Request for comment on 'Proposed Interagency Guidance on Third-Party Relationships: Risk Management'

October 15th 2021

Docket No. OP-1752

Ann E. Misback

Secretary

Board of Governors of the Federal Reserve System

20th Street and Constitution Ave., NW

Washington, DC 20551

RIN 3064-ZA26

Mr. James P. Sheesley

Assistant Executive Secretary

Attn: Comments-RIN 3064-ZA26

Federal Deposit Insurance Corporation

550 17th St., NW

Washington, DC 20429

Docket ID OCC-2021-0011

Chief Counsel's office

Attn: Comment Processing

Office of the Comptroller of the Currency

400 7th St. SW., Suite 3E–218,

Washington DC 20429

Subject: Request for Comment on 'Proposed Interagency Guidance on Third-Party Relationships: Risk Management'.

Dear Administrators,

We welcome the opportunity to comment on the 'Proposed Interagency Guidance on Third-Party Relationships: Risk Management'[1]. We organized our response as follows:

I. **Introduction**

II. **Third-Party Taxonomy and Third-Party Risk**

III. **Cost Terminology**

- Cost Types
- Cost of Risk Levels

IV. **Methodology and Business Arrangement Examples**

- Contract Management & RACI-chart
- Priority Critical Risks & Cross Cutting Risks (PCR & CCR)
- Supply Chain Risk (SCR) Mitigation Budget from Best Case to Stress test
- Business Arrangement 1 - Second-Party Credit to Third-Party Supply Chain for Bicycle Import
- Business Arrangement 2 - Third-Party Outsourcing of Cloud Services
- Business Arrangement 3 - Third-Party Outsourcing of Cleaning Services

V. **Summary Conclusions**

VI. **Comments and Recommendations on 'Proposed Interagency Guidance on Third-Party Relationships: Risk Management'**

VII. **Authors**

VIII. **Appendices**

Please share our response with your respective agencies

[1] *The proposed guidance describes third-party relationships as 'business arrangements between a banking organization and another entity, by contract or otherwise'*. Proposed Interagency Guidance on Third-Party Relationships: Risk Management Federal Reserve System, Federal Deposit Insurance Corporation and Department of the Treasury (Office of the Comptroller of the Currency), 2021.

I. Introduction

The awareness of supply chain risk[2] (SCR) has dramatically increased during the current pandemic and continues to frustrate corporations, consumers and oversight bodies alike. There is a need for more sophisticated risk measures to manage third-party risk as we increasingly rely on an interconnected global system for delivering products and services and to handle any associated risk along the way. Recently exposed supply chain vulnerabilities include supply chain choke points[3] which were well known before they started to severely impact global supply routes, yet for different reasons remained poorly mitigated. This in turn led to systemic risks ripple effects with quadruple container costs[4], goods price hikes and looming inflation threats.

There are multiple interpretations of third parties, third-party business arrangements and third-party risk among the risk community, business community and supply chain communities. Supply chains are also defined in various ways and the sourcing, procurement and logistic communities have all come up with relevant definitions. In its simplest form, a supply chain is '*the activities required by the organisation to deliver goods or services to the consumer'*[5]. For example, a product supply chain typically consists of a third-party vendor with a fourth-party manufacturer, a fifth party component supplier and a sixth-party raw material supplier but could extend as far back as say the 10th party and beyond.

A fourth party in the banking space may provide services to say a third-party fintech company and therefore the fourth party is a part of a supply chain such as a cloud servicing company providing critical services to the fintech company. These critical activities include significant bank functions such as payments, clearing, settlements, custody and shared services such as information technology services that could cause a bank to face considerable risk if a third party fails to meet expectations and could have a major bank customer impact.

---

[2] We will throughout our response use Supply Chain and Third-Party arrangements interchangeably.

[3] Medunic, P., A glimpse of the future: The Ever Given and the weaponisation of choke-points. European council on foreign relations, 2021. https://ecfr.eu/article/a-glimpse-of-the-future-the-ever-given-and-the-weaponisation-of-choke-points/?amp

[4] Page, P., Container Shipping Prices Skyrocket as Rush to Move Goods Picks Up. The Wall Street Journal, 2021. https://www.wsj.com/articles/container-ship-prices-skyrocket-as-rush-to-move-goods-picks-up-11625482800

[5] Supply Chain can be defined in many different ways and the sourcing, procurement and logistic communities have all come up with relevant options. For the purpose of this paper, we chose a most simple and broadly applicable one: *'In its simplest form a supply chain is the activities required by the organisation to deliver goods or services to the consumer.'* Chartered institute of procurement and supply. What is a Supply Chain? CIPS, 2020. https://www.cips.org/knowledge/procurement-topics-and-skills/supply-chain-management/what-is-a-supply-chain/

A well calibrated common terminology is a key to establish a best practice third-party risk approach. Terminology that is independent of which business sector is being addressed reduces any misunderstanding in terms of the communication among the banking sector, its regulators and any concerned stakeholder.

Many corporate key functions in a supply chain are being outsourced to new technology companies to more cost efficiently provide essential services and the ability to stay ahead of the technology curve. Specialized technology company solutions are usually far superior compared to an in-house solution such as generally providing superior data security and recovery systems. For example, cloud based services can be divided into multiple broad 'as a service' categories but there are risks associated with relying on each of these 'as a service' categories.

These evolving technologies, together with the geographically widening scope of supply chains, expand the impact that emerging risks such as cyber risk, a pandemic and environmental risk, have on supply chains. The need to measure and make transparent these emerging third-party risks therefore increasingly becoming a high priority. On the other hand, the interconnected nature that technology brings to supply chains should make it easier to capture supply chain risk at an enterprise level as well as potential risk areas at every step of these value chains.

The overall risk measurement and management of third-party risks would benefit from a broader, holistic view of the entire life-cycle of any third-party arrangement. We incorporate terminology commonly used by supply chain practitioners into our recommended approach. Supply chain practitioners have more extensive experience than the banking sector in monitoring third-party vendors and implementing useful performance monitoring programs. However, supply chain practitioners have a less in-depth approach to risk management and due diligence processes than banks. Our goal is to integrate the best of the banking and the supply chain worlds in order to significantly reduce the overall third-party risk facing the banking sector today.

After this brief introduction, we clarify the taxonomy and terminology surrounding third-party risk as a whole. We then present a practical risk assessment approach and risk mitigation methodology that we apply to three distinct types of business arrangements followed by our summary conclusions and responses to the 18 questions. In particular, we provide tables that illustrate our approach towards calculating risk and returns for the supply chain and making them transparent.

We hope that our approach and content will be well received and thank you for this opportunity to share our views on third-party risk and its adjacent intricacies.

II. Third-Party Taxonomy and Third-Party Risk

As mentioned in our introduction, there are multiple interpretations of third parties and third-party risk among the risk community, business community and supply chain communities. Our goal includes establishing a jointly accepted understanding of the various terminologies used during our discussion of third-party risk such as terms used by external vendors, service providers or suppliers. The variations in terminology are not always consistently applied within and between various industry sectors.

We define Kth party as described in Box 1 in order to facilitate discussion throughout our response as well as to reduce any possible misinterpretations among various communities.

First-party refers to the corporation's internal activities and should be a top priority since a bank needs to ensure that it fully complies with the same due diligence and risk mitigating demands required by any third-party relationship. Second-party relationships refers to risk exposures that flow from customers such as from lending activities.

Box 1 (Kth Party)

- First party - Refers to the internal operations of the bank
- Second party - Refers to high risk exposures to customers of the bank
- Third party[6] - Bank has a direct business supplier relationship that is commonly documented in a written agreement. Referred to as Tier 1[7] supplier among supply chain practitioners
- Fourth party - Sub-supplier to a third party (a tier 2 supplier)
- Fifth party - Sub-supplier to a fourth party (a Tier 3 supplier[8] [9])
- Kth- Party - Sub supplier to a K-1 party (a tier K-2 supplier)

[6]Venminder Experts. Who is considered a third-party or vendor?, Venminder, 2021. https://www.venminder.com/blog/who-considered-third-party-vendor

[7] 'The concept of Tier 1 suppliers is quite simple: They are the third parties you directly contract to provide goods and services that support the operations of your business.' Suarez, J. What you should know: Tier 1 vs Tier 2 supplier diversity spend. CVM Supplier Diversity Blog, 2014. https://blog.cvmsolutions.com/difference-between-tier-1-spend-and-tier-2-spend

[8] Young, S.B.; Fernandes, S.; Wood, M.O. Jumping the Chain: How downstream manufacturers engage with deep suppliers of conflict minerals. MDPI. 2019, *1-4*. https://www.mdpi.com/2079-9276/8/1/26

[9] Cramer, J.J. Sub tier suppliers are big contributors to risk exposure. Dun & Bradstreet, 2018. https://www.dnb.com/perspectives/supply-chain/supply-chain-risk-management-sub-tier-insights.html

Each bank needs to decide how deep they need to go into the supply chain to assess the amount of third-party risk. The level of depth is steered by the limits of financial and administrative feasibility as well as levels of confidentiality (such as IP) imposed by (or restricted by) all parties across the supply chain. The supply chain transparency for any product or service generally stops at areas such as:

- raw-material source for a product
- intellectual property creator
- owner of data related service concepts

A low level of priority cannot be arbitrarily assigned to any company in the supply chain without conducting a due diligence and self-assessment process to determine and compare the amount of risk. Our due diligence approach calls for:

* assessing the cost, quality and risk tradeoffs
* implementing risk measures which captures both expected and unexpected risk

for each party[10] in the supply chain. Our approach also calls for achieving a workable parsimonious middle ground between microscopic granularity and ease of executing an enterprise wide supply chain risk governance process as well as to maintain an intricate balance between cost, quality and risk.

We provide three practical business arrangement examples in section IV to support constructing good guidance to manage supply chain risk for banks. The three examples cover supply chain risk emanating from the:

- Loan Book (see Business Arrangement 1)
- Cloud services (see Business Arrangement 2)
- Cleaning services (see Business Arrangement 3)

[10] Venminder Experts. Who is considered a third-party or vendor? Venminder, 2021. https://www.venminder.com/blog/who-considered-third-party-vendor

III. Cost Terminology

Cost Types

Our cost related terminology to capture risk is as follows;

* Cost of goods sold (COGS) covers the manufactured product cost (or executed service cost) and some but not all costs to reach the point of sale or point of service[11].

* Total landed cost (TLC) includes **all** related costs to bring the item to the point of sale, including expected risk costs.

* Total cost of ownership (TCO) includes a significant portion of the operational expenses (OpEx) for indirect costs as well as a portion of capital reserves set aside for unexpected risk costs. TCO includes all cost elements in an end-to-end supply chain. Our definitions of TCO is consistent with leading authorities in supply chain methodology, for example the Association for Supply Chain Management, ASCP[12].

Cost of Risk Levels

Best Case (BC) - The stripped-down calculation of raw materials, components, labor and shipping to produce and deliver a product or a service to the end-user/consumer.

Cushion (C) - The open or hidden addition (or subtraction) to the final negotiation with each supply chain partner in order to avoid excessively frequent renegotiations of prices. It provides a certain stability for the manufacturer and other supply chain partners to absorb minor cost increases without having to contact the buyer. It is frequently added in the contract as a percentage deviation limit after which both parties would have the right to renegotiated the price. BC + C normally constitutes the bulk of all pre-negotiated cost scenarios and is budgeted on a cost account.

---

[11] Ryan, B., What Is Landed Cost? A Complete Guide. 3PL Logictics, 2021. https://www.3p-logistics.co.uk/3pl-blog/what-is-landed-cost-a-complete-guide/

[12] Eshkenazi, A. Alphabet soup: TCO, ROI and YOU. Association for supply chain management, 2017. https://www.ascm.org/ascm-insights/scm-now-impact/alphabet-soup-tco-roi-and-you/

Cost Increase Expected Risk (CIER) - The projected costs increase, not covered by the cushion, that is reserved for a certain raw material or service (like shipping) due to a variety of uncertain but expected risk factors. For example, if the demand for containers is expected to increase over the next 12 months then one should calculate the uncertain but expected impact (say 10%) on shipping cost. Anything above the CIER up to a stated degree of confidence is an unexpected risk. The CIER should be part of TLC and thus should be budgeted on a cost account.

Cost Increase Unexpected Risk (CIUR) with no correlation - The projected costs increase that is calculated for a certain raw material or service (like shipping) due to a variety of uncertain and unexpected risk factors. Anything above the CIER, up to a say a 99% confidence that the impact will be less than a particular amount, is an unexpected risk[13]. For example, if there is an expectation that the price of steel or tariff will rise in an uncertain and unexpected manner in geographical areas that are experiencing a trade conflict then it is prudent to calculate a CIUR. The CIUR reflects the high end of a plausible bad case scenario but stops well short of the extreme worst-case scenario computed during a stress test. The CIUR at this stage is said to be calculated at the 1% level assuming no correlation between the various priority critical risks.

Cost Increase Unexpected Risk (CIUR) with correlation - Similar to CIUR described above but where at least one priority critical risk has a cross cutting correlation with another priority critical risk. For example, the risk of containers queuing to unload in Los Angeles will have a direct impact on the availability of containers for loading in Asia, thus driving up the cost for shipping. CIUR with correlation, up to the prescribed confidence interval, is accounted for under capital.

Stress Test (ST) - The final risk assessment level is based on conducting a stress test and scenario analysis, in order to establish the amount at risk in severely adverse situations. A ST serves as a base for the preemptive preparation of extreme case emergency plans[14].

IV. Methodology and Business Arrangement examples

Methodology

- **Contract Management & RACI** (Responsible Accountable Consulted Informed) **chart**

[13] Practitioners and regulators also find that calculating expected risk in the tail is a useful measure of risk.

[14] A useful discussion on stress testing and scenario analysis can be found in Chapter 16 of Crouhy, M., Galai, D. and Mark, R.,2015," The Essentials of Risk Management (Second Edition)", McGraw Hill

The calculations mentioned in **Section III** can hardly be done by one person or one department alone. Assigned responsibilities and cross functional team work will be necessary to appropriately assess, evaluate and respond to the existing and future requirements from regulators, owners and other stake holders. The enhanced collaboration between sourcing, procurement and supply chain risk executives becomes a pre-requisite for accurately calculating preventative mitigation budgets[15]. We suggest the use of an expanded third-party contract management template by including the frequently used responsibility assignment matrix (or RACI-chart)[16] and making it more operational such as in our Business Arrangement examples (**Section IV**).

- **Priority Critical Risks (PCR) & Cross Cutting Risks (CCR)**

We examine a subset of PCR's from our list of close to 200 inherent supply-chain risks in order to introduce our views. We initially calculate risk distributions for both likelihood and severity and subsequently derive the total $-value impact as input into an intricate balance between cost of risk, cost of risk mitigation and gross profit. We use our supply chain risk analytics in order to preemptively react in cases where there are material deviations from budget as well as to provide input for the calculation of risk adjusted returns. The impact on risk is influenced by a cross cutting risk such as an external fraud and in turn consequently impacts abother cross cutting risk such as business risk. We present a schematic overview of all this in each of our three business arrangement examples.

- **Supply Chain Risk (SCR) mitigation budget from Best Case to Stress Test**

The lender needs to determine what risk levels and what related cost and profitability levels the third-party business arrangement must achieve in order to be cleared to move forward. The sourcing process owner, chief risk officer (CRO) and chief procurement officers (CPO) need to examine risk mitigation simulations that include examining the various events that drive material risks. Examining risk adjusted returns of alternative supply chain set-ups will be key to reach a well anchored cross-corporate decision for any in-house or outsourced supply chain.

---

[15] In its simplest term, without entering into hierarchical importance discussions, **Sourcing** deals with supply strategies from where to source products and services. **Procurement** negotiates prices and ensures compliance with SOW's and GPC's (in conjuncion with Sourcing and various SME's and process owners). **Logistics** develops and secures the most reliable and cost effective set-ups to bring goods to the required final destination. There are many interpretations of the above functions. These functions all have increasingly important roles in optimizing supply chain performance, including working in partnership with risk management to make supply chain risk transparent.

[16] Harned, B., RACI Charts Explained: Definitions, Example & Template. Team Gantt, 2021. https://www.teamgantt.com/blog/raci-chart-definition-tips-and-example

We start by discussing the process steps for our first business arrangement: second-party credit to third-party supply chain (Bicycle import), followed by third-party cloud services and third-party cleaning services. Our proposed approach applies to any third-party product or service and we hope that our business arrangement examples will be used as input to a guidance document for all banks, including regulators and government entities.

Business Arrangement examples

Business Arrangement 1 - Second-party credit to third-party supply chain for Bicycle import firm 'California Bike Import' (CBI).

A loan to California Bike Import (CBI), a bicycle retailer relying on imports, is a second-party customer with a credit involving a third-party supply chain. The size and interest rate of the bicycle loan to CBI varies as a function of the risk and the nature of the project. CBI requests a $50M loan for a prospective $150M venture. CBI states that their supply chain risk is relatively low and therefore the size of their loan is reasonable.

In order to ensure that due diligence and other contract related processes are carried out effectively, all major activities must be assigned to an owner and be fully implemented and operational. This not only helps the risk assessment process but sets up the framework for many other processes as well, such as the internal escalation process in terms of various disruptions. Tables 1 - 3 introduces an overview for the bicycle business supply chain.

The purpose of the overview is to visualize different components in the supply chain set-up in one single view. A useful level of transparency is obtained with the inclusion of the RACI-chart for assigned responsibilities, the priority critical risk columns for a particular contract and finally by displaying the key dates for each contract, compliance commitment, latest due diligence etc. Decisions about access to each part of the document, including confidentiality, safe storage etc., should be decided between top management and supply chain risk executives.
In our bicycle import example, Table 1 Column 1 shows if the activity is a product or a service. Column 2 indicates which supply chain role each row refers to. Note that Row 2 indicates that the banks credit customer is the second-party borrower, California Bike Import (CBI). All third-party vendor relations from row 3 and down are viewed from the perspective of CBI, to which these vendors are x-party relations.

Column 3 gives a high level description of each product or service while Column 4 is to be populated with a granular statement of work (SOW) upon which the cost, price and risk calculations

are based. Column 5 indicates the name of the second-party borrower (plus any co-borrower if applicable). Column 6 lists the product or service provider name with its respective geographical location (Column 7), tier (Column 8) and geographical supply or service area (Column 9).
Table 1, and the following Tables 2 & 3, are used as both an operational working tool as well as to make supply chain exposure transparent. For example, a CFO or CRO can use the template at any time to get answers to a variety of queries such as:

Question 1: How many third-, fourth- and fifth-party relations do our top 10 corporate clients supply chains have?
Answer 1: Observe in Table 1 our California Bike Import (CBI) example that we have 8 in our supply chain as follows:

- 1 third-party product supplier
- 2 third-party services suppliers
- 2 fourth-party product suppliers
- 1 fourth-party services supplier
- 1 fifth-party product supplier
- 1 fifth-party services supplier.

Question 2: How big portion of the total cost is sitting with a single sourcing supplier of suspensions in Asia?
Answer 2: Observe in Table 2, Row 3 that the cost is $8M or 8% of the total cost of $100M.

Table 1: Bicycle Import Third-party Management, Part 1

PRODUCT or SERVICE	Supply Chain Role	High level Product / Service description	Granular Product Description (SOW)	Second-party name	Third or N-party name	Third or N-party location	Tier	Supply or Service Region
PRODUCT	*BICYCLE IMPORTER (2nd party borrower, client to bank)*	*Mid and High-end bicycles sales*		*California Bike Import (CBI)*	-	-	-	*North America*
PRODUCT	BICYCLE MANUFACTURER	Full range bicycles		-	Best Bicycle Factory	Asia	1	Global
PRODUCT	BICYCLE PARTS MANUFACTURER	Suspensions		-	Component supplier No1	Asia	2	Asia
PRODUCT	BICYCLE PARTS MANUFACTURER	Derailleurs		-	Component suppler No2	Asia	2	Asia

Table 1: Bicycle Import Third-party Management, Part 1

PRODUCT	STEEL MANU-FACTURER	Stainless steel for Derailleurs		-	Steel sup-plier No1	Asia	3	Asia
PRODUCT	SURFACE TREATMENT SUPPLIER	Electro-coating		-	Coating industries	Europe	2	Global
SERVICE	SHIPPING	Ocean freight		-	World lead-ing shipping Co	Asia	1	Global
SERVICE	SHIPPING	Last mile		-	West coast logistics	California	1	United States
SERVICE	INSURANCE	Freight insurance		-	World lead-ing insur-ance Co	Europe	2	Global

In Table 2 (Columns 1 and 2) we repeat the Supply Chain Role and Type of Product/Service from Table 1 followed by the listing of the various responsibility assignments shown in Columns 3 - 7. Although there can be more than one **R**esponsible person or department for a particular activity, there should ultimately be only one who is the lead. For **A**ccountability, there should never be more than one name per activity. If the accountability is assigned to a specific office or department then it is the head of such department, or the VP/SVP for that process, who is ultimately accountable for all preparation, execution and output of that activity.

The **I**nformed and **C**onsulted columns includes multiple functions and entities. The task to coordinate their respective involvement rests firmly with the responsible function or entity. Column 8 shows the requested/confirmed loan amount, Column 9 shows the preliminary or confirmed cost budget for some of the major bicycle import cost drivers. Columns 10 - 14 contains the risk assessment overview and risk costs with details presented in Tables 4 - 11.

Risk costs can be to divided into 4 buckets[17]. If a bank calculates the risk associated with these buckets and incorporates mandatory risk mitigation language into the third-party agreement then it typically leads to better rates and conditions for the borrower since it reduces the lender's risk exposure.

[17] Bucket number: 1. Risk Costs included in the basic contract price and assigned to a cost account (usually COGS). 2.Risk Costs (expected) that are pre-negotiated price adjustments in the contract but not directly included in the basic contract price. For example, risks range from currency risk to raw material price fluctuations. 3.Risk Costs (unexpected) either referenced or not referenced in the contract that are above the expected risk level. These unexpected risks impact economic capital. 4.Stress test impact is not assigned to a cost account but is useful as a measure to make the risk transparent when evaluating various risk scenarios.

Seven PCR's are shown in Column 12. These risks are derived from a list of 198 inherent supply chain risks as shown in our 3-level risk taxonomy (see Table 6). A bank benefits from involving the subject matter expertise to ensure that the supply chain risk register covers all critical risks in the supply chain including sourcing, procurement, logistics[18] and supply chain risk. The SME's can and should be listed in column 6 as **C**onsulted.

Table 2: Bicycle Import Third-party Management, Part 2

Supply Chain Role	High level Product / Service descrip-tion	**R**ESPON SIBLE Lender (Bank), Process owner (Supply Chain)	RESPON SIBLE Buyer	**AC**-COUNT-ABLE Manager	**C**ON-SULTED (CRO, SCRO + any other SME)	**IN**FOR-MED internal and external stake holders	Loan amount	Total Landed Cost budget 2022	Risk assessed at 99% level (Latest assessed Date)	Total risk score	Priority Critical Risks	Stress Test out-come	Cost estimate Priority Critical risks (USD)
BICYCLE IMPORT/ RETAILER	*Mid and High-end bicycle sales*	*CFO Bank*	-	*CEO Bank*	*CRO Bank*	*Board*	*$50M*	-					
BICYCLE MANU-FACTURER	Full range bicycles	SVP Sales/ CCO/ CTO	CPO Bike Import	CEO Bike Import	CRO Bank	Board	-	$100M			1. Execution & Delivery (Vendor relations) 2. Tariffs 3. Supply risk (Stock outs, supplier concen-tration) 4. Govern-ment regula-tion (Taxes & fees) 5. Supply chain strate-gy 6. Deep tier risk 7. Govern-ment inter-vention		
BICYCLE PARTS MANU-FACTURER	Suspen-sions	CTO Manu-facturer	CPO Manu-facturer	CEO Bike Import	CRO Bank	Board	-	$8M					
BICYCLE PARTS MANU-FACTURER	Deraill-eurs	CTO Manu-facturer	CPO Manu-facturer	CEO Bike Import	CRO Bank	Board	-	$9M					
STEEL MANU-FACTURER	Stainless steel for Deraill-eurs	CTO Part manu-facturer	CPO Part manu-facturer	CEO Bike Import	CRO Bank	Board	-	$1M					
SURFACE TREAT-MENT SUPPLIER	Electro coating	CTO Manu facturer	CPO Manu-facturer	CEO Bike Import	CRO Bank	Board	-	$2M					

[18] See footnote 15 on page 9

Table 2: Bicycle Import Third-party Management, Part 2

SHIPPING	Ocean freight	VP Supply Chain Bike Import	CPO Bike Import	CEO Bike Import	CRO Bank	Board	-	$3.5M					
SHIPPING	Last mile	VP Supply Chain Bike Import	CPO Bike Import	CEO Bike Import	CRO Bank	Board	-	$2M					
INSURANCE	Freight insurance	VP Freight Manu-facturer	CPO Manu-facturer	CEO Bike Import	CRO Bank	Board	-	$1.5M					

The first column in Table 3 shows whether a contract is signed or still under negotiation. Columns 2 - 9 displays the sign and expiry dates for the various contracts and commitments linked to the agreement (as required by the corporation and/or the oversight bodies). Column 10 indicates if there is any action to be taken after a failed or audit-confirmed high risk business arrangement. Column 11 shows the assigned contract or work order number for each agreement.

Table 3: Bicycle Import Third-party Management, Part 3

Agreement status	Current Agreement Signed Date	Current Agreement Expire Date	Term & Notice	Latest GPC (General Purchase Condition) signed (Date)	Latest Executive Summary signed (Date)	Anti Corrup-tion letter signed (Date)	Latest SSA (Supplier self assess-ment) signed & received (Date)	SSA on location audit (Date)	Comment on failed SSA audit (incl. time to correct if apply)	Work order number
Under conside-ration										
Under conside-ration										
Existing										
Existing										
Existing										
Existing										

Table 3: Bicycle Import Third-party Management, Part 3

Under conside-ration										
Under conside-ration										
Existing										

Most of the supply chain costs for bicycles from Asia to United States increased during 2019-2020. These costs included steel, shipping and tariffs. The demand inelasticity in the bicycle market meant that retailers, such as in our example, were able to pass on almost the entire cost increases to the customers since the bicycle market still was in big demand despite higher prices. The inelastic demand[19] is very rare and was primarily caused by the pandemic. An elastic demand in normal markets would have caused a major dent in their bottom line result as shown in the example below.

The risk was elevated in our example since the supply chain was hit not only by cost increases but also by capacity shortage which led to lost sales. This would have led to severe out of stock situations for a smaller company since less cash strapped larger players were able to secure long term orders with upfront payments which blocked out the supply for others.

The disrupted supply chain led to a higher COGS and TLC. Also, the highly elastic demand impacted the bottom line as shown in the first column of Table 4. Observe that the:

* Cost in column 1 was set at $1,000 for each bicycle and includes a best case cost ($960) plus a Cushion ($40) for smaller cost increases in manufacturing and transportation.
* Revenue (sales price) was set at $1,500 for each bicycle.

Therefore:

* Gross margin = 33.33%
* Gross profit = $500

[19] Hayes, A., Elasticity. Investopedia, 2021. https://www.investopedia.com/terms/e/elasticity.asp

Table 4: Bicycle Import: Elastic Demand and Original Price at 3 Cost Levels

	Best Case + Cushion	BC + C+ Cost Increase Expected Risk	BC + C + CIER + Cost Increase Unexpected Risk	Best Case + Cushion for 100,000 bicycles	BC + C + Cost Increase Expected Risk for 100,000 bicycles	BC + C + CIER + Cost Increase Unexpected Risk for 100,000 bicycles
Cost/Bicycle	$1,000.00	$1,296.10	$1,646.05	$100M	$129.61M	$164.6M
Revenue as originally set at $1,500/bicycle	$1,500.00	$1,500.00	$1,500.00	$150M	$150M	$150M
Gross margin %	33.33%	13.59%	-9.74%	33.33%	13.59%	-9.74%
Gross profit $	$500.00	$203.90	-$146.05	$50M	$20.39M	-$14.6M

If we assume the market price could not exceed $1,500 due to demand elasticity, then all cost increases, including risk costs, would hit the company's bottom line. Unless, of course, the buyer could convince the manufacturer to absorb some or all of these costs themselves.

Our next scenario assumes that the bicycle import company experiences a disrupted supply chain at higher costs, static inelastic demand and maintained gross profit. The impact of the risk is minimized due to the unusually high market demand at any sales price level.

Customers were willing to pay 30%+ more for a same bicycle and therefore the company was able to pass on all cost increases of $296 (see column 2 of Table 5) for a total cost of $1,296 to the customer at a price of $1,944. The company was able to maintain the 33.33% gross margin and profit level. This unusual scenario will at some point hit a maximum price level that the market can tolerate. A lender to a supply chain benefits from frequent and consistent market analyses in order to know when the maximum price level is being approached.

Table 5: Bicycle Import: Inelastic Demand and Higher Price at 3 Cost Levels

	Best Case + Cushion	BC + C + Cost Increase Expected Risk	BC + C + CIER + Cost Increase Unexpected Risk	Best Case + Cushion for 100,000 bicycles	BC + C + Cost Increase Expected Risk for 100,000 bicycles	BC + C + CIER + Cost Increase Unexpected Risk for 100,000 bicycles
Cost/Bicycle	$1,000.00	$1,296.10	$1,646.05	$100M	$129.61M	$164.6M
Revenue with all cost risk increases passed on to customer	$1,500.00	$1,944.15	$2,469.07	$150M	$194.42M	$246.91M
Gross margin %	33.33%	33.33%	33.33%	33.33%	33.33%	33.33%
Gross profit $	$500.00	$648.05	$823.02	$50M	$64.8M	$82.3M

A preliminary quantitatively based risk assessment should take place prior to considering any proposal from either an in-house or out sourced service provider. The risk assessment should be included in request for information (RFI) stage and the amount of risk levels should be compared to the established risk appetite of the corporation.

The supply chain risk analyst utilizes historical data, supply chain subject matter expertise and risk analytics to determine the unexpected cost of risk at the 1% level. The analyst in our example determines that this unexpected cost of risk could result in an increase in cost to $1,646 as shown in the third column of Table 4 and 5. The 1% level was chosen since the bicycle company wanted to make this risk transparent to stakeholders in order to more fully describe what the cost might potentially be in an adverse situation. In particular, the risk analyst concludes that there is only 1% chance of exceeding the cost (i.e. $ 1,646) over the next year.

The quantitatively based risk assessment is accompanied by a questionnaire (see example in Appendix 1) which provides qualitative context to support the quantitative risk assessment. If a vendor response doesn't meet or exceed the minimum level of transparency and self declared compliance, including risk mitigation processes, then the vendor should not be selected to move forward in the bid process. In addition, prior to signing any agreement, all responses should ideally be verified on location to confirm coherence with the written answers.

A parallel approach to building a risk culture in the banking corporation can be found in building a problem-solving culture in a process industry or supply chain through the Lean[20] approach. Rather than hiding a problem, the focus is on making the problem transparent to quicker initiate root causes analysis and generate sustainable solutions. This in turn will improve throughput and reduce costs. From a risk perspective, it would mean making each assessed risk transparent in order to trace the origin of the risk, structure them in order of potential impact and start generating risk mitigating solutions.

To quote Koenigsaecker and Taha: "…building a root-cause problem-solving culture in the midst of our daily fire fighting is incredibly difficult. Let me say this again: Building a root-cause problem-solving culture is incredibly difficult." 'Toyota sensei talks about learning to see problems as 'golden nuggets' because they are the beginning of your next improvement.'

Each business areas SC's will have different risk profiles. Table 6 provides an illustrative example of priority critical risks (PCR) for a bicycle import supply chain:

Table 6. Bicycle Import: Priority Critical Risks

Category (8 inherent Risk Categories)	Sub Category (56 Sub Categories)	Element (198 Risk Elements)
Operational Risk (C2)	Execution, Delivery and Process Mgmt. Risk (C2SC7)	Vendor Relations (C2SC7E2)
Political Risk (C7)	Tariff Risk (C7SC8)	Tariff Risk (C7SC8E1)
Business Risk (C1)	Supply Risk (C1SC2)	Stockouts (lost sales) (C1SC2E3)
Business Risk (C1)	Supply Risk (C1SC2)	Supplier Concentration (C1SC2E8)
Business Risk (C1)	Government Regulation and Business Culture Risk (C1SC3)	Taxes & Fees (C1SC3E3)
Strategic Risk (C4)	Supply Chain Strategy status (C4SC1)	Supply Chain Strategy (C4SC1E1)

[20] Koenigsaecker, G. and Taha, H., A problem-identifying and problem-solving system, Page 14. Leading the Lean Enterprise Transformation, Second Edition, 2012. https://books.google.com/books?id=v3DKDwAAQBAJ&pg=PA14&lpg=PA14&dq=Six+Sigma+finding+the+golden+nugget&source=bl&ots=4AS3nbiHBY&sig=ACfU3U2P1XqRQUfW_-Btxx9KfrsrTXiSqg&hl=sv&sa=X&ved=2ahUKEwi-V1drh_MLzAhWldt8KHf28ANQQ6AF6BAgPEAM#v=onepage&q=Six%20Sigma%20finding%20the%20golden%20nugget&f=false

Systemic Risk (C5)	Deep Tier Risk (C5SC4)	Deep Tier Risk (C5SC4E1)
Systemic Risk (C5)	Government Intervention (C5SC7)	Government Intervention (C5SC7E1)

We first calculate risk at the 1% level assuming a zero correlation for the priority critical risk shown in in Table 6. We next incorporate correlations as shown in our cross cutting (CC) risk bi-cycle import example in Table 7 such as in the case of correlation between Execution & Delivery risk and Business risk. This cross-cutting risk table contains a yes (Y) in the row column cell location which illustrates that a material correlation exists.

Observe in Table 7 that a political risk may lead to rise in tariffs which in turn can result in higher total landed costs. If the market is not able to pay more for the product, then this will constitute a financial risk since the cost increase would impact the bicycle importers cash flow and ability to make good on credit installments. Similarly, if the media reveals that a deep tier sub-supplier has engaged in bonded labor then it may have repercussions on reputation risk leading to a drop in demand as part of the societal increase in activism and cancel culture.

Table 7. Bicycle Import: Cross Cutting Risks

Causing categories	Impact on: ->	Financial	Operational	Environment	Political	Business	Reputation	Strategic	Systemic
Risk causing category	Critical SC risks for 3rd party bicycle import	Y	-	-	Y	Y	Y	-	-
Financial Risk	-	n/a							
Operational Risk	Execution & Delivery (Vendor relations)	Y	n/a			Y	Y		
Environment Risk	-			n/a					
Political Risk	Tariff Risk	Y			n/a	Y			
Business Risk	Supply Risk (Stock outs, Supplier concentration). Government regulation (Taxes & Fees)	Y				n/a	Y		

Reputation Risk	-						n/a		
Strategic Risk	Supply Chain Strategy	Y				Y	Y	n/a	
Systemic Risk	Deep Tier Government Intervention	Y			Y	Y			n/a

We next consider the impact that the set of priority critical supply chain risks, inclusive of the cross cutting risks, may have on our best case (BC) estimate of $960 plus the cushion (C) of $40 to provide a quantitatively derived risk informed view of our potential costs increase over the next year. (See Table 8)

We project a **C**ost **I**ncrease arising from **E**xpected **R**isk (CIER) of nearly 30% ($296.10). The CIER is based on analyzing historical and projected going forward risk factors for a particular risk type (e.g. tariff increases). We also calculate a projected cost increase due to the **C**ost **I**ncrease arising from Uncertain **R**isk (CIUR) up to certain level of confidence.

In our example, we calculate risk up to the point that there is 1% chance the CIUR adds to BC + C + CIER an amount greater than:

- $ 115 where there is a zero correlation between all critical risk types[21]
- $ 234.95 over the zero correlation case when we consider the actual correlation between all critical risk types[22].

We project both the CIER and the CIUR up to the confidence interval based on our selected probability functions which best describe the marginal and joint frequency and severity probabilities associated with a particular risk type.

Observe that if the price of the bike is not adjusted to reflect the potential risk then the gross margin turns negative when the overall cost rises to $1,646 (which is larger than the selling price of a bike at $1,500). In other words, there is a 1 % chance that the overall cost may be greater than $1,646 and the gross margin may be worse than -$146.05.

[21] Observe from Table 8 that $1411.10 - $1296.10 = $115

[22] Observe that $1646.05 - $1411.10 = $234.95

Our risk analysis provides greater transparency in terms of the amount of risk taken and facilitates the formulating of various mitigation budgets and their respective impact on the overall profitability.

Table 8. Bicycle Import: Priority Critical Risk Cost (Accumulated)

Not mitigated				Cost Increase Unexpected Risk (CIUR)		
	Best Case	BC + (C)	BC + C + Cost Increase Expected Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + Stress Test (ST)
Cost/Bicycle	$960.00	$1,000.00	$1,296.10	$1,411.10	$1,646.05	$2,500.00
Revenue as originally set at $1,500/bicycle	$1,500.00	$1,500.00	$1,500.00	$1,500.00	$1,500.00	$1,500.00
Gross margin %	36.00%	33.33%	13.59%	5.93%	-9.74%	-66.67%
Gross profit $	$540.00	$500.00	$203.90	$88.90	-$146.05	-$1,000.00

We next examine the components of cost for the PCR's in Table 9. The individual CIER components for each PCR (PCR 1 to 4) are shown along with overall CIER. Similarly, the CIUR components for each PCR are shown along with the overall CIUR.[23] We also stress test the supply chain risk based on scenarios constructed by supply chain practitioner experts working in partnership with supply chain risk experts.[24]

[23] For ease of explanation, the portfolio benefits have been attributed back into the individual priority cost risks so that they sum to the CIUR

[24] We also assume for ease of explanation that the four priority critical risks remain the same in Table 9. In reality this may not be the case. For example, some of the top four priority critical risks may not show up in the Stress Test column. We also ignore all risks not included in the top four priority risk calculations for ease of explanation.

Table 9. Bicycle Import: Priority Critical Risk Cost Breakdown

				Cost Increase Unexpected Risk (CIUR)		
	Best Case	Cushion (C)	Cost Increase Expected Risk (CIER)	CIUR with no correlation	CIUR with correlation	Stress Test (ST)
Priority Critical Risks (PCR) cost	$0.00	$40.00	$296.10	$115.00	$234.95	$853.95
PCR 1- Supply Chain Strategy	$0.00	$0.00	**$130.00**	$25.00	**$100.00**	**$350.00**
PCR 2 - Supply Risk	$0.00	$20.00	$60.00	$10.00	$19.97	$40.00
PCR 3 - Government intervention	$0.00	$0.00	$56.10	**$60.00**	$89.98	**$375.00**
PCR 4 - Execution & Delivery	$0.00	$20.00	$50.00	$20.00	$25.00	$88.95
PCR cost check	$0.00	$40.00	$296.10	$115.00	$234.95	$853.95

Red marked cells in Table 9 have been prioritized for mitigation due to their impact on the cost of risk.

Given that we have established the impact of the four priority critical risks in Tables 6 and 9, we can now move on to Tables 10 and 11 to examine possible risk reduction counter measures. This is helpful when considering the return to risk tradeoffs of reducing the cost impact of the PCR's. Risk informed counter measures enable us to now engage in a productive dialogue about the best and most cost effective ways to reduce their respective cost impacts on overall financial performance. In Table 10 we pair these PCR's with examples of mitigating actions as follows:

- PCR 1 - (single sourcing) Supply Chain Strategy *mitigated by* Multi sourcing
- PCR 2 - Supply Risk *mitigated by* Buffer stock increases
- PCR 3 - Government Intervention *mitigated by* Regional Supply
- PCR 4 - Execution & Delivery problems *mitigated by* Dual Sourcing and VMI[25]

The first Row in Table 10 indicates the cost of risk for each risk scenario. Rows 2 - 5 show both the investment (with positive numbers) along with how much each mitigating action (with negative numbers) impacts the cost for each cost scenario. Row 6 shows the total risk mitigating impact.[26] We inserted the Row 6 numbers from Table 10 in Table 11 in order to show how the risk

[25] VMI = Vendor Managed Inventory

[26] Assumes portfolio effects have been incorporated for ease of explanation

mitigating action impacts gross profit and gross margin.

Table 10. Bicycle Import: PCR Costs Mitigating Impact (Incremental)

				Cost Increase Unexpected Risk (CIUR)		
Mitigating Action	Best Case	Cushion (C)	Cost Increase Expected Risk (CIER)	CIUR with no correlation	CIUR with correlation	Stress Test (ST)
Total PCR cost	$0.00	$40.00	$296.10	$115.00	$234.95	$853.95
PCR 1- Multi sourcing	$60.00	$20.00	-$50.00	-$10.00	-$50.00	$0.00
PCR 2 - Increase buffer stock	$20.00	$0.00	-$40.00	-$5.00	-$10.00	$0.00
PCR 3 - Regional supply	$0.00	$0.00	-$30.00	-$35.00	-$60.00	$0.00
PCR 4 - Dual sourcing & VMI	$10.00	$0.00	-$30.00	-$15.00	-$15.00	$0.00
Total mitigated PCR cost impact	$90.00	$20.00	-$150.00	-$65.00	-$135.00	$0.00

Table 11. Bicycle Import: PCR Costs Mitigated Impact (Accumulated)

Mitigated				Cost Increase Unexpected Risk (CIUR)		
	Best Case	BC + Cushion	BC + C + Cost Increase Expect-ed Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + ST
Non-mitigated cost/bicycle	$960.00	$1,000.00	$1,296.10	$1,411.10	$1,646.05	$2,500.00
Mitigated PCR cost impact	$90.00	$20.00	-$150.00	-$65.00	-$135.00	$0.00
Mitigated total cost/Bicycle	$1,050.00	$1,110.00	$1,256.10	$1,306.10	$1,406.05	$2,260.00
Revenue as originally set at $1,500/bicycle	$1,500.00	$1,500.00	$1,500.00	$1,500.00	$1,500.00	$1,500.00
Gross margin %	30.00%	26.00%	16.26%	14.85%	12.93%	-50.67%
Gross profit $	$450.00	$390.00	$243.90	$193.90	$93.95	-$760.00

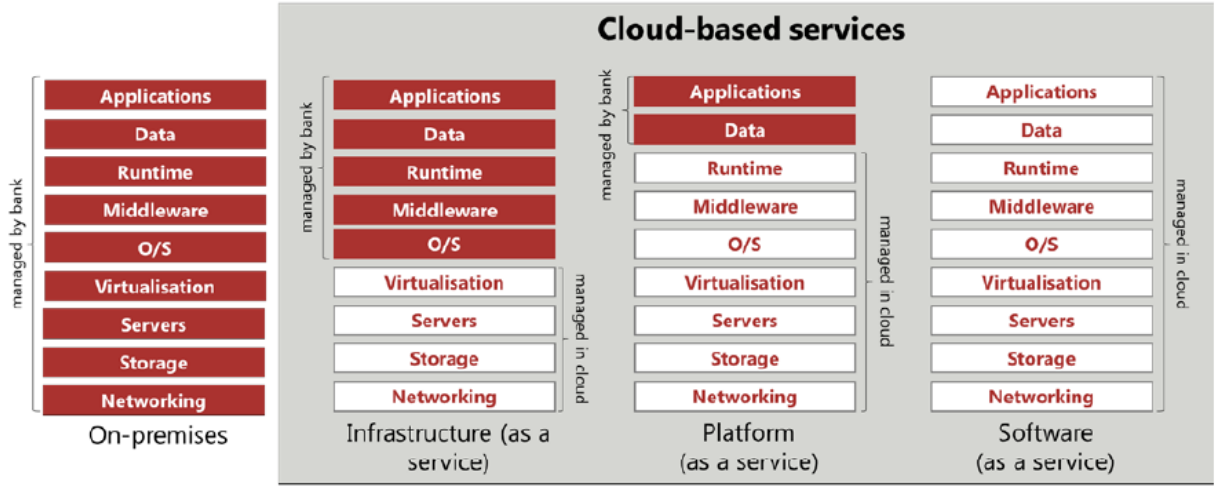
If we compare the non-mitigated and mitigated cost then it shows that the BC and BC + C levels in the mitigated example are slightly higher than in the non-mitigated one ($960 vs $1,050 and $1,000 vs $1,110 respectively). However, if both the expected and unexpected cost risks are considered then the mitigated version now provides a slightly more acceptable 12.93% gross margin. This number is to be compared with the negative -9.74% for the non-mitigated scenario. Observe that the mitigated version does not reach red figure territory until the stress test stage.

If both expected and unexpected cost of risks are considered then the mitigated example then shows a gross profit of $93.95/bicycle in contrast to the loss of -$146.05/bicycle for the non-mitigated one. We are looking at a gross profit of $9.4M vs a loss of $14.6M at 100,000 bicycles sold which clearly underscores the ability (or lack thereof) to make good on periodic loan installments and possibly even long term survival.

Business Arrangement 2 - Third-party Outsourcing of Cloud services

Cloud based services are divided into those that are on premises vs those that are off premises. Cloud based services can also be divided into three broad 'as a service' categories as follows (see Figure 1 below).

Figure 1: Cloud Based Services



Source: Technet.

Third-party cloud servicing spend across all categories is expected to significantly increase over the next decade[27] [28]. Yet there are still very few banking corporations who are open to share detailed cost break-downs to enable adequate cost-quality-risk analysis from a financial perspective[29]. We decided to use an example of a major bank spending approximately $500M in annual cloud services spend[30] [31].

The relationship that a bank has with a cloud service company, as used in our illustrative example, calls for the bank to have a clear understanding of the controls that the cloud service provider and the bank are responsible to configure and manage.

The bank is ultimately responsible for the effectiveness of control management regardless of the division of control responsibilities between the cloud service provider and the bank. As with other third-party relationships, the bank needs to conduct due diligence to calculate the risk associated with the cloud servicer. The bank cloud servicer can satisfactorily oversee and monitor their subcontractors as presented in Tables 12 - 14.

Similarly, a fintech company may involve critical third-party bank activities. The OCC provides criteria the banks may use to determine the critical fintech activities. These critical activities include significant bank functions such as payments, clearing, settlements, custody and significant

---

[27] Worldwide Public Cloud Services Market Totaled $312 Billion in 2020 with Amazon Web Services and Microsoft Vying for the Top Position Overall, According to IDC. IDC Media center, 2021. https://www.idc.com/getdoc.jsp?containerId=prUS47685521

[28] Cloud Computing Market Size, Share & Trends Analysis Report By Service (SaaS, IaaS), By Enterprise Size (Large Enterprises, SMEs), By End Use (BFSI, Manufacturing), By Deployment, And Segment Forecasts, 2021 - 2028. Grand View Research, 2021. https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry

[29] 'Expressed in a recent study on the subject: *'Banks who agreed to participate, had strict rules regarding this research. As contribution was only possible if quantitative and financial data were excluded of this research and participation was guaranteed anonymously. Furthermore, databases, descriptive or structured data-sets regarding cloud migration costs were not publicly available during the time of this research. Profit and loss statements of banks for IT related costs are generally accumulated as one general cost category and not specified per cost type. As a consequence, it is not possible to perform quantitative research'* . Kaya, F. et al, The banking industry underestimates costs of cloud migrations. Research gate, 2020. https://www.researchgate.net/publication/341112723_The_Banking_Industry_Underestimates_Costs_of_Cloud_Migrations_Cloud_Computing/link/5eaeba07299bf18b95912bd1/download

[30] Butcher, S. Here's how much banks spend on tech vs. Amazon and Google. Efinancialcareers. 2021. https://www.efinancialcareers.com/news/finance/banks-tech-spending-vs-google-and-amazon

[31] Columbus, L. 32% of IT budgets will be dedicated to the cloud by 2021. Forbes editors pick. 2020. https://www.forbes.com/sites/louiscolumbus/2020/08/02/32-of-it-budgets-will-be-dedicated-to-the-cloud-by-2021/?sh=106f35ce5fe3

shared services such as information technology or other activities that could cause a bank to face significant risk if a third-party fails to meet expectations or could have a significant bank customer impact.

The OCC points out that banks need to consider the financial condition of third parties, such as fintech, during due diligence and ongoing monitoring. For example, assessing the changes in the financial condition of third parties is an expectation of the ongoing monitoring component of the banks risk management. The scope of due diligence and the due diligence method should vary based on the level of risk of the third-party relationship. Once the risk is known, various mitigation strategies can take place such as acquisition of fintech services in order to reduce the banks business risk[32].

We presented a combined RACI-chart and contract management overview for a consumer product intended to be sold to a customer in **Business Arrangement 1**. We next turn our focus to third-party services procured by the bank to be consumed by an end-user in **Business Arrangements 2 and 3**. We do not differentiate between a product or a service supplier in terms of responsibility to ensure that risk assessment and mitigation are executed according to bank standards. Both can and will have considerable impact on the financial performance of the bank.

Column 1 in Table 12 indicates if the activity is a product or a service. Column 2 indicates the overall business area (IT/Communication in this case). Column 3 indicates the type of service while Column 4 contains more specificity such as the areas described in Figure 1. Column 5 provides a more granular statement of work (SOW) that forms the foundation on which the cost, price and risk calculations are based. Column 6 reveals the name of the product or service provider with its respective geographical location (Column 7), tier (Column 8) and geographical supply or service area (Column 9). A geo redundant[33] architecture can be an important risk mitigating element for cloud services.

[32] Berkowitz, B., 5 Acquisitions That Will Help JPMorgan Chase Grow and Better Compete. The Motley Fool, 2021. https://www.fool.com/investing/2021/07/14/5-acquisitions-jpmorgan-chase-grow-compete/

[33] Team Cloudify., Geo Redundancy Explained. Cloudify, 2021. https://cloudify.co/blog/geo-redundancy-explained/

Table 12. Cloud Services: Third-party Management, Part 1

PRODUCT or SERVICE	Business Area	Service Area	High level service type	Granular statement of work (SOW)	Third or N-party name	Third or N-party location	Tier	Supply/ Service region
SERVICE	IT / COMMUNI-CATION	Cloud services (IaaS, PaaS, SaaS, and other)	Software Services	Described in detail by responsible process owner and signed off by responsible buyer in terms of market availability. Four eye principle to be kept at all times while maintaining an open collaborative working relation between the two.	Software services provider	United States	1	GLOBAL/REGIONAL, geo redundancy
SERVICE	IT / COMMUNI-CATION	Cloud services (IaaS, PaaS, SaaS, and other)	Server Services	Described in detail by responsible process owner and signed off by responsible buyer in terms of market availability. Four eye principle to be kept at all times while maintaining an open collaborative working relation between the two.	Server warehouse company	Canada	2	GLOBAL/REGIONAL, geo redundancy

We repeat the type of product/service in Columns 1 and 2 of Table 13, followed by a listing of responsibilities shown in Columns 3 - 7. There should ultimately be one person or function who takes the lead for **A**ccountability. There could be more than one **R**esponsible person or department for a certain area but there should never be more than one responsible who owns the process. If the accountability is assigned to a specific office or department then it is the head of the department, or the VP/SVP for that process, who is ultimately accountable for every preparation, execution and output of that activity.

The **I**nformed and **C**onsulted columns includes multiple functions and entities. The responsibility to coordinate all tasks rests firmly with the overall responsible function or entity. The estimated/confirmed budget for the required cloud services is shown in Column 8. Columns 9 - 13 contains an overview of the risk assessment which is detailed in Tables 15 - 21.

Table 13. Cloud Services: Third-party Management, Part 2

PRODUCT or SERVICE	Business Area	**RE**SPONSIBLE Process owner (Supply Chain)	RESPONSIBLE Buyer	**A**CCOUNTABLE Manager	**C**ONSULTED (CRO, SCRO + any other SME)	**I**NFORMED Internal and external stake holders	Total Landed Cost Budget 2022	Risk assessed at 99% level (latest assessed date)	Total risk score	Priority Critical Risks	Stress Test out come	Cost estimate Priority Critical risks (USD)
SERVICE	IT / COMMUNICATION	CIO	VP IT Procurement	CPO	CRO	CEO/OCC	$500M			**1**. External fraud risk (Cyber risk). **2**. Ability to fulfill promises (Data privacy, data loss prevention, security challenges) **3**. Ethical practices. **4**. Alignment with business strategy. **5**. Supplier integration. **6**. Deep tier risk		
SERVICE	IT / COMMUNICATION	CIO	Cloud services provider (Tier 1)	CIO	CRO	CEO/OCC	$25M			**2**. Ability to fulfill promises (Data privacy, data loss prevention, security challenges) **6**. Deep tier risk		

The first column in Table 14 indicates if a contract is either signed or is still under negotiation. Columns 2 - 9 contains the sign and expiry dates for the agreement and its various related documents (as required by the corporation and/or oversight bodies). Column 10 indicates if an audit was successful or failed and provides a lead time for corrections (when applicable). Column 11 displays the agreement or work order number for easy retrieval.

Table 14. Cloud Services: Third-party Management, Part 3

Agreement status	Current Agreement Signed Date	Current Agree-ment Expire Date	Term & No-tice	Latest GPC (General Purchase Condi-tion) signed (Date)	Latest Executive Summary signed (Date)	Anti Corrup-tion letter signed (Date)	Latest SSA (Sup-plier self assess-ment) signed & received (Date)	SSA on location audit (Date)	Com-ment on failed SSA audit (incl. time to correct if applies)	Agree-ment or Work order number
Under negotia-tion										
Existing										

Despite the high budget for cloud services, we argue that in many cases cost is a less important factor than risk and quality due to the potential cost of the PCR's, inclusive of cross cutting risk.

As we did in the bicycle example, we next consider what impact the priority critical supply chain risks, inclusive of the cross-cutting risks, have on our initial cloud services costs (See Table 15). Our goal is to provide a quantitatively derived risk informed view for the upcoming 12 month period of potential costs increases for cloud services.

We project a **C**ost **I**ncrease arising from **E**xpected **R**isk (CIER) of $25 per user from a BC + C cost of $500 to $525. The CIER is based on analyzing historical and projected risk factors that drive cost for a particular risk type (e.g. Cyber Risk).

We also calculate a projected **C**ost **I**ncrease due to **U**nexpected **R**isk (CIUR) up to certain level of confidence. In our example, we calculate risk up to point that there is 1% chance that the sum of BC + C + CIER + CIUR is greater than $667 per user. In other words, the sum of the CIER and the CIUR adds $167 to the BC + C amount of $500 per user (almost a 45% increase in cost).

The calculation of cost, based on our confidence interval, is derived from our selected probability functions which best describe the marginal and joint probabilities for frequency and severity associated with a particular cloud services risk type. Observe in Table 15 that the cost for 1 million cloud service users adjusted to reflect the potential risk rises to $667 million. In other words, there is 1% chance that the overall cloud service cost may be greater than $667 million.

Our risk analysis provides significant transparency for the amount of risk taken for cloud service costs and facilitates the formulating of various mitigation budgets along with their respective impact on the overall cloud service cost.

Table 15. Cloud Services: 3 Cost Levels (Accumulated)

	Best Case (BC) + Cushion (C)	BC + C + Cost Increase Expected Risk (CIER)	BC + C + CIER + Cost Increase Unexpected Risk (CIUR)	BC + C for 1,000,000 users	BC + C + CIER for 1,000,000 users	BC + C + CIER + CIUR for 1,000,000 users
Cloud cost/user/year	$500	$525	$667	$500M	$525M	$667M
Total IT Cost Budget/Year	$0	$0	$0	$1,500M	$1,500M	$1,500M
Cloud Services % of total IT Costs	n/a	n/a	n/a	33.33%	35.00%	44.45%

Few, if any, banks are keeping 100% of their data in an on-premises data warehouses. Further, very few are putting all their eggs in one cloud basket via having 100% of their data assigned to a single third-party cloud service provider. 'Hybrids' and multi or dual sourcing services are more of the norm in order to balance Cost, Quality and Risk.

The risk return tradeoffs from using third-party cloud services should be compared to in-house solutions. For example, cloud servicing companies generally provide superior data security and recovery systems. The same goes for quality service and performance. There are distinct cost savings opportunities to consider for both in-house and outsourcing options. Investments in servers and the real estate for in-house data warehouses will require significant initial cash despite the lower up-front costs. Further, the cloud services may end up costing more over time in terms of the required upgrades

The cost, risk, quality tradeoffs need to be quantitatively measured. For example, we measure the priority critical risks for outsourced cloud services based on the CIER and CIUR approaches we describe in Tables 16 - 19.

Table 16. Cloud Services: Priority Critical Risks

Category (8 inherent Risk Categories)	Sub Category (56 Sub Categories)	Element (198 Risk Elements)
Operational Risk (C2)	External fraud risk (C2SC2)	Cyber Risk (C2SC2E1)
Operational Risk (C2)	Business Disruption/System Failure Risk (C2SC6)	Network Failure (C2SC6E3)
Reputation Risk (C3)	Ability to fulfill promises risk (C3SC1)	Data loss prevention (C3SC1E6)
Reputation Risk (C3)	Ability to fulfill promises Risk (C3SC6)	Data loss (C3SC6E6)
Reputation Risk (C3)	Follows Ethical Practices Risk (C3SC9)	Data loss prevention (C3SC9E6)
Strategic Risk (C4)	Alignment with Business Strategy (C4SC4)	Business Strategy Alignment (C4SC4E1)
Systemic Risk (C5)	Supplier Integration Risk (C5SC3)	Supplier Integration Risk (C5SC3E1)
Systemic Risk (C5)	Deep Tier Risk (C5SC4)	Deep Tier Risk (C5SC4E1)

Table 17. Cloud Services: Cross Cutting Risks

Causing categories	Impact on: ->	Financial	Opera-tional	Environ-ment	Politi-cal	Business	Reputa-tion	Strategic	Systemic
Risk causing category	Critical SC risks for out sourced Cloud Services	Y	Y	-	-	Y	Y	Y	-
Financial Risk	-	n/a							
Operational Risk	External Fraud Risk (Cyber Risk)	Y	n/a			Y	Y	Y	
Environ-ment Risk	-			n/a					
Political Risk	-				n/a				
Business Risk	-					n/a			
Reputation Risk	Ability to fulfill promises (Data privacy, Data loss prevention, Security challenges) Ethical practices.	Y	Y			Y	n/a	Y	
Strategic Risk	Alignment with Business Strategy							n/a	
Systemic Risk	Supplier Integration, Deep Tier	Y	Y			Y	Y	Y	n/a

Table 18. Cloud Services: 6 Cost of Risk Levels (Accumulated)

Not mitigated				Cost Increase Unexpected Risk (CIUR)		
	Best Case	BC + (C)	BC + C + Cost In-crease Expected Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + Stress Test
Cloud cost 2021	$475M	$500M	$525M	$575M	$667M	$800M
Cloud cost budget 2021	$500M	$500M	$500M	$500M	$500M	$500M

Table 18. Cloud Services: 6 Cost of Risk Levels (Accumulated)

Not mitigated				Cost Increase Unexpected Risk (CIUR)		
	Best Case	BC + (C)	BC + C + Cost Increase Expected Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + Stress Test
Deviation from budget 2021 in %	-5.26%	0.00%	4.76%	13.04%	25.04%	37.50%
Deviation from budget 2021 in $	-$25M	$0M	$25M	$75M	$167M	$300M

The increase from $525M to $667M may seem excessively high. However, as recently as 2019, one major bank ended up paying $150M in various damages after an unexpected cloud breach[34]. It is unclear how much of that sum was anticipated in the form of reserved capital.

Table 19. Cloud Services: Priority Critical Risk Cost Breakdown

				Cost Increase Unexpected Risk (CIUR)		
	Best Case	Cushion (C)	Cost Increase Expected Risk (CIER)	CIUR with no correlation	CIUR with correlation	Stress Test (ST)
Priority Critical Risks (PCR) cost	$0	$25M	$25M	$50M	$92M	$133M
PCR 1- Alignment with business strategy	$0	$7M	$4M	$5M	$6M	$11M
PCR 2 - Ability to fulfill promises	$0	$10M	**$11M**	**$25M**	**$35M**	$30M
PCR 3 - Supplier integration	$0	$4M	$3M	$5M	$11M	$22M
PCR 4 - Ethical practices	$0	$4M	**$7M**	**$15M**	**$40M**	$70M
PCR cost check	$0	$25M	$25M	$50M	$92M	$133M

Red marked cells in Table 19 have been prioritized for mitigation due to their impact on the cost of risk.

[34] Flitter, E & Weise, K., Capital One data breach compromises data of over 100 million. The New York Times, 2019. https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html?referringSource=articleShare

Traditional Return on Investment (ROI) calculations from investing in a third-party cloud solution[35] should be supplemented with Risk Adjusted Return on Capital calculations. Further, similar to our discussions in the bicycle import example, we quantify various mitigation measures as shown in Tables 20 and 21 that benefit from the quantification of the four most critical risks (PCR's). In particular, we look at possible counter measures to reduce the cost impact of the PCR's for cloud servicing.

In other words, we engage in a productive dialogue about the best and most cost effective ways to limit any negative cost impact and other damaging effects on an organization by incorporating the CIER and CIUR calculations with examples of mitigating actions in Table 20 as follows[36]:

PCR 1 - (lack of) Alignment with Business Strategy *mitigated by* Align w Business Strategy
PCR 2 - Ability to fulfill promises *mitigated by* Enhanced fulfillment simulations
PCR 3 - Supplier Integration *mitigated by* Preemptive Supplier and interface analysis
PCR 4 - Ethical Practices *mitigated by* Enhanced Due Diligence

The first Row in Table 20, shows the risk cost for each risk scenario. Rows 2 - 5 shows how much each mitigating action increases or reduces the cost for each scenario while Row 6 shows the total risk mitigating impact.

In Table 21 we then insert the Row 6 number from Table 20 to show how the mitigating action impacts gross profit and gross margin.

Table 20. Cloud Services: PCR Mitigating Measures Impact (Incremental)

				Cost Increase Unexpected Risk (CIUR)		
Mitigating activity	Best Case	BC + (C)	BC + C + Cost Increase Expected Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + ST
Total PCR cost	$0	$25M	$25M	$50M	$92M	$133M
PCR 1- Align with business strategy	$3M	-$2M	-$3M	-$3M	-$3M	$0M
PCR 2 - Ability simulations to fulfill promises	$5M	-$3M	-$6M	-$13M	-$20M	$0M

[35] Building ROI from cloud computing. The Open Group, 2020. http://www.opengroup.org/cloud/cloud_for_business/p6.htm

[36] As described earlier in Tables 16 and 19.

Table 20. Cloud Services: PCR Mitigating Measures Impact (Incremental)

				Cost Increase Unexpected Risk (CIUR)		
Mitigating activity	Best Case	BC + (C)	BC + C + Cost Increase Expect-ed Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + ST
Total PCR cost	$0	$25M	$25M	$50M	$92M	$133M
PCR 3 - Process and interface analysis	$2M	-$2M	-$1M	-$3M	-$8M	$0M
PCR 4 - En-hanced due diligence	$5M	-$3M	-$5M	-$8M	-$25M	$0M
Total mitigated PCR cost impact	$15M	-$10M	-$15M	-$27M	-$56M	$0M

Table 21. Cloud Services: PCR Costs Mitigated Impact (Accumulated)

Mitigated				Cost Increase Unexpected Risk (CIUR)		
	Best Case	BC + Cushion (C)	BC + C + Cost Increase Expect-ed Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + ST
Total cloud cost 2021	$475M	$500M	$525M	$575M	$667M	$800M
Mitigated PCR cost impact	$15M	-$10M	-$15M	-$27M	-$56M	$0M
Mitigated total cloud cost 2021	$490M	$505M	$515M	$538M	$574M	$707M
Cloud cost budget 2021	$500M	$500M	$500M	$500M	$500M	$500M
Deviation from budget 2021 in %	-2.00%	1.00%	3.00%	7.60%	14.80%	41.40%
Deviation from budget 2021 in $	-$10M	$5M	$15M	$38M	$74M	$207M

The $15M investment in risk mitigating efforts allowed the bank to limit their cloud services spend to $15M over budget compared to $25M over budget when taking into account the ex-

pected risk. When comparing the unexpected cost of risk at the 1% level, the total spend drops from $167M to $74M over budget, a cost avoidance of $93M on a $15M investment.

Business Arrangement 3 - Third-party Outsourcing of Cleaning Services

Cleaning services is an important part of a bank corporations facility management budget. A bank with 1,000 branches/offices with an average surface of 3,000 sqft/unit, could spend $3,000/month or $36,000/office/year on cleaning services. Our cleaning services cost of risk example, similar to our previous examples for bicycle import and cloud services, includes:

- the best case scenario
- a cushion for minor anticipated increases
- the expected risk cost such as for example staff costs and fuel, and finally
- the unexpected risk costs such as for data breaches, natural disasters.

The cross cutting risks in certain cases may lead to a significant increase in overall costs for the third-party services. For example, if a malicious data breach occurs at only one of the 1,000 branches then it may lead to a cross cutting risk, like reputation risk, with severe impact on the banking corporation as a whole.

The risk calculations are used to construct a mitigation budget that can be used to enhance items such as on-location security and/or expand due diligence efforts of potential business partners.

As we did in the prior examples, we next review the RACI and contract management tables for cleaning services.

Column 1 in Table 22 indicates whether the activity is a product or a service. Column 2 indicates the overall business area we are examining, in this case Operations. Column 3 provides a rough description of the required service. Column 4 provides the SOW. Column 5 lists the product or service provider name with its respective geographical location (Column 6), tier (Column 7) and geographical supply or service area (Column 8).

Table 22. Cleaning Services: Third-party Management, Part 1

PRODUCT or SERVICE	Business Area	High level service type/ Supply Chain Role	Granular statement of work (SOW)	Third or N-party name	Third or N-party location	Tier	Supply/ Service region
SERVICE	OPERATION	*Cleaning Services for 1000 branches*	3000 sqft x 1000 branches				United States
SERVICE	OPERATION	Cleaning Services vendor for 1000 branches	Described by responsible process owner and signed off by responsible buyer in terms of market availability. Four eye principle to be kept at all times while maintaining an open collaborative working relation between the two.	Cleaning services provider	Chicago	1	United States
SERVICE	OPERATION	Cleaning Services franchisee for 400 branches	Described by cleaning services provider's responsible process owner and signed off by responsible buyer in terms of market availability. Four eye principle to be kept at all times while maintaining an open collaborative working relation between the two.	Franchisee 1	Anaheim	2	West Coast
SERVICE	OPERATION	Cleaning Services franchisee for 300 branches	Described by cleaning services provider's responsible process owner and signed off by responsible buyer in terms of market availability. Four eye principle to be kept at all times while maintaining an open collaborative working relation between the two.	Franchisee 2	Chicago	2	Mid-west
SERVICE	OPERATION	Cleaning Services franchisee for 300 branches	Described by cleaning services provider's responsible process owner and signed off by responsible buyer in terms of market availability. Four eye principle to be kept at all times while maintaining an open collaborative working relation between the two.	Franchisee 3	Trenton	2	East coast

Table 22. Cleaning Services: Third-party Management, Part 1

SERVICE	OPERATION	Cleaning Services equipment supplier	Described by franchisee responsible process owner and signed off by responsible buyer in terms of market availability. Four eye principle to be kept at all times while maintaining an open collaborative working relation between the two.	Equipment supplier	Nashville	3	United States
SERVICE	OPERATION	Cleaning Services products supplier	Described by franchisee responsible process owner and signed off by responsible buyer in terms of market availability. Four eye principle to be kept at all times while maintaining an open collaborative working relation between the two.	Detergent supplier	Germany	3	United States

The third-party (Tier 1) supplier in our example is the cleaning services company under contract. The cleaning services company executes the services through a network of franchisees (fourth party, or Tier 2). There are three franchises in our example that are geographically split with each franchisee covering a portion of the 1,000 offices. The franchisees all use the same supplier for equipment (National Supply) and detergents (Global Supply) which then becomes fifth-party (Tier 3) business arrangements. The contracting bank in our example examines deep tier product contents to be used in their facilities to assess any potential environment risk.

We repeat the type of product/service in Columns 1 and 2 of Table 23 that is followed by the listing of responsibility assignments through Columns 3 - 7. There should not be more than one function who takes the lead role for **A**ccountability. There could be more than one **R**esponsible function or department for a certain area but there should never be more than one process owner per activity. If the accountability is assigned to a specific office or department then it is the head of the department, or the VP/SVP for that process who is ultimately accountable for every preparation, execution and output of that activity.

The **I**nformed and **C**onsulted columns hosts multiple functions and entities. The responsibility to coordinate all tasks rests firmly with a function or entity. The estimated/confirmed budget for the required cloud services is shown in Column 8 for the required cleaning services and Columns 9 - 13 contains the risk assessment overview which will be presented in detail in Tables 25 - 31.

Table 23. Cleaning Services: Third-party Management, Part 2

PROUCTor SERVICE	Busi-ness Area	RESPON-SIBLE Process owner (Supply Chain)	RESPON-SIBLE Buyer	ACCOUN-TABLE Manager	CON-SULTED (CRO, SCRO + any other SME)	IN-FORMED Internal and external stake holders	Total Landed Cost Budget 2022	Risk as-sesse-dat 99% level (latest as-sessed date)	Total risk score	Priority Criti-cal Risks	Stress Test out come	Cost esti-mate Priority Critical Risks (USD)
SERVICE	OPERA TIONS	COO	CPO	CEO	CRO/ SCRO	CEO/ OCC	$36M			1. Internal & External Fraud. 2. Employ-ment practices. 3. Execution. 4. Environ-ment impact.		
SERVICE	OPERA TIONS	CTO Cleaning services provider	CPO Cleaning services provider	COO Bank	CRO/ SCRO	CEO/ OCC	$36M			1. Internal & External Fraud. 2. Employ-ment practices. 3. Execution. 4. Environ-ment impact.		
SERVICE	OPERA TIONS	CTO Cleaning services provider	CPO Cleaning services provider	CEO Cleaning services provider	CRO/ SCRO	CEO Bank	$12M			1. Internal & External Fraud. 2. Employ-ment practices. 3. Execution. 4. Environ-ment impact.		
SERVICE	OPERA TIONS	CTO Cleaning services provider	CPO Cleaning services provider	CEO Cleaning services provider	CRO/ SCRO	CEO Bank	$9M			1. Internal & External Fraud. 2. Employ-ment practices. 3. Execution. 4. Environ-ment impact.		
SERVICE	OPERA TIONS	CTO Cleaning services provider	CPO Cleaning services provider	CEO Cleaning services provider	CRO/ SCRO	CEO Bank	$9M			1. Internal & External Fraud. 2. Employ-ment practices. 3. Execution. 4. Environ-ment impact.		

Table 23. Cleaning Services: Third-party Management, Part 2

SERVICE	OPERATIONS	CTO Franchisee	CPO Franchisee	CEO Franchisee	CRO/ SCRO	OSHA Federal/ Underwriters Laboratory	$1M			2. Employment practices. 4. Environment impact.		
SERVICE	OPERATIONS	CTO Franchisee	CPO Franchisee	CEO Franchisee	CRO/ SCRO	DEP Federal/ FDA	$1.5M			4. Environment impact.		

The first column in Table 24 shows whether a contract is signed or still under negotiation. Columns 2 - 9 contains the sign and expiry dates for the various contracts and commitments linked to the agreement (as required by the corporation and/or oversight bodies). Any action to be taken after a failed or audit-confirmed high risk business arrangement would be entered in Column 10, while Column 11 shows the assigned contract or work order number for each specific agreement.

Table 24. Cleaning Services: Third-party Management, Part 3

Agreement status	Current Agreement Signed Date	Current Agreement Expire Date	Term & Notice	Latest GPC (General Purchase Condition) signed (Date)	Latest Executive Summary signed (Date)	Anti Corruption letter signed (Date)	Latest SSA (Supplier self assessment) signed & received (Date)	SSA on location audit (Date)	Comment on failed SSA audit (incl. time to correct if apply)	Agreement or Work order number
RFI										
Under negotiation										
Existing										
Under negotiation										
Existing										
Under negotiation										
Under negotiation										

As we did in the cloud service case, we next take into consideration the impact that the set of priority critical supply chain risks, inclusive of the cross-cutting risks, has on our budgeted cleaning services cost of $36,000 per branch. We next provide a quantitatively derived risk informed view of our potential costs increase for cloud services over the next year (See Table 25)

We project a **C**ost **I**ncrease arising from **E**xpected **R**isk (CIER) of $3,000 per branch to $39,000. The CIER is based on analyzing historical and projected going forward risk factors for a particular cleaning service risk type (e.g. malicious acts and crimes).

We also calculate a projected **C**ost **I**ncrease due to **U**nexpected **R**isk (CIUR) up to certain level of confidence. In our example, there is a 1% chance that the sum of BC + C + CIER + CIUR is greater than $70,000 per branch. In other words, the sum of the CIER and the CIUR adds $44,000 to the BC + B amount of $36,000 per branch (a 135% increase).

The confidence interval is based on our selected probability density functions (pdf) which best describe the marginal and joint distributions for frequency and severity probabilities associated with a particular cloud services risk type. Observe in Table 25 that the cost for one thousand branches is adjusted to reflect a 1 % chance that the overall cleaning cost is greater than $70 million.

Our risk analysis approach provides greater transparency in terms of the amount of risk taken for cleaning service costs and facilitates the formulating of various mitigation budgets and their respective impact on the overall cleaning cost.

Table 25. Cleaning Services: 3 Cost of Risk Levels (Accumulated)

Per branch + Per 1000 branches	Best Case + Cushion (C)	BC + C + Cost increase expected risk (CIER)	BC + C + CIER + Cost increase unexpected risk (CIUR)	BC + C for all 1,000 branches	BC + C + CIER for all 1,000 branches	BC + C + CIER + CIUR for all 1,000 branches
Cost for cleaning services/branch	$36,000	$39,000	$500,000	$36M	$39M	$70M
Initial cleaning budget/Year	$36,000	$36,000	$36,000	$36M	$36M	$36M

Table 25. Cleaning Services: 3 Cost of Risk Levels (Accumulated)

Per branch + Per 1000 branches	Best Case + Cushion (C)	BC + C + Cost increase expected risk (CIER)	BC + C + CIER + Cost increase unexpected risk (CIUR)	BC + C for all 1,000 branches	BC + C + CIER for all 1,000 branches	BC + C + CIER + CIUR for all 1,000 branches
Cleaning services % of initial budget	100%	108%	135%	100%	108%	135%

The responsibility for preventing security breaches doesn't rely solely on the third-party service provider to perform due diligence such as conducting background checks on their franchisees. The banks internal risk and security culture also has a major role to play as highlighted by the following statements:

'*Tim Roberts of wehackpeople.com, …told Computer Business Review in a DM: "Data mediums may change, but physically accessing said data or the threat of safety will not.*' And as further noted by Shelton Newsham, operator of one of 12 spokes of the NCSC at the regional cyber crime level; *"Communication with corporations is still the Achilles heel. People aren't proactive in coming to us when there's been a breach." "These criminals almost have daily meetings with set objectives, and people are held responsible if these aren't met." "Security teams might meet up fully once a month: they're already 30 days behind. With cyber criminals consistently pushing for access, for lateral movement, it's very hard for CISOs to stay on top of this*[37].

We also analyze the quality of the organization's real estate. For example, storage, offices and customer frequented areas should vary in cleaning frequency and cleanliness as well as for any emergency cleaning needs. Each area needs to be kept safe from a sanitation and infection point of view.

The total cost of ownership includes the cost of cents/sqft (say between $0.07 - $0.20/sqft) and other related items. A well prepared statement of work (SOW), prepared in partnership with subject matter experts, is a necessary input to optimize spend. The SOW separates out what is included in the basic services and what are add-on services. The add-on services may surpass the basic services depending on the final scope of work. The risk analysis should weight the essential services that constitute the main body of the agreement more than services that can

[37] CBR Staff writer., Police Warning: Cyber Criminals Are Using Cleaners to Hack Your Business. Computer Business Review, 2020. https://techmonitor.ai/techonology/hardware/cyber-criminals-cleaners

be eliminated or performed less frequently. For example, the analytic models are designed to optimize the balance between productivity considerations and cleanliness in order to arrive at an optimal cost.

A handful of initial providers are selected based on evaluation thresholds of Quality and Risk. Proposals from the 3 - 5 strongest contenders are next analyzed in detail and subsequently negotiated with to reach an optimal total cost from an optimal vendor for the required services.

Each business area SC's will have different risk priorities. Table 26 provides the priority critical risks. Table 27 shows the cross cutting risks. Table 28 provides the six cumulative cost of risk levels and Table 29 displays the incremental PCR cost breakdown for our cleaning services example.

Table 26. Cleaning Services: Priority Critical Risks

Category (8 inherent Risk Categories)	Sub Category (56 Sub Categories)	Element (198 Risk Elements)
Operational Risk (C2)	Internal Fraud Risk (C2SC1)	Circumventing Regulations (C2SC1E7)
Operational Risk (C2)	External Fraud Risk (C2SC2)	Malicious Acts & Crime (C2SC2E2)
Operational Risk (C2)	Employment Practices Risk (C2SC3)	Safeguard employment practices (C2SC3E1)
Operational Risk (C2)	Execution, Delivery and Process Mgmt. Risk (C2SC7)	Vendor Relations (C2SC7E2)
Environmental Risk (C8)	Environmental Risk caused by own Supply Chain (C8SC2)	Waste Liquid Continuous (C8SC2E4)

Table 27. Cleaning Services: Cross Cutting Risks

Causing categories	Impact on: ->	Financial	Operational	Environment	Political	Business	Reputation	Strategic	Systemic
Risk causing category	Critical SC risks for out sourced Cleaning Services	Y	-	Y	-	Y	Y	-	-
Financial Risk	-	n/a							
Operational Risk	Internal Fraud (circumventing regulations), External Fraud (Malicious acts & crime) Employment practices (Safeguard practices) Execution & Delivery (Vendor Relations)	Y	n/a	Y		Y	Y		
Environment Risk	Environment Impact (Liquid waste)			n/a			Y		
Political Risk	-				n/a				
Business Risk	-					n/a			
Reputation Risk	-						n/a		
Strategic Risk	-							n/a	
Systemic Risk	-								n/a

Table 28. Cleaning Services: 6 Cost of Risk Levels (Accumulated)

Not mitigated				Cost Increase Unexpected Risk (CIUR)		
	Best Case	BC + (C)	BC + C + Cost Increase Expected Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + Stress Test (ST)
Cleaning cost 2021	$34M	$36M	$39M	$54M	$70M	$120M
Cleaning cost budget 2021	$36M	$36M	$36M	$36M	$36M	$36M
Deviation from budget 2021 in %	-5.56%	0.00%	8.33%	50.00%	94.44%	233.33%
Deviation from budget 2021 in $	-$2M	$0M	$3M	$18M	$34M	$84M

Table 29. Cleaning Services: Priority Critical Risk Cost Breakdown

				Cost Increase Unexpected Risk (CIUR)		
	Best Case	Cushion (C)	Cost Increase Expected Risk (CIER)	CIUR with no correlation	CIUR with correlation	Stress Test (ST)
Priority Critical Risks (PCR) cost	$0M	$2M	$3M	$15M	$16M	$50M
PCR 1- Internal & External fraud	$0M	$0M	$0M	$8M	$6M	$24M
PCR 2 - Employment practices	$0M	$0M	$0M	$2M	$5M	$18M
PCR 3 - Execution & Delivery	$0M	$2M	$1.5M	$2M	$1M	$3M
PCR 4 - Environmental impact	$0M	$0M	$1.5M	$3M	$4M	$5M
PCR cost check	$0M	$2M	$3M	$15M	$16M	$50M

Cells marked in red in Table 29 have been prioritized for mitigation due to their impact on the cost of risk. Tables 30 and 31 provide possible counter measures to reduce the cost impact of the PCR's for third-party cleaning services.

As mentioned in the two previous examples, a thorough risk assessment and quantitative deep risk analysis is is necessary to distinguish the risks with the highest overall cost impact on your supply chain. This would be of particular importance in a high rotation in-person domain such as third-party cleaning services.

The risk analytics for the four PCR's for cleaning services in Tables 26 and 29 are used as input to determine the most effective ways to limit any exposure to these risks and their respective impact they may have on your business. We pair these PCR's with examples of mitigating actions in Table 30 as follows:

PCR 1 - lnternal & External Fraud *mitigated by* Enhanced Security routines
PCR 2 - Employment Practices *mitigated by* Clarified Facility Management Supervision
PCR 3 - Execution & Delivery *mitigated by* Agreed SOW & Operational Checklist
PCR 4 - Environmental Impact *mitigated by* Reinforced Transparency Protocol

The first Row in Table 30, shows the risk cost for each risk scenario. Rows 2 - 5 show how much each mitigating action increases or reduces the cost for each scenario while Row 6 shows the total risk mitigating impact. Positive numbers in Rows 2 - 5 are the investments necessary to reduce the cost of risk in each scenario.

In Table 31 we then reintroduce the Row 6 number from Table 30 to show how the mitigating action reduces the deviation from the original cleaning service budget for the bank.

Table 30. Cleaning Services: PCR Costs Mitigating Impact (Incremental)

				Cost Increase Unexpected Risk (CIUR)		
Mitigating activity	Best Case	Cushion (C)	Cost Increase Expected Risk (CIER)	CIUR with no correlation	CIUR with correlation	Stress Test (ST)
Cost per cost of risk level	$0M	$2M	$3M	$15M	$16M	$50M
PCR 1- Enhanced security routines	$3M	$0M	$0M	-$4M	-$3M	$0M
PCR 2 - Clearer facility manage-ment supervision	$1M	$0M	$0M	-$1M	-$3M	$0M
PCR 3 - Mutually agreed SOW with operational checklist	$1M	-$1M	-$0.75M	-$0.75M	-$0.5M	$0M
PCR 4 - Rein-forced trans-parency protocol	$1M	$0M	-$1M	-$2M	-$3M	$0M
Total mitigated PCR cost impact	$6M	-$1M	-$1.75M	-$7.75M	-$9.5M	$0M

Table 31. Cleaning Services: PCR Costs Mitigated Impact (Accumulated)

Mitigated				Cost Increase Unexpected Risk (CIUR)		
	Best Case	BC + Cushion (C)	BC + C + Cost Increase Expect-ed Risk (CIER)	BC + C + CIER + CIUR with no correlation	BC + C + CIER + CIUR with correlation	BC + C + CIER+ CIUR + ST
Total cleaning cost 2021	$34M	$36M	$39M	$54M	$70M	$120M
Mitigated PCR cost impact	$6M	-$1M	-$1.75M	-$7.75M	-$9.5M	$0M
Mitigated total cloud cost 2021	$40M	$41M	$42.25M	$49.5M	$56M	$106M
Cleaning cost bud-get 2021	$36M	$36M	$36M	$36M	$36M	$36M
Deviation from budget 2021 in %	11.11%	13.89%	17.36%	37.50%	55.56%	194.44%
Deviation from budget 2021 in $	$4M	$5M	$6.25M	$13.5M	$20M	$70M

We ultimately calculate the combined bank risk of cloud services and cleaning services exam-ples. For example, we calculate the correlation between the risk components of cloud service and cleaning service in order to subsequently calculate the combined overall cost of risk at the 1% risk level.

V. Summary Conclusions

We have been motivated to dig deeper into the third-party risk management due to the significantly increasing supply chain risk (SCR) at the enterprise level. We argued that integrating risk analytics with supply chain knowledge is necessary to make the root causes of the supply chain risk transparent and pointed out that the utilization of new technologies together with the geographically widening scope of supply chains calls for implementing new approaches to evaluate the impact that emerging risks have on our supply chains. The need to measure and make transparent these emerging third-party risks has, if not before, now become a top priority.

For the updated interagency guidance, we strongly suggest guidance should be organized under three main areas of enhanced focus. These areas/activities also constitute the core of our business arrangement examples and overall contribution throughout our response:

Transparency – of SCR is a critical policy objective. Mapping all activities as well as tiers and responsibilities directly or indirectly involved in each bank's third-party business arrangements is an unavoidable activity in any fact based risk assessment. Our proposed tools for this exercise provide a way forward for how to facilitate making SCR transparent that can easily be adapted to fit any size or type of corporation. Once this first main area is concluded, one would be in a good position to move on to…

Risk assessment - of the multitude of possible risks that each third-party relationship and supply chain is exposed to over their term should be fully documented. For example, a mapping of their respective frequency, severity and impact based on a confidence interval will paint a risk picture to facilitate the management of the priority critical risks, including where the third-party and overall supply chain risk is most vulnerable and therefore exposed to costly losses. The Transparency activity will provide clarity in terms of where and under who's responsibility each PCR would belong and hence the leadership assigned to address the risk and its subsequent mitigations falls naturally.

Risk mitigation and RAROC - calculations that flow from the initial risk assessment along with the PCR's that have emerged, enables the bank to rank them according to potential incremental cost impact on the total cost for each supply chain. The tables in our three business arrangement examples that result from the collaborative effort among the supply chain, the financial and the risk function in the company, provides the components and overall cost impact of four PCR's for each example. The following decisions can now be made: a) what PCR's should we select to reduce the risk by investing in mitigating activities. b) what mitigating activities to address for each specific PCR and c), how much should we invest in the mitigating activity to reach significant reduction in our risk cost for each PCR.

These three overall activities would optimally be done early, ideally at the due diligence and RFI stages of any new business arrangement, as well as to revisit any existing third-party arrangements on a regular basis as conditions can and will change during the term of each arrangement.

The risk management and supply chain communities have not sufficiently interacted with one another. The role that risk management department plays in a supply chain department is minimal in most non-financial organizations when compared to the role that the risk management department plays in a financial organization. We are confident that cross functional meetings will enhance the risk culture for third-party risk and contribute to reducing the type of economic losses due to SCR that so many experienced over the last 18 months.

We believe that what we say in our RFI response will add value to a board or management committee that needs to understand more about the role that a formal risk management organization can play in SCRM. Our RFI response strives to provide a deeper knowledge of SCR at a strategic level (such as for a board) as well as at an operating level for executives who are responsible for managing supply chain on a daily basis.

All of this gets increasingly more challenging as we drill down into the nuances of SCR for a particular industry because it introduces an entirely new vocabulary of risk terms and becomes more quantitative for those responsible for executing supply chain management programs. SME's in supply chain need to work together with risk analysts to measure priority critical risks, find their respective root causes and invest in mitigating measures. As we describe in our business examples, a relatively small investment amount upfront to mitigate the risk can and will save millions of dollars in risk cost avoidance during a disruption mode.

We project that best practice methods for calculating the distributions of frequency and severity to measure supply chain risk will become increasingly common. We showed how the SCR analytics can provide valuable quantitative risk detail for those that are actually managing supply chain risk on a daily basis and expressed these analytics in ways that will be understood without needing an advanced degree in mathematics.

We project that the direct near term cost of risk for third-party and supply chain services will be a significantly increasing cost and exposure for any bank. We pointed out that our estimated dollar figures in our tables may only partially cover losses over time stemming from potential lawsuits and/or reputation damage due to various types of third-party fraud, employment

practices or various types of cross cutting risk. Such costs may well exceed even the total cost for the services themselves.

We hope that our contribution in this paper will be used as input into a go-to guidance document for any organization in the banking sector, including regulators and government entities as well as provide a roadmap that can be used to assess, monitor and manage third-party risk well.

VI. Comments and Recommendations on 'Proposed Interagency Guidance on Third-Party Relationships: Risk Management'

Scope & Goal;

'*to respond and comment on proposed interagency guidance to Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC) and Office of Comptroller of Currency (OCC), on managing risks associated with third-party relationships. Ambition to offer a framework, sound risk management principles for banking organizations, for developing risk management practices for all stages in the life cycle of third-party relationships. The final guidance would replace each agency's existing guidance and be directed to all banking organizations supervised by the agencies.*'

The agencies also seek comments on the following :

- 'Should any of the concepts in OCC's 2020 FAQ's be included in the final version of the new guideline?
- Should any additional concepts that would be helpful be included?'

Our goal is to show the universal applicability of our proposed tools for both smaller and larger banks. Towards this goal, we used practical examples in our response with focus on areas that impact risk across widely different supply chains. We chose Cloud Services and Cleaning Services business arrangement examples since they both constitute typical third party activities which often lead to significant cost of risk exposures. We chose lending to a bicycle business startup in an expanding business sector in order to insert second-party business arrangement risk into our response. We believe examples similar to what we discuss in our response can be used to enhance the proposed guidance toward helping banks manage risks associated with any third-party relationship.

A. General

Q 1. To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures? In what areas should the level of detail be increased or reduced? In particular, to what extent is the level of detail in the guidance's examples helpful for banking organizations as they design and evaluate their third-party risk-management practices?
A 1. As indicated in our **Section I (Introduction)**, we suggest that a greater level of detail should be provided in terms of what is meant by third-party risk management since there are multiple interpretations of third parties and third-party risk management amongst the risk community, business community and supply chain community. We include the entire supply chain in our definition of "third party". For example, a product supply chain consists of a third-party vendor with a fourth-party component supplier and a fifth-party raw material supplier…, and therefore we examine each Kth party in the supply chain for K= 1,2…n as defined in Box 1 on page 3.

Providing detailed Due Diligence guidance for hard to measure supply chain risks such as cyber security risk and knock on impacts such as reputation risk would add value. For example, a cyber security leak would quickly reflect negatively on the bank.

We believe that banks of all sizes with different structures should be able to adjust and adopt the risk management practices described in our submission. As we illustrate in our three business arrangement examples, quantitative assessment of supply chain risk along with continuous monitoring of the risk should be at a granular level. The proposed guidance should include a discussion on how banks of all sizes can perform a quantitative assessment of supply chain risk that is fit for purpose.

Q 2. What other aspects of third-party relationships, if any, should the guidance consider?
A 2. The guidance would benefit from inserting standard cost related terminology to capture the risk at a variety of cost levels.

For example, cost related terminology to capture the risk should include terms like:
- cost of goods sold (COGS)
- total landed cost (TLC)
- total cost of ownership (TCO)

Further, terminology at six risk linked cost levels are as follows;
- A best case

• A cushion
• An expected cost increase risk measure
• An unexpected cost increase risk measure with:
    •no correlation between the risk factors
    •correlation between the risk factors
• A stress test measure

We define these terms in our **Section III (Terminology)** in our submission.

B. Scope

Q 3. In what ways, if any, could the proposed description of third-party relationships be clearer?
A 3. Providing business arrangement examples for different categories of third-party relationships with definitions would add value. For example, categories for third-party relationships could be organized as follows:

- Service providers (e.g. cloud services, cleaning services)
- Customers (e.g. loans made to counter parties, interest rate swaps with counter parties)
- Insurance companies (e.g. hazard insurance, property insurance)
- Fully owned entities
- Partially owned entities[38]
- etc.

As described in Section IV, numerical Business Arrangement examples should be provided to illustrate key points. For example, a comprehensive diverse **list of service providers** would include:

- Cloud services (see **Business Arrangement, example 2**)
- Cleaning services (see **Business Arrangement, example 3**)
- Security
- Data warehousing
- Facility management
- Courier services
- Rating institutions
- External auditors

[38] There is a formal legal definition of ownership such as provided by the global LEI (Legal Entity Identifier) effort where parent and child aspects are tightly defined.

- Accounting firms
- Legal Counseling

Q 4. To what extent does the discussion of "business arrangement" in the proposed guidance provide sufficient clarity to permit banking organizations to identify those arrangements for which the guidance is appropriate? What change or additional clarification, if any, would be helpful?
A 4. A detailed broadened discussion of 'business arrangements' is crucial in terms of determining the scope of the new interagency guidance. For example, as we provide in our submission, it would be beneficial to make the discussion more specific with numeric examples in order to support establishing new or updated risk management practices. Further, it would be important to make sure the list of business arrangements is comprehensive. For example, the document doesn't cover business arrangement without a contract.

Q 5. What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third parties?
A 5. Providing country specific compliance requirements for third parties such as a list of mandatory third-party monitoring requirements of each country's national laws and regulations would be useful. For example, this list would include compliance related to any laws and precedents related to data infringement and laws related to internal and external data fraud. Due diligence may also include checking to see if there is a rating of the data security from an independent global bona fide source.

Providing business arrangement examples of best practice country specific approaches to performing a due diligence process such as liability related questions in terms of employer/employee relationship (Including third-party NDA documents), currency specific risk considerations and such, would also be useful.

C. Tailored Approach to Third-Party Risk Management

Q 6. How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?
A 6. Providing educational tools with numerical examples along the lines we describe in our three business arrangement examples should be included in order to standardize the policies, methodologies and infrastructure aspects that are necessary to roll out a scaled bank-wide third-party risk management program. The educational tools should be used facilitate a global train-the-trainer program, which in its initial stage should be carried out by in-house educators

but could partially be outsourced. Roles and responsibilities associated with the third-party risk management program should include Level 4 processes to better understand and operationalize flow charts along with RACI-charts[39].

Q 7. In what ways, if any, could the proposed guidance be revised to better address challenges a banking organization may face in negotiating some third-party contracts?
A 7. Providing basic sourcing and procurement third party servicing training, along with negotiation techniques, would address many of the challenges a banking organization may face in negotiating third-party contracts. The training would include examples similar to what we describe in **Section IV**. The training can be carried out in collaboration between in-house trainers together with external consultant on topics such as best practices for conducting operational due diligence (ODD) and making risk calculations such as stress tests of third-party risks.

Q 8. In what ways could the proposed description of critical activities be clarified or improved?
A 8. Providing examples of critical activities and the associated priority critical risks along with risk mitigation activities that worked well (or didn't work well) to mitigate these critical risks would add value to the proposed guidance. Let's examine two routine illustrative examples that may fall under the radar as follows:

1. A single critical routine activity like waste management can cause severe injury or infection risk. A potential third-party vendor in a due diligence process may respond that risk mitigating measures for waste management are in place. An on-location audit is a useful exercise to establish the effectiveness of such risk mitigating measures. If not in place, then lackluster risk mitigation measures can severely harm both the employees of the vendor and the reputation of the bank.
2. Non-discrimination clauses are routinely required from or offered by a majority of third-party service providers in their contracts. Despite this fact, there are frequent hidden and publicly exposed breaches to these protocols which suggests that any company (or buyer) must go deeper into the service providers internal routines to ensure that a non-discrimination culture is truly implemented in their operations.

If organizations deploy the risk mitigation activities described in our three business arrangement examples along with our proposed Supplier Self Assessment tools shown in Appendix 1, then the risk of negative occurrences will be significantly reduced.

---

[39] '…level of process that people mean when they talk about "end-to-end" processes, because these processes typically begin with a market or customer input (an order, a product idea) and end with an output that either goes to the customer or becomes an input to another stage of the value chain.' Ramias, A. When you say "Process," You Mean…?' bpminstitute.org https://www.bpminstitute.org/resources/articles/when-you-say-process-you-mean%E2%80%A6

D. Third-Party Relationships

Q 9. What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third parties?
A 9. Providing documents that describe how to make a quantitatively based risk assessment for a variety of third-party business arrangements, including a full-scale check-list to ensure that every possible inherent risk has been assessed according to a taxonomy similar to what we describe in Tables 6, 16 and 26, would add significant value. We provide a partial list of critical risks from our risk register for each example in Section IV for each of our three business arrangement examples. Providing a:

- database of historical performance that includes examples that show the amount at risk based on the historical frequency and severity statistics.
- description of best practice approaches to mitigate the risk along with the root cause of the risk that we describe in our three business arrangement examples,

would also add value.

Q 10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?
A 10. Revisions on a regular schedule such as quarterly, bi-annual or annual (at a minimum) would assist banking organizations in assessing third-party risk. The revision would include the latest development of any inherent risk exposure stemming from technology evolution.

Q 11. What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third-party platforms that directly engage with end customers?
A 11. Requirements for managing risk associated with third-party platforms that directly engage with end customers, such as data loss prevention and fraud prevention platforms, should be addressed at the Statement of Work (SOW) stage. Guidance should provide illustrative examples of relevant tools and templates for good practice to manage this risk anywhere along the supply chain similar to what we provide in Tables 12 - 14 for our cloud services example in **Section IV**.

Q 12. What risk management practices do banking organizations find most effective in managing business arrangements in which a third party engages in activities for which there are regulatory compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?

A 12. A General Purchasing Conditions (GPC) document (or the equivalent) that we discuss in Table 3 can be used to fully articulate regulatory compliance requirements for third parties. For example, the GPC can be used to make transparent and facilitate the monitoring of multiple rules and regulations to fully adhere to local and regional laws that influence various aspects of the preparation and delivery of third-party services and products.

Guidance can assist banks in managing the compliance risks of business arrangements by providing examples of supplier self assessment (SSA) templates and associated working method similar to what we discuss in Table 14 and share an example of in Appendix 1. Guidance should include a comprehensive checklist for banks to include in their due diligence activity that need to be periodically performed as part of an ongoing third-party performance monitoring process, inclusive of references to general national and global compliance sources.

E. Due Diligence and Collaborative Arrangements

Q 13. In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?
A 13. Sharing third-party due diligence would certainly add value. Nevertheless, a third party would normally be reluctant to share proprietary non-public information (say without an NDA) which by definition would prevent it from being shared.
It would be worthwhile to examine special corner cases where a general modified NDA language could be constructed which makes it mandatory for any company wanting to offer goods or services to have a portion of their answers shared with banking organizations in a Banking Sector GPC that we discuss in Table 3. Further, there could be certain cases that require a company to make available certain information in terms of previous violations with access given only to authorized banks. There are multiple indirect ways for companies to share due diligence. For example, companies can be listed as they pass various certifications such as: 1) ISO certifications for data security[40], 2) approvals from federal agencies like the Food & Drug Administration (FDA) and 3) approvals from global certification companies like Underwriters Laboratories (UL) to ensure the prospective third-party vendor meets the stipulated requirements to actually deliver the contracted products or services to their intended markets.

Q 14. In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed

[40] ISO/IEC 27001 Information Security Management. https://www.iso.org/isoiec-27001-information-security.html

guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?
A 14. Initiating the proposed guidance process with a supplier self-assessment (SSA) that we discuss in our three Business Arrangement examples in **Section IV** and show in Appendix 1, serves to make the due diligence process more cost effective. The SSA should be constructed to fit the unique requirements of a particular type of company such as utilities, consortiums and standard-setting organizations.

F. Subcontractors

Q 15. How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships? To what extent would changing the terms used in explaining matters involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance? What other practices or principles regarding subcontractors should be addressed in the proposed guidance?
A 15. The proposed guidance should provide clarity on conducting due diligence for subcontractor relationships by clearly describing what each term means similar to what we did in **Section III**. For example, synonymous terms could be added for increased clarity such as the the various definitions of fourth parties[41]. A description of what the guidance covers as well as what it doesn't cover should be included.

Providing examples in the guidance of good practices, such as implementing third-party risk and performance management systems that are fit for purpose, similar to what we discuss for the three business arrangement examples that we describe in **Section IV,** would be well received. Good practice also includes providing the tools for appropriate management action such as following up early on any troubling incident reporting as well as communicating frequently with the third party to obtain early warnings on a priority set of critical risk similar to what we describe in Tables 6, 16 and 26.

Q 16. What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?
A 16. The primary factors for determining the types of subcontracting a bank is comfortable accepting in a third-party relationship includes having the right policies and methodologies in

[41] A fourth party can also be defined as: a) a Third party's sub-supplier, or, b) a Tier 2 supplier or Tier 2 service provider. Definition of Fourth party: Venminder Experts., 2019, 'Fourth Party Vendors: How Far Do You Need to Go?', venminder.com https://www.venminder.com/blog/bank-credit-union-4th-party-vendors-management

place to manage the risk. For example, measures of risk include calculating the expected (CIER) and unexpected (CIUR) cost increases described in Section II. The bank needs to trade off items such as cost efficiency, quality of service and amount of risk. Ultimately, the bank may wish to keep any IP-related assets in-house regardless of risk return considerations.

If the cost efficiency and risk analysis are properly conducted then the bank can subcontract a substantial portion of their third-party risk. Nevertheless, if the bank has strong risk mitigation and cost efficiency capabilities then it may be financially motivated to keep this capability in-house. The bank may however, wish to keep any IP-related assets in-house regardless of cost-benefit.

G. Information Security

Q 17. What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?
A 17. The proposed guideline should provide information with examples on the new vulnerabilities that banks face that have emerged through third-party fintech companies as well as an extended IT supply chain. This information would add value to banks who are increasingly focusing their in-house IT to focus on their core competencies and outsourcing the rest to other specialists such as cloud service providers to innovate new services cost effectively.

A deep, multi-layered and highly specialized supply chain exposes financial institutions to new risks, threats and vulnerabilities. The multiple layers of that chain obscure those risks. Ultimately, the information should help financial institutions measure the third-party risk, using the risk measures we discuss in **Section IV**, that the institution faces from its outsourcing choices.

H. OCC's 2020 FAQ's

Q 18. To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?
A 18. If any of the OCC 2020 FAQ concepts are deemed mandatory, we recommend they be included in the type of guidance we discussed in our submission[42]. If the concepts are more in the form of suggestions and recommendations then we believe it would be sufficient to include them in a separate section such as in an Appendix.

[42] See also our expressed views on OCC's 2020 FAQ's incorporation in Section VI.

Conclusion and closing comments to the 18 Questions:

We decided to dig deep into the overall subject of third-party risk management in our response due its complexity and the need to develop practical third-party risk solutions across the entire supply chain. We believe that the material introduced in our response can be used by oversight bodies, banks of any size or structure and risk management executives alike. The majority, if not all, of our answers in response to the interagency questions should find its corresponding responses in our material.

Authors:

Dr. Bob Mark
*Dr. Bob Mark, Managing Partner at Black Diamond Risk Enterprises***,** *serves on several boards, led Treasury/Trading activities and was a Chief Risk Officer at Tier* 1 *banks. He is the Founding Executive Director of the MFE Program at UCLA, co- authored three books on Risk Management and holds an Applied Math PhD. Bob* is a past *GARP Risk Manager of the Year and is a cofounder of PRMIA.*
Contact: bobmark@blackdiamondrisk.com

Holger A. Carlsson
Holger A. Carlsson, Founding Owner at Carlsson International, specializes in supply chain process improvement, works with ThroughPut inc using AI for supply chain visibility. As Managing Director at IKEA, developed and led several global procurement organizations in Europe and North America and was awarded Six Sigma Process Improvement Project of the Year. As Section- and Service Chief at the United Nations Supply Chain Management, created and implemented cross functional performance management operational guidance for all UN field missions.
Contact: hac@carlssoninternational.com

VII Appendices:

Appendix 1. Banking Sector supplier self assessment (SSA)

Page 1 - SSA Introduction letter (example)

Oct 15, 2021

This is a generic document used for suppliers
offering all types of products and services.

Request for Information

Third-party Supplier Self Assessment (SSA) for potential banking sector vendors

Dear Vendor,

Thank you for taking the time to complete this questionnaire. It is of utmost importance for our entire industry sector to ensure that all our vendors and other third-party providers are and act like good corporate citizens. This also applies to sub-suppliers and further back in the supply chain in order to assess and mitigate any potential safety, security and costly risks. The following questionnaire focuses on your standards and priorities on Environmental and Social aspects in addition to requirements on quality and service assurances for your products and services.

It is a prerequisite to have all questions answered to be considered as a banking sector supplier. It is considered a generic document used for suppliers offering all types of manufactured products and services.

If any of the questions do not apply to you, please briefly explain why. The yellow answer section will expand to accommodate your text. Please reply electronically, either as an attachment to an e-mail.

Yours sincerely,

The Requesting Organization

Page 2 - SSA Questionnaire (example)

Oct 15, 2021

EXAMPLE!

US Banking Sector questionnaire

Supplier Self Assessment

Supply Chain Quality, Social and Environmental compliance

Supplier name: _____

Address: _____

_____

Contact person: _____

Date _____

	Questions If a question does not apply to you, please briefly explain why. The yellow answer fields expand to accommodate your text. If more space is needed, simply use a separate Word document clearly indicating question number and attach with finalized questionnaire.	Answers
1	What applicable licenses and certifications does your business/facilities have in order to be legally compliant to carry out all your production/services commitments? Please list all your licenses & certificates in your answer.	
2	Have you read, understood and agreed with the "Banking Sector guidelines"? Please include any comments or information you may have in your answer.	
3	How do you maintain records on working hours, wages and other working conditions?	
4	What insurances for medical treatment and lost wages does your employees have access to in case of a work related accident?	
5	Do you, or have you in the past, made use of child labor, forced labor or bonded labor? If Yes, when and why? Please describe circumstances and and whether or not this was in violation of local laws and standards.	
6	Do you require documentation from your co-workers, foreign or domestic, that they are of legal working age and legally able to work in the country? If yes, what documentation is obligatory?	
7	Does your company, or any of your sub-suppliers, have an impact on the environment as result of your/their production or operation? If No, please explain how it is monitored. If Yes, please explain how and why.	
8	Are your employees exposed to safety hazards which could pose a risk to their lives or cause severe injury?	
9	Please list what programs, committees, certifications or other initiatives you have in place to ensure legal compliance and continuous improvements in Environmental, Social and Quality compliance.	
10	If wood is an important component in your products, how do ou trace the original source of the wood?	
11	How and where are the final and in production inspections of products or services performed? With what frequency is this taking place and how and to whom is the information shared?	