Field Project Part 1 - Group Assignment

Scotiabank

Ayokunle Oluwole, Chinonyelum Melvina Nwanna, Melvin Obioha,

Haris Jameel, Jessica Egbadon, Sonali Sagar

MGD426

Professor Francis

University of Toronto

22-11-2018

Executive Summary

This report is formulated using the interview response of three Scotiabank executives. Scotiabank offers traditional and modern banking services, both in-person and online**.** This paper will seek to identify their banking services geared towards the user-end and provide recommendations based on our analysis. Our team chose to conduct interviews with people across the corporate ladder at Scotiabank to get a broader view of their services and associated risk issues. We met up with three Scotiabank employees, Leoreta Frrokaj, who is a Universal Banker employed at a local branch, Anthony Afolabi, an Associate Director for Business and Data Strategy from the head office, and the third employee was an Operational Risk Officer (name is being withheld due to a privacy request).

Based on primary research interview question and literature review secondary research, the report was properly structured and concluded. Some interview questions were focused on day-to-day departmental and cross-functional risks, and the remaining questions were catered to the employees' knowledge of overall risk assessment and management practices. Through compiling all the accumulated information, there is a produced documentation of the key learning points, current plans and strategies, knowledge of the severity and impact of some of these risks on digital and non-digital industry spaces, and future recommendations for Scotiabank. These are important aspects noted in the banking industry because of the continued increase in innovative technology. The delivering of pristine customer service will define the banking industry for the next few years. As a result, it is knowledgeable to be able to conduct a field project and gain insight, which will continue to be relevant and essential in the future.

Key Learning Points

Scotiabank is a large multinational bank headquartered in Toronto, Canada, with approximately 25 million customers, and offers a range of products and services including banking, investment, and wealth management activities. By interviewing three Scotiabank employees at various corporate levels, major overlapping risks, personal and professional views on risk management are identified. These interviews were focused on the end user of their financial products and services:

Internal Data Security (Hacking)

Digital banks deal with large amounts of sensitive data being transferred through various channels. With online channels increasing rapidly, new types of potential security issues such as hacking, and data breaches can result in the loss of private banking and customer data. Scotiabank takes this issue seriously; they have no major breaches till date. During the interview with the Universal Banker, Leoreta Frrokaj, the recent hacking of *Equifax's* data was brought up, along with what it implied for Scotiabank's own security systems. The breach "in which millions of customer's data was released to people intending to do harm with it", proved that banking information could be hacked by third party companies like Equifax (see appendix B). Therefore, this requires Scotiabank to review their security measures, and enhance security on their data collection procedures and storage.

External Data Security (Phishing)

While Scotiabank itself can keep its data secure through internal multi-layered security, the security at the customers end remains difficult to control. According to the interview with

Ms. Frrokaj, there has been occurrences of clients mistakenly disclose sensitive data to scammers through emails or messages, leading to issues such as fraud and identity theft (see Appendix B). Scotiabank tries to prevent this through continually making users aware of these threats and ways in which to prevent them. However, once the fraud occurs, Scotia Bank has a fraud department, which "is able to verify whether or not the client was complicit in the fraud by determining where it occurs and how it occurs" through the use of technologies that aggregate various factors and track regular transaction patterns" (see appendix B).

Technical Issues

Web-based and software issues such as accidental server shutdowns, website malfunctions, finance system errors, and general network issues. These issues could cost banks large amount of money and create unease for the customers. The Operational Risk Officer interviewee (name withheld) revealed that Scotiabank does have procedures for the likelihood that these problems do occur, through mitigating technical issues via capacity, business continuity, and contingency planning to ensure availability of banking systems and service (see Appendix C). The main areas where managers typically tend to focus is on the scalability, compatibility, and accuracy of the functionality of the implemented technology.

Data Protection Issues

There are risks associated with the daily tasks being completed and new technology being utilized in the company. Scotiabank's customer data must be protected across the digital ecosystem. For banking institutions, data is power. If a customer feels like their information is not properly protected, they could easily take their business to another financial institution. As a

result, there should be a key focus on trying to control areas that would include data classification, data processing, data encryption, and data retention. As evident during the recession, it is essential to keep customers at ease.

Third party Outsourcing and Solutions Risk

According to the interview with the Operational Risk Officer, Scotiabank has previously used Fintech in credit risk underwriting partnerships to aid with fraud detection and regulatory compliance. As a result, Scotiabank would need to properly analyze the technology to make sure it will positively impact the business in the finance sector (see Appendix C). Furthermore, if these third-party solutions are not checked appropriately for quality, risk mainly occurs due to inappropriate control of third-party vendors. Regarding this type of risk, the areas that needs to be focused on include internal data sharing, technology integration, vendor resiliency, and operations dependency.

Poorly Defined Scope

According to the interview with Mr. Afolabi, a defined scope is an internal process that includes people, data, or systems (see appendix A). Since a project involves various people across different functions, one small error could cause all other work to stop and going back to fix those errors could take a lot of time and money (see appendix A). In order to prevent this, it is essential that the project scope is outlined. The quality is maintained throughout the life cycle of the data use (see appendix A). All errors and discrepancies are communicated effectively to all relevant employees, so that work does not stop, and people can create a contingency plan to deal with the risk in a timely manner.

Security Guidelines

According to Ms. Frrokaj, the rationale behind Scotiabank giving customers a variety of tools to better deal with risk is, if the customer can take a proactive role in preventing security risks, it benefits both parties (see appendix B). One of tools administered is offering a free *McAfee antivirus* software to their customers. This prevents hacking and security breaches on hardware with sensitive banking data. Also, Scotiabank's website has a dedicated space to help inform their customers of everything they need to know about data security (Scotiabank, "Computer Security", n.d.). Overall, this shows that Scotiabank takes steps towards identifying and preventing risks, and go beyond just their own systems, by helping customers learn about and secure their own systems.

Literature Review, Analysis, and Recommendations

To effectively review and analyze the key learning points of the digital and non-digital industries, their defining characteristics must be known. Digital industries, or increasingly digital hybrid industries, refer to business sectors that implement core "intangible", online or cloud-based, software tools into their business model (König, Ungerer, Baltes, & Terzidis, 2018, p. 4). For example, online banking, marketing or advertising, social media, and cloud-based software or mobile application companies are part of the digital industries. Non-digital industries, or largely non-digital hybrid industries, refer to business sectors that have a "tangible" hardware, or physical machine-based, business model (König et al, 2018, p. 4). For example, brick-and-mortar (traditionally physical) retail stores are non-digital. Also, General Electric,

Schneider Electric, Siemens, and other industrial companies are examples of largely non-digital hybrid companies.

Digital Industry Literature Review

Digital industries, or largely digital hybrid industries, are project and product management intensive industries "capable of building, testing, and supplying a digital product or a service to the market that immediately creates revenue" (König et al, 2018, p. 7). Unlike non-digital industries, digital industries do not require large "tangible" (physical) financial investments (e.g. property, plant, equipment - PP&E). König et al (2018) accurately states that it is not a "precondition for their market growth". For example, a startup cloud-based software or mobile application company could begin operations with a few remote employees. Therefore, the company does not pay extra rent, property tax, utility, and other associated costs. König et al (2018) explains that "early-stage ventures trying to fundraise investment for an idea seems to be rejected by the innovation system...the innovation system learned from the burst of the dot-com bubble: do not invest in untested business models". Instead, current early-stage digital companies focus on defining its target market, customer acquisition, and transactions (gradual retentions) before searching for tangible financial investments. For digital companies, financial investments are usually acquired through "innovation intermediaries" like angel investors, shareholders, government grants, or bank loans, which is usually the last resort (König et al, 2018, p. 8).

Non-digital Industry Literature Review

Non-digital industries, or largely non-digital hybrid industries, are "hardware and asset-oriented industries" (König et al, 2018, p. 7). These small businesses and hardware giants

(e.g. brick-and-mortar retail stores, General Electric, Schneider Electric, Siemens) require a costly market entry, financial, and performance risk management because of the reliance on depreciating physical assets, patenting activities, and post-financial activities (e.g. rent, property tax, utilities, plant or land maintenance, and equipment diagnostics and repair). Unlike digital companies, for value creation, these fully or partial non-digital companies require instant or beforehand investment in "capital-intensive" fixed assets, which are both products and services (König et al, 2018, p. 7 - 8). Examples of these types of fixed assets are in-house hardware (e.g. cash registers, ATM machines, CPUs, printers, scanners, and monitors), biotechnology developments, "automobile manufacturing, oil production and refining, steel production, telecommunications and transportation [development and maintenance], like railways and airlines" (Investopedia, "Capital Intensive", n.d.).

Digital, Non-digital, and Key Learning Points Analysis

All businesses and industries have transformed because of data, analytics and the digital tools that harness them. The banking sector is undergoing its own digital revolution with significant implications for risk management (McKinsey & Company, "The future of risk management in the digital era", 2017; Dietz, Lemerle, Mehta, Sengupta, & Zhou, 2017). McKinsey (2017) refers to an earlier digital risk survey, where it is noted that about 10% of banks have digital risk on their high-priority list and about "70% of banks have digital risk prominently on the radar, with a middling level of management attention". Similarly, "respondents indicate that 22% of banks - nearly 30% in Europe and the rest of world - have

invested more than 25% of the annual risk budget to digitize risk management" (McKinsey & Company, "The future of risk management in the digital era", 2017).

These transformations are caused by dynamic trends in areas like internal data protection and external data security. They disrupt the norms, and give a reason for change, attributing to financial and performance risk management practices:

1) Internal Data Protection (Hacking)

Digital risk management is a term used to describe all digital enablement that improve risk effectiveness and efficiency, especially process automation, decision automation, and digitized monitoring, and early warning. The approach uses workflow automation, advanced analytics (including machine learning and artificial intelligence), new data sources, and the application of robotics to processes and interfaces. Essentially, digital risk implies a concerted adjustment of processes, data, analytics and IT, and the overall organizational setup, including talent and culture (McKinsey & Company, "Digital risk: Transforming risk management for the 2020s", 2018).

For digital companies, internal data protection includes the use cloud-based data storage and computing. For non-digital companies, internal data protection may include backing up data on hardware like monitors, printers, CPUs etc. The digital and non-digital companies are similar because there is a need for data protection in both cases. These practices individually secure data but work best together.

2) External Data Security

For digital companies, or hybrid companies, consumers and businesses so accustomed to personalization through social media and rapid fulfillment through e-commerce. They expect the same kind of near-instantaneous service and customized products from their banks (McKinsey & Company, "The future of risk management in the digital era", 2018). However, some customer-targeted data threats include “phishing”, “smishing” and “vishing” (using telephone communication, emails, and voicemails to steal people’s personal information). Scotiabank constantly warns consumers against them and offer security guidelines. For non-digital companies, or hybrid companies, external, customer-targeted, data risks may include ‘old-fashioned’ (in-store) identity theft through stolen laptop and mobile devices, government ID cards, debit and credit cards. Also, another identity or data theft technique is the close observation and retention of significant financial and contact information. A non-digital company can counter identity theft risk by implementing data barriers, so customer cannot see or hear inputted data (e.g. queue line barriers, debit and credit card swipe machines with barriers that stops snooping eyes).

Like in the internal data protection digital and non-digital methods, external data protection practices for digital and non-digital companies individually secures data but work best together.

Recommendations

Digital and non-digital industries have differences regarding how they approach businesses activities. Digital industries display greater financing activities when approaching the market entry stage because it is required to have an initial investment in assets, which creates value for

potential customers. Digital industries do not tend to rely on these tangible financial activities, but "focus initially on developing transactions with their customer before searching for investments" (König et al., 2018, p. 8). These businesses can build and supply a product or service that is digital to the market, which will instantly create profits for them.

Scotiabank is in the digital industry, having both digital and nondigital (hybrid) characteristics. The company has been successful regarding their day-to-day objectives. However, some traditional methodologies, which is mostly associated with full non-digital industries, could be useful for the company:

1) Improving Tangible Investments

The idea of investing heavily during the market entry stage should be considered when developing strategies for the company. It is indicated that digital companies do not need this procedure. However, it is something to consider regarding investing in capital-intensive fixed assets such as in-store products and services. The ATMs, printers, scanners and monitors are examples of products used in the bank, which can be improved on. People tend to complain become some of these products can be very slow. This usually leads to a lineup, which makes customers angry and overall affects perception of customer service quality. If Scotiabank can invest more in these products and include up-to-date systems for each branch, they will be more productive.

2) Increase in Patent Activities

Another recommendation would be to invest in patent activities. Non-digital companies are very fond of spending heavily on patent activities when starting up. It is confirmed that these

activities lead to more success and less legal disputes for the companies. Based on Scotiabank's computer science and management resources, inventing unique products or services that can help them increase their competitive advantage over banking competitors has proven to be achievable for Scotiabank. Patenting activities is good because it gives the bank ownership and entitlement to a product or service (invention) for a specified period. This is a factor non-digital companies consider when creating their tangible strategic benefits.

3) Balanced Hybrid Methodologies

Scotiabank should not to digitize everything in the company. According to Newman (2018), companies tend to digitize everything when approaching the digital world and it ends up backfiring for them. He believes that "it is critical to understand the consequences that come from a failed digital transformation. Businesses will suffer in more ways than one: Loss of revenue, loss of productivity and loss of time" (Newman, 2018). Newman (2018) indicated that companies should think about what in their workflow must be improved by digitization, then start from there without venturing too far. Scotiabank could consider this procedure by focusing on the areas that are mainly needed for digitization in their branches (e.g. online banking activities), then analyzing the results to improve on them.

Task Summary

In doing this project, the whole team contributed to writing the report successfully. We decided to choose what we wanted to do and gave ourselves deadlines to make sure it done. For example, we had to list three companies where we have connections, come up with candidates to

interview, draft email and in-person interview questions, and sent it. We identified three companies, which are IBM, DAC Group, and Scotiabank, and reached out to them. Next Sonali, Melvina, and Haris came up with the interview questions. After forming the questions, we had to draft and email. The emails were constructed to make sure those who read it are confident that the interview would be confidential (see Appendix D). After a few days, we decided to go with three Scotiabank executives. All three candidates were the first to reply promptly.

We interviewed Miss Leoreta Frrokaj, who works as a universal banker at the Port Credit Scotiabank branch, Mr. Ayobami Anthony, who--until last week Monday--was the Associate Director of business and data strategy, global banking markets, in the headquarters downtown, and the last candidate, who wanted to stay anonymous, is the Operational risk Assistant Manager. Ayokunle, Haris, and Sonali decided to interview each candidate and provide their transcripts (see Appendix A, B, and C). The transcripts helped the other group members understand what was discussed during the interviews. Once we successfully interviewed each candidate, we sent a follow-up email to thank them for taking their time and trusting us with their answers. Finally, we used these answer in the construction of the final report, which was written and edited by all the group members (see Appendix E).

References

Dietz, M., Lemerle, M., Mehta, A., Sengupta, J., & Zhou, N. (2017). *McKinsey & Company.* Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/remaking-the-bank-for-an-ecosystem-world

Investopedia. (n.d.). Capital Intensive. *Investopedia.com*. Retrieved from https://www.investopedia.com/terms/c/capitalintensive.asp

König, M., Ungerer, C., Baltes, G., & Terzidis, O. (2018). Different patterns in the evolution of digital and non-digital ventures' business models. *Technological Forecasting and Social Change*. doi:10.1016/j.techfore.2018.05.006

McKinsey & Company. Digital risk: Transforming risk management for the 2020s. (2018). Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/digital-risk-transforming-risk-management-for-the-2020s

McKinsey & Company. The future of risk management in the digital era. (2018). Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era

Newman, D. (2018). 3 Ways Companies Are Messing Up Digital Transformation, and 3 Steps To Fix It. Forbes. Retrieved 20 November 2018, from

https://www.forbes.com/sites/danielnewman/2018/05/24/3-ways-companies-are-messing-up-digital-transformation-and-3-steps-to-fix-it/#2ab521ad2794

Scotiabank. (n.d.). Computer Security. Scotiabank.com. Accessed from https://www.scotiabank.com/ca/en/0,,5773,00.html

Appendix A

Interview with Anthony Afolabi

My name is Anthony Afolabi up until last week Monday, I was the associate director for Business and data Strategy worked with the global banking markets. In a nutshell, I oversee the progress, application, and strategy of data management principles, protocols that are of utmost importance to the Enterprise data management policies. In a summary, Scotiabank's digital service from my end is fast growing. Each day there is something to look forward to. As we get new international students trusting us with their account, to stakeholders seeing the technological advancement we make each quarter, it is important to note that this is what drives the business and everyone to be successful. I manage the critical data element inventory to make sure there is a glossary used for those who need it as well as making precise and relevant information glossary that is easily accessible for those in banking. In some simple terms, Scotiabank has grown from when I started to this big global giant who is not afraid to operate and lead in the digital space. Because in our day to day business, we must rely on a uniform and sustainable technology. Dealing with risks are very important because I deal with data. And data is useful information. It is information the company would use, it is information those in retail banking would use, those in the upper management as well as anyone who works within Scotiabank and those who would transform the data into useful information.

There are mainly 2 types of risks I deal with: operational risk, data risk – compliance risk.

The first risk is having to deal with a poorly defined scope on the internal process such as people, system, data. Etc. Having to deal with risks like this is very important because one wrong

number in the datasheet can lead to multiple errors within the organization and trying to find the error takes up problems for those around and those who want to use the data. Having said this, this risk is a problem that can affect Scotiabank. Having a failed process allows a bad reputation and leads to incompetence, which affect how a job function is done and leads to data mismanagement. Which brings me to my second point data risk. To be more specific, Compliance risk. Because I work with data, the quality must be of high standards and of great use. A result in the failure to meet data quality results in sanction and problem for Scotiabank. Because we promise you're richer than you think, it is important to give that mindset that data released, recycled and reused is of great quality to ensure everyone does their job right while providing an articulate service.

Because I work in the data side of the business and the global market, I have no idea what goes on in the cloud, but I know that we all collaborate with each other to generate get and useful information. A blind spot that is very important is that of technology and data. Because we live in a technological world, technology is always going to be evolving and what better way is there than to evolve with technology as it grows. Many companies so I've heard would don't fully realize the importance of a new technology. it is better to hop on the technology than waiting for its full potential.

Appendix B

Interview with Leoreta Frrokaj

<u>What are your roles and daily tasks at Scotiabank?</u>

My current role within the bank is meeting every client's sales and service needs. This ranges from answering any customer issues and aiding them in any digital demonstrations but I also assess the bank's risk in providing certain customers with banking products. Since I am oftentimes opening accounts for clients, I have to introduce them to our online banking, so I mention risks associated with banking online and ensure they are protected by our offer of free McAfee protection.

Briefly highlight Scotiabank's digital services?

We provide accessible online banking services to all our clients where they can see their account numbers and balances at all times of the day. Not only can they see the balance, they also have access to their previous statements for the last 18 months, see their updated credit score which is retrieved on a monthly basis, send email money transfers and Western Union transfers and apply for new products with the bank. Scotiabank also provides InfoAlerts, which allows clients to choose whether they want to receive texts/emails regarding their activity. Our digital services provide an extensive amount of services, but they also hold an extensive amount of information about a client at any given moment.

Do you deal with risks in your department/job tasks? How do you assess and manage those risks?

I primarily assess the risk of providing a new or existing client with products. This is associated mainly with loaning new client's money in the form of a credit card or overdraft protection. I must assess this risk adequately since it impacts the success of the bank overall. Moreover, because my desk is in an accessible space, I also must make sure that I am not risking

a client's data safety by ensuring that no one else can see my screen and no client information is left lying around where other people can access it.

Furthermore, I must consider the risk to the client in terms of their online banking as there is high risk for security compromises to a client's data due to phishing and other scamming methods. I mediate this by informing clients of our InfoAlerts, McAfee services and frequently used scamming techniques in order to ensure they are protected from potential fraud.

What are top risks in the company (in digital space). How severe is the impact and how often do they occur?

As mentioned, the major risk is the loss of customer data. This is especially important after the Equifax hack in which millions of customer's data was released to people intending to do harm with it. Luckily, we have not had any hacks into our personal system as we do have teams of people to protect our clients from this data breach. At a client level, there is more risk as the company cannot determine what actions a client will take, or the risk associated with that action. Since clients are susceptible to believe in scammers who send text messages or job offers that ask for online banking information, the bank needs to ensure that it is monitoring activity online to prevent fraud and theft of client data. Scotiabank personally has messages on online banking services which informs users that the bank will not text you or ask for your information over the phone which helps to a certain extent. This however, does not mitigate all risk as clients may still overlook this information and expose themselves to immense levels of personal risk and bank loss.

What current risk assessment practices does Scotia bank undergo (e.g. in-person, cloud-based software, collaboration/management tools)?

As mentioned, we do provide McAfee for free to avoid from common phishing techniques and provide notifications online when we see large bouts of fraud occurring. As well, we have new techniques which allow our department to better detect fraud so that people don't have to contact us before travelling. When fraud does occur, we have a fraud department which is able to verify whether the client was complicit in the fraud by determining where it occurs and how it occurs through consistent tracking of regular transaction patterns. The bank also allows customers to receive text messages for every single purchase that they make t help mitigate extreme levels of fraud as a client can inform the bank of the fraud immediately.

Briefly highlight "corporate blind spots" that need constant risk management attention?

While risk is often mitigated through advanced fraud detection services, I think there should be a program that is implemented for everyone who does online banking that will inform clients of current fraud techniques and how to avoid them. As well, the employees are not always notified of new techniques so when clients come in dealing with fraud, if the employee is not aware it is fraud, there is higher potential for it to occur.

Furthermore, I think they need to implement better security measures around current employee email services because there have been many instances where employees have received fraudulent emails to their personal work email. This can be dangerous because if the employee is unaware of the fraudulent techniques, they may become a victim as well and put the bank at a higher risk.

Appendix C

Interview with the Operational Risk Officer (Name withheld due to privacy request)

Some thoughts that I think that you should know:

The Bank of Nova Scotia created a new unit called Digital Factory to pursue innovations in tech and mobile banking. Digital Factory will bring together a network of teams, all focused on transforming the way the bank delivers service to its customers globally. They also partnered with fintech companies and startups outside the bank. Technology's role in delivering a superior customer experience will define banking for the next five to 10 years.

Role and Daily tasks at Scotia bank?

Sound Security Control Practices for E-Banking:

Scotiabank has practices in places for example specific authorization privileges assigned to all users of e-banking systems and applications, including all customers, internal bank users and outsourced service providers. We also employ logical access to support proper segregation of duties. E-banking data and systems are classified based on sensitivity and importance and protected accordingly. There are also appropriate mechanisms, such as encryption, access control and data recovery plans to protect all sensitive and high-risk e-banking systems, servers, databases and applications. In terms of storage of sensitive or high-risk data on the organization's desktop and laptop systems are all minimized and properly protected by encryption, access control and data recovery plans.

Sound Practices for Managing Outsourced banking Systems and Services:

Scotiabank has appropriate processes for evaluating decisions to outsource e banking systems or services. Bank management must clearly portray the, benefits and costs associated with outsourcing arrangements for e-banking with third parties. It also needs to be a clearly defined business need and recognize the specific risks that outsourcing entails. The bank conducts appropriate risk analysis and due diligence before selecting an e-banking service provider. Scotiabank ensures that adequate resources are provided to oversee outsourcing arrangements. In terms of documentation of the risks there are procedures used to notify the bank of service disruptions, security breaches and other events that pose a risk to the bank and should be spelled out. Performance expectations, under both normal and contingency circumstances, are defined. We conduct independent reviews, audits of security, internal etc. This is in the case of outsourcing we have appropriate contingency plans for outsourced e-banking activities.

Briefly highlight Scotia bank's digital services?

Mobile deposits, e-receipts, PayWave and Mobile wallet which is for Android devices and Apple Pay for iPhones. It applies the same principle as a PayWave. Lastly, we provide e-statements.

What are the top risks in the company (in digital space)? How severe is the impact when they occur?

The risk framework that we follow but where we could also improve on:

There are procedures in place for the safeguarding of data at the core. This is in order to try and prevent from data Leakage as well as to Ensure the protection of data across the digital ecosystem at various stages of data life-cycle–data. There are some areas where we need to

focus which would include data classification, data retention, data processing, data encryption. For example, as I previously mentioned using fintech Reviewing the integrity of fintech and third-party solutions are integrated into the bank's solutions. For example, we have used FinTech's in credit risk underwriting partnerships, fraud detection, and regulatory compliance or supervisory reporting. In terms of Cyber Security risks some key controls may include platform hardening, network architecture, application security, vulnerability management, and security monitoring. There is also the potential of fraud risk such as identity theft. The rise of analytics requires risk managers to pay close attention to model risk. There is also reputational risk which has an impact on brand value and the company's overall reputation. Social media and other platforms are key in terms of trying to maintain a good reputation. There is also technology risk some of the key risk areas include scalability, compatibility, and accuracy of the functionality as well as implemented technology.

What current risk-assessment practices does scotia bank undergo?

1. Effective management oversight of e-banking activities.

2. Establishment of a comprehensive security control process.

3. Comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies. Scotia bank has a clear Vendor Management policy and processes.

4. Security Controls

5. Authentication of e-banking customers

6. Data integrity of e-banking transactions, records, and information.

7. Focus on Legal and Reputational Risk Management

8. Privacy of customer information.

9. Incident response planning and crisis management

Appendix D

Email Templates and Interview Questions Sent to Interviewees

Email Template

Hello_____,

My University of Toronto DEM student group is doing a risk management (CRO) project on ___. We would like to ask a few questions on ___ risk assessment and risk management. This is a simple student-based management project, so it will not be shared publicly, and our written student essay can be sent to you if requested. We would appreciate your involvement in the assignment by answering a few simple questions about your role at ___. We would like to send you the questions, which you could respond to via email, or through a phone call. I hope you are interested. Please respond with how you would like to be contacted.

Thanks,

NAME

Phone: _____

Email: _____

Interview Questions

1. What is your role and daily tasks at Scotiabank?
2. Briefly highlight Scotiabank's digital services?
3. Do you deal with risks in your department/job tasks? How do you assess and manage those risks?
4. What are the top risks in the company (in digital space)? How severe is the impact and how often do they occur?
5. What current **risk assessment practices** does Scotia bank undergo (e.g. in-person, cloud-based software, collaboration/management tools)?
6. Briefly highlight "corporate blind spots" that need constant risk management attention?
7. What risk assessment and management procedures do you think Scotiabank's should consider in the next few years?
8. What key challenges did you face in Scotiabank in terms of risk

Sent emails to:

IBM - Leenah Hassan (Consultant), Christine Samuel (UX Director), Tobias Woerthle (Senior Technical Analyst), and Karel (Director of IBM Design)

Scotia Bank - Mr. Anthony Afolabi and Leoreta Frrokaj

DAC GROUP - Laura Hincapie, Justin Teng, and Martin Siemsen

Appendix E

Table Identifying the Tasks of Each Group Member

TEAM MEMBER	ROLES	TASK
Sonali Sagar	Prepare interview questions, find potential candidates: IBM, Find potential candidates: Scotiabank Report: Executive Summary and Key Learning Points (about risk management practices)	Highlight important interview questions to ask, interview candidates, and write assigned report section.
Haris Jameel	Interviewing candidates, prepare email draft, find potential candidates: Scotiabank Report: Executive Summary and Key Learning Points (about risk management practices)	Edit email draft, interview Candidates, and write assigned report section.
Ayokunle Oluwole	Interviewing candidates, find potential candidates: Scotiabank Find potential candidates: DAC GROUP Report: Executive Summary and Task Summary	Edit email draft, interview candidates, and write assigned report section.

Chinonyelum Melvina Nwanna _____ Melvin Obioha _____ Jessica Egbadon	Prepare interview questions, interviewing candidates, prepare email draft, find potential candidates: IBM Report: Literature Review, Analysis, Recommendations, and editing draft _____ Report: Literature Review, Analysis, Recommendations, and editing draft _____ Report: Literature Review, Analysis, Recommendations, and editing draft	Edit email draft, interview candidates, and write assigned report section. _____ Write and edit assigned report section. _____ Write and edit assigned report section.
All members	write report	complete team report before the 16th.