jones during the time period from September 1, 2015 through January 31, 2016.

From a general point of view, the scope of internal audit includes:

- the examination and evaluation of the adequacy and effectiveness of the internal control systems;

- the review of the application and effectiveness of risk management procedures and risk assessment methodologies;
- the review of the management and information systems, including the electronic information system and electronic banking services;
- the review of the accuracy and reliability of the log records and technology reports;
- the review of the means of safeguarding assets;
- the review of the bank's system of assessing its capital in relation to its estimate of risk;
- the appraisal of the economy and efficiency of the operations;
- the testing of both transactions and the functioning of specific internal control procedures;
- the review of the systems established to ensure compliance with legal and regulatory requirements, codes of conduct and the implementation of policies and procedures; and
- the testing of the reliability and timeliness of the regulatory reporting;

Audit Approach

The audit methodology included a review of policy and procedures, and other internal and external documentation; a review of a sample of work papers and the respective ROE; a review of compliance reporting; and, the evaluation of data reliability of Capital Jones's database.

We obtained and/or reviewed the following information:

a) Capital Jones policies (i.e. Overdraft Policy, Dormant Account Policy, Contingency Plan Policy, FCRA Policy, Identity Theft Prevention Policy, Anti-Money Laundering Policy, Risk Management Policy).

b) Capital Jones procedures (i.e. Opening/Closing account procedures, ATM visa debit card procedure, Bank wire transfer procedure, foreign currency procedure, incoming/outgoing collections procedures, teller transaction procedure, guard force management procedure, lost stolen checks NS funds procedure)

c) Guidance compiled by Capital Jones from FDIC, FRB, FFIEC and other entities that is listed as "Reference Material" and accessible at Capital Jones website.
d) Data from Capital jones's Examination Database Information System on the Network (EDISON) 6 Strengths Annual Internal Audit Report Fiscal Year 2016
e) Capital Jones's internal reporting on compliance with examination priorities, dated January 5, 2017.
f) Sample selection of IT examination work papers and respective ROE.
g) Personal training profile report for IT examiners as of March 3, 2017.

We performed various procedures, to include the following:

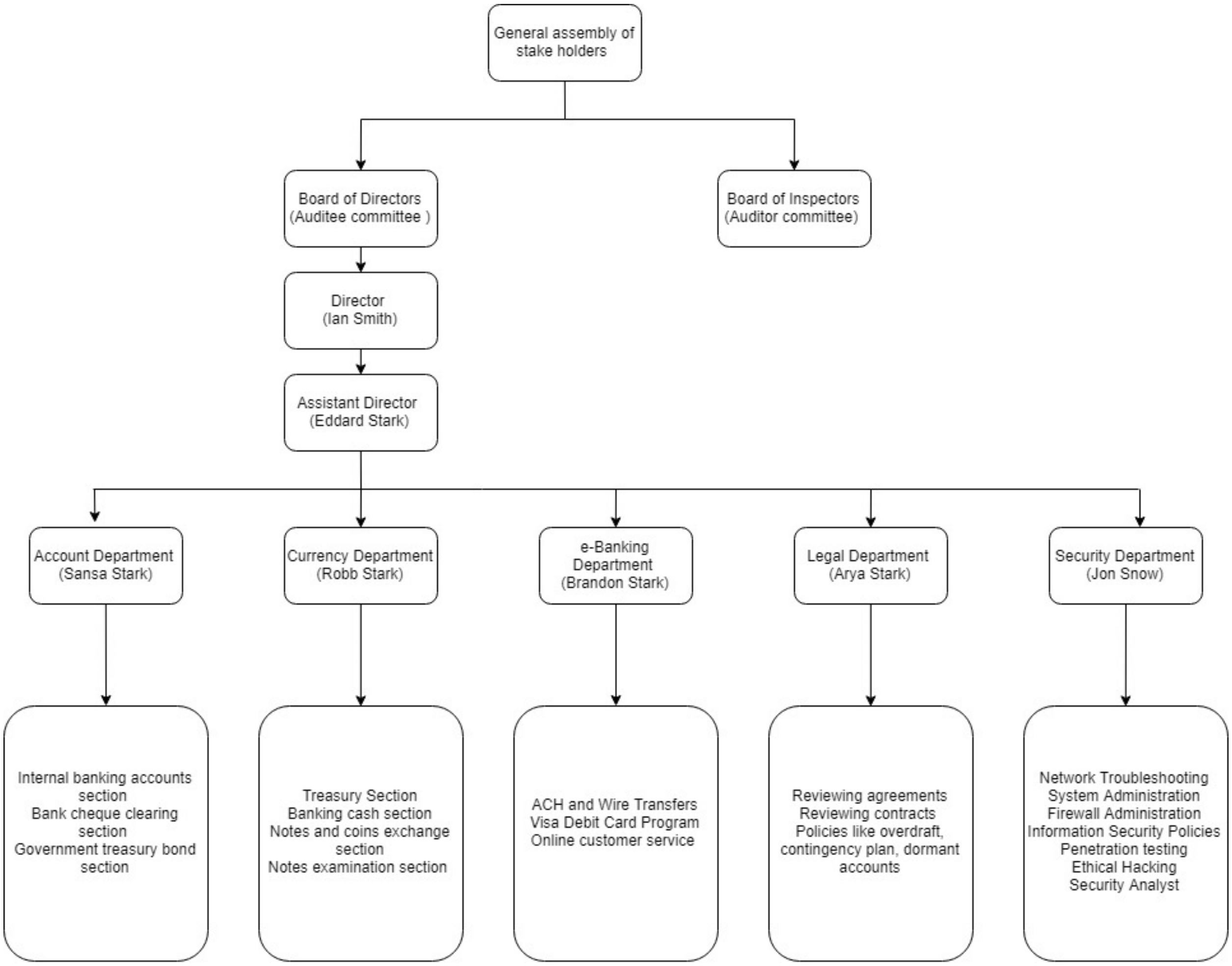
a) Obtained an understanding of the controls in place over the IT Examinations area through review of Capital jones's established policies and procedures; applicable laws and regulations; and, an interview with the Assistant Director.
b) Reviewed the ROEs of all IT examinations to determine whether they (a) are reflective of the examination results documented in the work papers; (b) report accurate information; and, (c) are prepared in accordance with established policies and procedures.
c) Reviewed Capital Jones's Personal Training Profile Report as of March 1, 2017 to determine whether commissioned IT examiners meet Capital Jones's training requirements.
d) Obtained Capital Jones's "Past Due Report" for the period from September 1, 2017 through January 31, 2017 to determine whether—
    a) IT examinations are performed in a timely manner;
    b) the data agrees to Capital Jones's examination priorities compliance reporting; and,
    c) the report was complete by comparison to a listing of regulated banks and trust companies.

Strengths

- Capital Jones has developed and implemented controls to ensure IT examinations are performed in a timely manner. During the period reviewed, 88% of the IT examinations performed by Capital Jones were on time.
- Work performed was well documented in work papers. Amongst the work papers we reviewed, all Report Worthy findings identified in the Summary of Findings (SOF) were included in the ROE, and all Findings included in the ROE were listed as Report Worthy in the SOF.

Organizational Chart

Below attached is the organizational chart that Capital Jones has implemented


General assembly of stake holders
Board of Directors (Auditee committee)
Board of Inspectors (Auditor committee)
Director (Ian Smith)
Assistant Director (Eddard Stark)
Account Department (Sansa Stark)
Currency Department (Robb Stark)
e-Banking Department (Brandon Stark)
Legal Department (Arya Stark)
Security Department (Jon Snow)
Internal banking accounts section
Bank cheque clearing section
Government treasury bond section
Treasury Section
Banking cash section
Notes and coins exchange section
Notes examination section
ACH and Wire Transfers
Visa Debit Card Program
Online customer service
Reviewing agreements
Reviewing contracts
Policies like overdraft, contingency plan, dormant accounts
Network Troubleshooting
System Administration
Firewall Administration
Information Security Policies
Penetration testing
Ethical Hacking
Security Analyst

Findings and Recommendations

1. A proper Segregation of Duties (SoD) should be implemented

Segregation of Duties controls are designed to ensure that staff do not have access to a risky mix of functions. Ensuring that the positions involved in performing departmental IT processes do not have conflicting duties is critical to reduce risk of errors, misappropriations, and fraud and to maintain a strong financial transaction control environment. Adequate segregation of duties should be maintained at all times in ant IT process.

The preferred number of individuals that should be involved in handling a process is three or more. In absence of an adequate level of staffing, segregation of duties can be maintained via compensating controls.

Objective

The Auditors involvement was intended to ensure the proper consideration and integration of process controls, including (but not necessarily limited to) control design and effectiveness appraisal.

Finding

During the audit review a gap in internal controls was noted. It was identified that in case of system changes the same personnel is responsible to authorize a change request as the person doing the procedure for the change request. Also, for logical and physical breaches the same personnel is responsible for security and privacy events. Security incidents that are a threat should go to a security personnel and privacy incidents to privacy personnel. Mention everywhere that so check is required

The lack of SoD can provide the person with ability to create unauthorized transactions by creating a fictious vendor; this can lead to fraudulent activities and potential loss of funds.

Recommendation

Consider the following in assigning duties to each of the individuals involved in handling any process:

- The most basic segregation is a general one: segregation of the duties of the IT function from user departments. Generally speaking, that means the user department does not perform its own IT duties. While a department will sometimes provide its own IT support (e.g., help desk), it should not do its own security, programming and other critical IT duties. To mix critical IT duties with user departments is to increase risk associated with errors, fraud and sabotage.
- Because of the level of risk, the principle is to segregate DBAs from everything except what they must have to perform their duties (e.g., designing databases, managing the database as a technology, monitoring database usage and performance). The IT auditor should be able to review an organization chart and see this SoD depicted; that is, the DBA would be in a symbol that looks like an island—no other function reporting to the DBA and no responsibilities or interaction with programming, security or computer operations
- The development and maintenance of applications should be segregated from the operations of those applications and systems and the DBA. That is, those responsible for duties such as data entry, support, managing the IT infrastructure and other computer operations should be segregated from those developing, writing and maintaining the programs. The same is true for the DBA.
- Much like the DBA, the person(s) responsible for information security is in a critical position and has "keys to the kingdom" and, thus, should be segregated from the rest of the IT function. This person handles most of the settings, configuration, management and monitoring (i.e., compliance with security policies and procedures) for security. Login credentials may also be assigned by this person, or they may be handled by human resources or an automated system. Therefore, this person has sufficient knowledge to do significant harm should he/she become so inclined. This risk is especially high for sabotage efforts.

The SoD should be reflected in a thorough organizational chart:

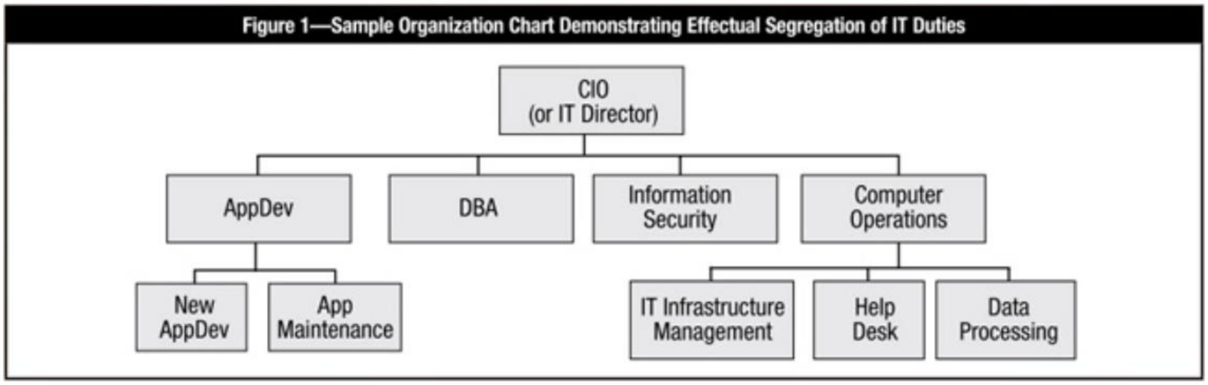


Figure 1—Sample Organization Chart Demonstrating Effectual Segregation of IT Duties

Conclusion

Based on the Auditor's review, the control design is not adequate to properly mitigate development, security, operations and compliance risks. A proper segregation of duties (recommended above) must be implemented.

Manager Response:

There was a reduction in force (RIF) that occurred In 2013 and two retirements that occurred in 2014 of which only one position was allowed to be filled. This has created a situation where certain employees have incompatible duties from an optimal internal control perspective. While each of these employees has their own job duties to perform, they also backup other employees in the section in cases of absences. In order to create a compensating control, reports will be developed to monitor data inputs performed by these employees to ensure the integrity of the processes.

2. Disaster Recovery plans are not defined completely and they need to be tested and maintained

Objective:

The objective of our work was to assess:

- The IT disaster and recovery in place to meet Capital Jones contractual requirements
- The methods, process and controls employed to validate the IT disaster and recovery capability through testing
- The methods, process and controls employed in maintaining the IT disaster and recovery capability as the company adds new services or updates the old ones

Finding:

The audit has identified 1 high and 2 medium risk findings in the internal audit. The high risk finding is:

a) The capital Jones contract includes IT service recovery only during business hours:

The wider contract with Capital Jones only covers business hours between 8am to 6pm in the working week, excluding bank holidays and weekends. If a disaster occurred out of hours Capital Jones are not obliged to start recovery until 8am the next business day, even if the IT service has a 2 hour Recovery Time Objective (RTO). Additionally for those that have longer RTO’s, i.e. the Tier 2 IT services with 48 hours, the recovery would potentially stop and start if the recovery actions exceeded the contracted hours, again taking longer than expected. From a business impact perspective, if a disaster happened out of hours, it would mean that company would be without the services far longer than expected and may cause a material impact as services to the public would be interrupted. This would particularly impact any function that work out of hours and that rely on a Tier 1 service with an RTO of 2 hours

- The current Capital contract for all IT services only covers the hours of 8am to 6pm during the week and excludes bank holidays.
- IT services with ITDR capability at Capital Jones are split into two tiers. Tier one services have an Recovery Time Objective (RTO, the time from invocation the IT service has operational) of two hours and hours and a 1 hour Recovery Point Objective (RPO, permanent data-loss, i.e. if a system with an RPO of 1 hour fails at 1300 it will be brought back the in state it was at 1200, with an hours permanent data loss).
- Tier two IT services have an RTO of 48 hours and an RPO of 24 hours.
- If an incident happens out of hours, Capital Jones would not be obliged to start recovery until 8am the next day. Additionally, if recovery had started, for example, at 4.30pm, recovery would stop at 6pm and re-start at 8am.
- In a Tier two service case, as the RTO is 48 hours, this potentially could extend the recovery over several days.

Risk

If a disaster occurs out of hours IT services will not be recovered to their RTO. The risk is that teams that work out of hours may not be able to operate and will not be able to provide the service are required to, to the public.

Recommendation:

- Capital Jones should extend out of hours support
- Also consider extending DR (disaster Recovery) provision for these critical services.
- The target to resolve this should be December 2017

Manager Response:

Capital Jones staff, who is responsible for the ITDR programme has been notified for inclusion of this finding in the system. In order to extend our out of hours support, we would need more staff and knowing that the risks of this finding are high; the committee has been notified to take an immediate action for this and resolve the out of office hours IT service issue.

One of the medium risk finding is as follows:

b) IT Disaster Recovery plans are not complete and its invocation and mobilization processes are not defined sufficiently: -

Whilst technical ITDR plans are complete for Tier 1 IT services, the plans for Tier 2 are not complete. Instead there is generic guidance on how to recover a system from back-up, rather than the specifics on each Tier 2 system and the order they are supposed to be recovered in. Additionally the processes to invoke the ITDR capability are not clear, particularly with respect to the transition of responsibility from the business as usual major incident management process to the IT Business continuity plan and the mobilization of central Capital Jones resources, who are essential for the execution of the recovery. The impact is that without sufficiently detailed plans or clear mobilization and invocation processes, the overall recovery may be delayed with IT services being recovered later than expected, which could cause a material impact to the business dependent on what public services were affected.

- IT services that have ITDR capability are now split into two tiers. Tier 1 IT services have an RTO of two hours and an RPO of one hour.
- Tier 1 ITDR technical recovery provision is based replicating data to the ITDR site and failing over the services using a tool called Site Recovery Manager (SRM) to prepared IT infrastructure, and is a relatively simple operation.
- Tier 2 IT services as provisioned have an RTO of 48 hours and an RPO of 24 hours. Tier 2 recovery technical provision is from the last available back-up, which may be up to 24 hours old, hence the RPO, which is then recovered to IT infrastructure in the recovery data centre.
- The technical recovery plans currently only cover the Tier 1 IT service recovery steps in significant detail, which would allow for easy coordination and execution
- The recovery plans do not currently cover the specific steps or order that Tier 2 IT services will be recovered, in the event of a disaster. Instead there are generic instructions on how to apply a back-up.

- Management is aware of this issue and intend to address it once the revised list of Tier 2 IT services has been formally agreed. In the event of a major incident, including a disaster, the initial stages will be managed by Capital Jones Major Incident Management process (MIM).
- The objective of this process is to quickly understand the incident, mobilize the correct technical teams and then manage the incident to conclusion within four hours. If the incident requires the invocation of ITDR, the IT Business Continuity plan is then used to invoke recovery and then over manage the recovery detailed in the ITDR technical plan. Whilst there are links between the MIM process and the IT Business Continuity plan, they are not clear as to how one transitions into another, in terms of coordination. Additionally, whilst the ITDR technical plan specifies the types of resources it requires to execute the plan, it and the IT Business Continuity plan do not specify when and who secures them.

Risk

- If sufficiently detailed plans are not in place to support the recovery of Tier 2 IT services then the risk is that they may not be recovered in time or in a suitable operable state.
- If the manner in which MIM passes over to ITDR and then the processes to invoke and secure resources are not clear then there is a risk that recovery will be delayed, which may lead to Tier 1 IT services, in particular, missing their recover times.
- In both cases there is a risk of material impact to the council as key IT services may not be available in the agreed recovery time to enable its functions to operate key public services

Recommendation

- The flight manual should be updated to include a repeatable process for each Tier 2 IT service following an order of recovery.
- The IT Business Continuity plan should be updated so that it clearly reflects how MIM transfers responsibility to it with respect to the incident in terms

of responsibility and managing any groups or communication that MIM may have setup or started.

- The IT Business Continuity plan should be updated so that it clearly states, how and when it stands up the recovery team detailed in the ITDR technical plan

Management Response

Capital Jones staff, who is responsible for the ITDR programme has been notified for inclusion of this finding in the system. In order to cross the bridge with MIM plan, Business continuity plan and invoking ITDS steps, we have notified both MIM team and business team to conduct a meeting and resolve which duties go where and the steps to be followed. We know that the risks of this finding are high; the committee has been notified to take an immediate action for this and resolve the out of office hours IT service issue.

Another medium risk finding is as follows:

c) A full ITDR test has not been carried out:

Whilst project testing has been executed, a full ITDR test has not been carried out. Management has agreed the scope of the test that will be executed following the transfer of the programme to business as usual, which whilst more comprehensive is not a full test. We understand, given the technical setup that executing a full test may not be feasible. The risk is that without a comprehensive testing programme that the recovery will not operate as planned when needed, which could lead to IT services being recovered later or in a state that cannot support the council. The impact would be that council functions would not be able to function and this could materially impact the provision of public services

- As part of the ITDR project, Capital Jones has carried out unit tests on different aspects of the technical recovery.
- These tests were controlled adequately, with defects being identified and then scheduled for resolution.

- The Council and Capital Jones have discussed the scope of the ITDR test, which currently involves moving a number of services to the secondary site and operating them there for its duration. Whilst this is useful test, it does not test an en-masse recovery (where everything is tested together)

Risk:

- If ITDR processes and technical capability are not tested sufficiently then there is a risk that if there is a disaster ITDR enabled services may not be recovered
- This could materially impact as IT services may not be available in the agreed recovery time to enable its functions to operate key public services.

Recommendation:

- We strongly suggest an en-masse test for recovery where all the units are tested together as a system.
- In absence of an en-masse test the test regime should consist of the following ongoing basis:

1. Execute the agreed test.
2. Run SRM tests on a quarterly basis.
3. Conduct table table-top walkthroughs of the entire recovery, starting at the MIM process, through invocation and technical recovery on six monthly basis.

Manager Response:

Our infrastructure is shared with other clients and hence isolating the second data center for test is not possible in case of an en-masse test. Although, we do understand the severity of this finding and the committee has been notified to take an immediate action for this.

3. Effective communications with clients is an issue. There is a lack of Service Level Agreements (SLAs) with Capital Jones clients

Finding

At the time of the audit there was no management initiative underway to define, implement, or monitor SLAs with business clients of Capital Jones. As a preliminary step to start to address the need for tools to handle service requests better, a Capital Jones initiative exists to obtain and install technology to allow a consolidated database to be created reflecting client service requests and Helpdesk calls. At the time of the audit no projects existed to create and manage a services catalogue and service level agreements. The Helpdesk and IT Services outsourcing contracts are not part of a regular review reflecting changing business needs in the Agency. Interviews with Capita Jones clients revealed general dissatisfaction with services provided and with service levels.

There is a lack of an effective process in Capital Jones to deal with client service requests. Ineffective communications with clients has led clients to believe that they must prepare business cases for requests whether minor or major. We expected that rigorous business cases would be required for adding new services to the catalogue and for any deviations from the catalogue of agreed services or predetermined service levels, whereas use of defined and agreed services within agreed service levels should not require such a business case. Clients are not aware of any documented Capital Jones client service philosophy.

Recommendation

It is recommended that Capital Jones establish a process to develop a catalogue of defined and agreed services, and to establish mutually agreed service levels within the context of legislation, policy, and budgetary capacity. This should include monitoring, reporting and reviewing services and service levels with clients. Independent surveys that test services and service levels should be part of the process.

Manager Response

Agree. The absence of a project to define a service catalogue and SLAs is consistent with Capital Jones's focus on stabilizing the infrastructure, staffing the organization and imbedding IT best practices as foundations to delivering and improving service. An initiative will be started to establish such a catalogue and appropriate SLAs as part of its deliverables.

4. Significant service desk issues occur when incidents are reported

Analysis

Helpdesk and Incident Management have been in place since 2015. The Helpdesk is outsourced and 1st, 2nd, and 3rd level support escalation procedures are defined. Individual incident reports are escalated as problem reports if many similar incidents are reported.

Clients told us of various service desk issues:
• Poor response to an incident report at the service desk,
• Lack of root cause and trend analysis, and
• Lack of timely, effective communications between clients, IMTB staff and Helpdesk staff concerning root causes.

The Helpdesk outsourcer executes a brief survey of clients on selected closed incidents. The survey results are summarized in regular reports to IMTB. The stated goal is to have 90% of the clients satisfied or very satisfied with the handling of the incident. According to the outsourcer, approximately 70% of calls are resolved by the 1st level support at the Helpdesk.13% of calls are abandoned. There is no estimate of the number of users that do not bother to call Helpdesk. Daily, incidents reported to Helpdesk are noted within ISD if appropriately escalated and the relevant ISD teams are notified of a problem requiring analysis. The incident count reported to Helpdesk in 215 is approximately 170 per day. There is little formal incident management in IMTB beyond the Helpdesk incident summary report produced daily by the outsourcer and lessons learned are captured from incidents informally. Ad hoc and regular reports are prepared on the request of the CIO for problems. Reports on Helpdesk incident activity are produced for management, but they are not analyzed or evaluated by senior management so as to address trends. Helpdesk staff is not regularly supplied with information by IMTB. Providing information to the Helpdesk could facilitate better 2-way communication with IM/IT users. Helpdesk may not have been informed by IMTB unless they had received incident reports from other clients.

Recommendation

It is recommended that Capital Jones establish a process to develop a catalogue of defined and agreed services, and to establish mutually agreed service levels within the context of legislation, policy, and budgetary capacity. This should include monitoring, reporting and reviewing services and service levels with clients. Independent surveys that test services and service levels should be part of the process.

Manager Response

Agree. The absence of a project to define a service catalogue and SLAs is consistent with Capital Jones’s focus on stabilizing the infrastructure, staffing the organization and imbedding IT best practices as foundations to delivering and improving service. An initiative will be started to establish such a catalogue and appropriate SLAs as part of its deliverables.

Conclusion

Although diligent and important efforts have been made over the past few years to get all processes in line and in compliance with all policies and regulations and to meet industry best practices; controls, processes and practices show significant areas in need for improvement. Johnson Yang has initiatives underway that are intended to address these deficiencies if carried through full agency support.

Acronyms and Abbreviations

Acronym or abbreviation	**Description**
ROE	**Return of Equity**
FCRA	**Fair credit reporting act**
FDIC	**Federal Deposit Insurance Corporation**
FRB	**Federal Reserve Bank**
FFIEC	**Federal Financial Institutional Examination Council**
SOF	**Summary Of Findings**
RIF	**Reduction in Force**
RTO	**Recovery time objevtive**
RPO	**Recovery Point Objective**
MIM	**Major incident management process**
ITDR	**Information technology disaster and recovery**
SRM	**Site recovery manager**
SLA	**Service Level Agreement**
ISD	**International Subscriber Dialing**
IMTB	
IM/IT	**Information Management/ Itformation Technology**
CIO	

Reference

http://documents.worldbank.org/curated/en/619321516726670360/pdf/LIRENAP-audit-report-Final-13-12-17-002.pdf

https://www.dob.texas.gov/public/uploads/files/Applications-Forms-Publications/Publications/auditrpt2016.pdf

https://annualreport.deutsche-bank.com/2017/ar/supplementary-information/auditors-report.html

https://www.slideshare.net/jkyriazoglou/published-audit-report-model-and-sample-2

https://audit.wa.gov.au/wp-content/uploads/2018/08/report2018_14-IS-GCC-App-Pass.pdf

https://www.cima.ky/upimages/commonfiles/StatementofGuidance-InternalAudit-Banks_1516379814.pdf