Creating Reliable Risk Assessments:

How Financial Institutions Can Overcome Bias and Structural Obstacles to Better Understand Risk

NCONTRACTS
The Upside of Risk

EXECUTIVE SUMMARY:

This whitepaper explains how financial institutions can avoid common pitfalls to conduct reliable, consistent, and timely risk assessments. From the risk management lifecycle to learning how to recognize internal biases to practical exercises in assessing risks and controls across four key areas (BSA/AML/OFAC, GLBA, compliance and cybersecurity), it will demonstrate the necessary steps and mindset for conducting effective risk assessments.

INTRODUCTION

Risk is unavoidable, but it's not unknowable. While every financial institution faces its share of surprises and setbacks, many of the risks of doing business can be identified and mitigated with the help of thoughtful risk assessments.

The key word here is thoughtful. When conducted properly, risk assessments are highly effective tools that help ensure risk is aligned with an institution's strategic objectives. A well-executed risk assessment digs into real-world risks and the specific controls an institution uses to mitigate their impact, allowing the board and management to make better, more insightful decisions. From big picture ideas to specific areas of concern, a good risk assessment looks at the good and bad in every situation to provide a thorough understanding of threats and opportunities.

The applications are broad. From observations on potential new products and services to setting budget priorities to pointing out areas in need of compliance reviews, a smart risk assessment gives the board and management a valuable viewpoint. It can uncover weaknesses in controls or risk scenarios when disaster planning, shed light on policies that act as controls, aid with vendor selection and ongoing vendor management, and suggest improvements.

But that's only when they are done correctly. Inconsistent and unreliable risk assessments can cause an institution to make poor decisions by providing inaccurate information. This happens when:

- **Risk assessment processes aren't consistent across the organization, leading to varying definitions of risk in each department and more potential risk exposure.**
- **Employees fail to identify potential risks because they are afraid it will reflect negatively on their performance.**
- **Employees don't know what the parameters are.**
- **There is no ongoing process or reliable checkup to ensure that risk controls are valid throughout the risk lifecycle.**

This whitepaper explains how financial institutions can avoid these and other issues so that they can conduct reliable, consistent risk assessments. From the risk management lifecycle to learning how to recognize internal biases that can color assessments to practical exercises in assessing risks and controls across four key areas (BSA/AML/OFAC, GLBA, compliance and cybersecurity), it will demonstrate the necessary steps and mindset for conducting effective risk assessments.

> A well-executed risk assessment digs into real-world risks and the specific controls an institution uses to mitigate their impact, allowing the board and management to make better, more insightful decisions.

THE RISK ASSESSMENT LIFECYCLE

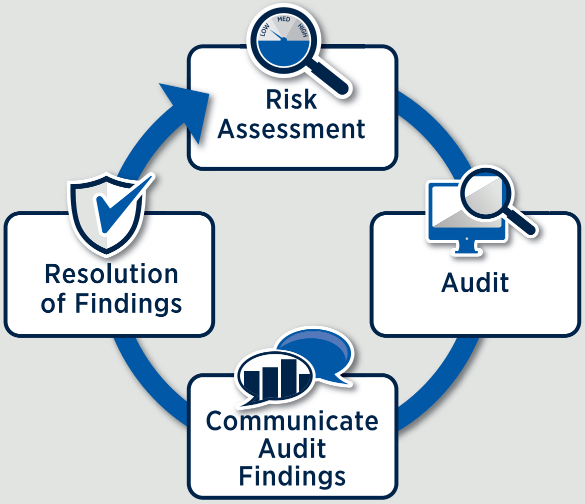
Too many financial institutions view risk assessments as one-time events. They gather information to help set strategy and make operational decisions. Once they identify risks that could derail strategic objectives, the assessment is forgotten.

That's a mistake. A risk assessment isn't an event or an item that can be completed once and crossed off a checklist. As the world both outside and inside an institution evolves, so does the institution's risk exposure. An institution must actively engage in risk management, assessing risk and making adjustments to ensure its risk exposure is aligned with its goals. This active engagement is needed to determine if those goals are even still appropriate.

> An institution must actively engage in risk management, assessing risk and making adjustments to ensure its risk exposure is aligned with its goals.

A risk assessment is just the first step in the risk assessment lifecycle, a multi-step process that includes audits, findings, and action based on those findings. On its own, a risk assessment is a valuable tool, but it's just the beginning. Without follow up to ensure that the information it contains is used, evaluated and updated, it quickly becomes a dead document.

The diagram below depicts the risk assessment lifecycle. It begins with the risk assessment. Once the risk assessment is completed, its insights are used to drive the scope and frequency of audits. Recommendations from the audit are then passed on to management, who review the findings and make decisions to accept, defer, or reject the recommendations. This often involves updating risks and controls, beginning the cycle begins anew.



Risk Assessment Lifecycle

Initially the lifecycle was developed as an annual exercise, but realistically it has been extended to roughly once in-between examinations. The FFIEC Audit Guidance suggests that the audit frequency of any particular control is directly related to the inherent risk value that the control remediates. For example, controls that remediate high inherent initial risks should be audited at least annually. Controls that remediate low inherent risks can be audited every three years.

THE RISK ASSESSMENT PROCESS

Now that we understand where the risk assessment fits into the overall risk assessment lifecycle, let's delve into the specifics. Before starting a risk assessment, it's essential to bring together all of the actors and agree upon some basic ground rules. These include:

1. **Establishing the context**
2. **Risk identification**
3. **Risk analysis & evaluation**
4. **Risk treatment**
5. **Monitoring and review**
6. **Communication**

1. Establishing the context

An accurate risk assessment is only possible when the whole team knows what is being assessed and how it works. The institution needs to decide on the specific business activity, process or project that is going to be covered to determine the scope or context of the risk assessment. This can be a broad category like operational risk or credit risk or a specific department, product or service like compliance, credit cards or mobile banking. Periodically assess each business line, product, service, or system against each risk category to identify key risk drivers.

Once the area is selected, the institution needs an extensive review of background information. Business plans are an excellent source of information, helping the team to understand management's objectives. It's also important to understand management's risk tolerances and thresholds. Look at marketing plans to determine what and how the organization plans to communicate to those who use its products and services.

> An accurate risk assessment is only possible when the whole team knows what is being assessed and how it works.

Review the results of any strengths, weaknesses, opportunities and threats (SWOT) or political, environmental, social and technological (PEST) analysis as well as ratio analysis. Determine if there have been any changes to applicable guidance since the last assessment.

This information will help ensure that assessors aren't working in a vacuum. The more they know about how an area functions and where things can go wrong, the more equipped they'll be to address those risks. It also ensures they are looking at the same defined area.

2. Risk identification

Every institution faces a host of risks and opportunities. Some of them are obvious while others are harder to sleuth out. The most common categories of risk include operational, transaction, compliance, credit, strategic, reputation, third-party, cyber, and concentration risk. An effective risk assessment probes deeply into these broad categories and explores risk at a granular level. Checklists, roundtable discussions, and existing management reports can be great sources for brainstorming potential risks. Go beyond the obvious, easy-to-spot risks. This takes time and creativity, but will result in a vastly improved risk assessment.

> Gauging risk in the absence of any controls. is a very subjective task, which makes it necessary to have guidelines in place to help assessors understand what defines risk categories.

Use this time to think globally about the broad range of things that can go wrong at institutions of a similar size and type. A mid-sized community institution shouldn't necessarily compare itself to a multi-national organization, nor should it rely exclusively only on its own experiences. The guidance from federal regulators and the FFIEC can help guide this process.

3. Risk analysis and evaluation

Like a panel of judges, the job of a risk assessor is to evaluate the institution's level of risk by measuring and scoring two key forms of risk: inherent risk and residual risk.

Inherent risk

Inherent risk scores represent the level of risk an institution would face if there weren't controls to mitigate it. For example, think of the risk of a cyberattack if the institution didn't have any defenses in place.

One way to look at inherent risk is through the following formula:

Inherent risk = Impact of an event * Probability

This formula demonstrates the relationship between an event's impact and its probability when determining inherent risk. The impact is an estimate of the harm that could be caused by the risk. For example, a cyberbreach could have a catastrophic impact. Probability is how likely a risk is to occur. For example, a cyber breach seems a very likely occurrence when there's no firewalls, anti-virus software or intrusion detection software to prevent it.

Gauging risk in the absence of any controls is a very subjective task, which makes it necessary to have guidelines in place to help assessors understand what defines risk categories and whether risks are labeled "high," "moderate," and "low" or "catastrophic," "significant," "moderate," "minor" and "insignificant." Guidelines limit subjectivity and add objectivity. For example, a guideline for probability might include frequency of audit findings. An audit finding from the past year may indicate a risk is highly likely/probable while one from five years ago with no repeat findings may indicate an unlikely or remote risk.

> "If everything is important then nothing is."
>
> —David Wilhelm

The overly cautious might be tempted to label every risk a significant or high risk, but that's a terrible idea. In a world with limited audit resources, it's incumbent on assessors to provide information about where to best spend those resources. If every risk is labeled with the highest possible risk level, the board won't know where to deploy resources. Higher residual risks should be addressed more frequently and their control effectiveness reviewed more aggressively. That can't be done if every risk is a labeled a high risk.

Residual risk

Residual risk is the risk that remains after controls are taken into account. In the case of a cyber breach, it's the risk that remains after considering deterrence measures. This score helps the organization review its risk tolerance against its strategic objectives. It's all about understanding the relationship between risk and controls. This relationship can be demonstrated with the following formula:

Residual risk = Inherent risk * Control effectiveness

Residual risk is greatest when the inherent risk is high and the controls for mitigating the risk aren't effective. It decreases when controls are effective.

That makes it important to have a method for determining how effective controls are. This comes down to two factors: the impact of the control and how likely it is to work. This relationship can be expressed with the following formula:

Control effectiveness = Control impact * % ineffective

A control's impact is the expected value of its risk mitigation. A control can be viewed as very important, important or not very important. For example, a firewall can be very important for keeping out hackers because it covers the entire institution. A control's effectiveness is the probability that the control will function as intended based on assessments. When it comes to firewalls, monitoring reports can show evidence of the firewall fending off specific attacks, but it may also indicate that occasionally a new attack has made some inroads. When assessing effectiveness, make sure controls are regularly monitored for trends to help understand if they are performing as expected.

When determining impact and probability for risks and controls, draw on the background information gathered and address the issue with an open mind.

Consider the risk of a fire. A fire can have a huge impact, but many don't consider it a high risk because it may seem unlikely. Often that's because they've never experienced a fire or don't know anyone who has. Fires seem like rare events.

However, these individuals are failing to properly consider the inherent risk: the risk in the absence of controls. The reason there are relatively few building fires is that the modern world has many tools to prevent fires. We don't heat our homes with open flames or use oil lamps and candles for lighting. There are building and electrical codes, sprinkler systems, and fire-resistant building materials. Take those controls away and fires become more common. This is an example where personal experience may cloud practical judgement. Fire is an inherently high risk.

> Different controls work better in different situations and some are just more effective at mitigating risk than others.

Now let's look at controls. There are multiple controls to mitigate the inherent risk of a fire, including fire extinguishers, sprinkler systems, smoke detectors, alarm systems, etc. While these can all be valuable controls, they are not equal. Different controls work better in different situations and some are just more effective at mitigating risk than others.

For instance, a fire extinguisher has a lower expected risk mitigation value than a sprinkler system. It simply isn't of much value in the event of a large-scale fire. Therefore, if an institution doesn't have as many working fire extinguishers as it should, but its sprinkler system is operational, the fact that its fire extinguishers aren't 100 percent effective won't necessarily have a dramatic impact on the residual risk. Conversely, if there are plenty of operable fire extinguishers but the sprinkler system isn't working properly or consistently, then the residual risk would be impacted because the sprinkler system is a more impactful control.

The same control can have a high impact score in one situation and a low impact score in another. The difference is the situation in which it is used. For example, a handheld fire extinguisher is great for a small, contained fire, but not particularly helpful if the building is already engulfed in frames. When thinking about the impact rating, assume that the control is being used for its intended purpose. Also think about how a control can fall short. A handheld fire extinguisher won't work unless someone knows where the fire extinguisher is and how to operate it. The extinguisher must be fully charged. If any of these items is missing, the probability that particular control will be effective is lowered.

A fire is a common example used in risk management, but let's apply this logic to something a little more relatable to the banking industry: collecting data for the Customer Identification Program (CIP) provisions of the USA PATRIOT Act. The PATRIOT Act requires that an institution collect five key pieces of customer information before opening an account. A review of enforcement actions related to anti-money laundering violations indicates there is a significant inherent risk in failing to fill this requirement.

This risk can be reduced with several controls. They include:

- **Automated software that prevents an account opening from moving forward without the information.**
- **A checklist for employees.**
- **Quality control by double checking a sample of new accounts.**

On the surface, these all seems like great controls, but assessments over time can demonstrate the strengths or weaknesses of each control.

For example, the automated software ensures that information is entered 100 percent of the time. No fields are left blank. However, it can't guarantee that the correct information is entered. The checklist has potential for human error and an assessment may demonstrate that employees often skip this step. Finally, an assessment of quality control procedures may show that it's extremely effective in ensuring the proper information is entered, but it's only used on a sampling of new accounts because it's too time consuming to do for each new account.

The fact that the institution is inconsistent on the checklist, a relatively unimportant control, probably won't have a huge impact on the institution's overall residual risk. It might even decide to discontinue the control due to its ineffectiveness. It all comes down to risk tolerance and effectiveness. If after assessing its controls, it decides the residual risk is too high, it can introduce new controls or dedicate more resources to existing ones.

That's why it's important to think locally when it comes to scoring controls. While an institution should draw from peer institutions' experience when thinking about potential risks, control scores must be specific to the institution being assessed. This is one instance where it doesn't matter what the institution down the street is doing.

Risk and control scoring

To compare risks and controls, it's necessary to have a scoring system. The way that scale is structured can influence risk and control scores. Some institutions use a three-point scale of high, medium and low. Others use a five-point scale since it offers more nuance. For example, risk can be rated on a scale from 1 to 5 with 1 representing a low risk and 5 representing the highest possible level of risk. Others use terms like catastrophic, significant,

> While an institution should draw from peer institutions' experience when thinking about potential risks, control scores must be specific to the institution being assessed.

moderate, minor, and insignificant. Similarly, controls can be ranked on a scale of 1 to 5 with 1 representing controls that do the least to reduce risk and 5 representing those that are the most effective. Others use terms to assess the probability that a control will be effective. These can include "certain," "likely," "possible," "unlikely" and "remote."

The scoring of risks and controls can be time consuming, especially when the process turns into scoring debates. If this happens, change gears to make sure those debating the scores have a similar understanding of the risk or control. Time spent on education pays far larger dividends than debates on individual scores. Instinctive reactions are far more likely to be accurate when assessors share a common knowledgebase. Without that knowledge, they are just guessing and risk assessments will not be consistent.

4. Risk Treatment

Once risks are identified and assessed, an institution needs to be sure it understands those risks. It should consider a variety of options for mitigating them and settle on a plan. That plan should identify risk owners, typically departments or business processes. There also needs to be a risk manager tasked with remediation and implementation under a specific timeframe. The institution should also think about establishing an early warning system using Key Risk Indicators (KRIs) and other regulatory monitored ratios or data so it is aware when risks are evolving.

5. Monitoring and Review

Once risks are known and understood, they must be monitored and reviewed. The institution should have thresholds in place and a plan for acting on new information. For example, if the institution has a KRI early warning system, there should be policies and procedures in place for determining when action is necessary and when a wait-and-see approach is appropriate.

Change is inevitable and an institution needs to decide when it will update its risk assessment. Will it update the risk assessment on an as-needed basis or wait until the designated risk assessment? To properly manage risk, updates should be made in as close to real time as possible. Manage risks, not risk lists.

A timely response to all risk assessment and remediation efforts is essential. Management and the board need all the relevant information so that they can study both the risks and the opportunities.

A timely response to all risk assessment and remediation efforts is essential. Management and the board need all the relevant information so that they can study both the risks and the opportunities.

6. Communication

An institution can have the most carefully thought out risk assessments and intricately crafted risk tolerances, but if they aren't communicated throughout the institution, they are almost worthless. Risk management must be part of the institution's culture. Otherwise, it's just going through the motions.

This can be communicated by training, but only if it is presented the right way. Training shouldn't just tell people what they should and shouldn't do. It should explain the reasoning for why activities are encouraged or prohibited so that employee learn how to manage risk. Consistent communication is essential and should hold up successes just as often as it highlights failures.

CONSISTENCY MATTERS

In a simple world, one person or department would be responsible for conducting every risk assessment. The same approach would be used each time, ensuring consistency.

Unfortunately, nothing is ever simple. At the typical institution, management reviews the results from a variety of risk assessments from every corner of the organization. That makes a consistent approach to preparing and reporting of risk assessments absolutely essential. This includes:

- **Similar approach and methodology.** While risk assessments are subjective, everyone working on a risk assessment should be aware of how others in the organization are approaching their assessments and the form that those assessments take.
- **Risk and control scores.** The same scales with the same meaning should be used across the institution. A moderate risk rating should have the same meaning for all of the organizations assessments.
- **Formulas for calculating initial and residual risks.** These should be consistent in every risk assessment.
- **Use of initial and residual risks.** These should be consistent throughout the various risk assessments. It may seem obvious, but there are institutions where one risk assessment considers only residual risk while another assessment in the same organization only considers inherent risks.

Risk assessment consistency isn't just a lofty ideal. It has practical value. Consistency allows for easier comparison and provides a common language for understanding what the results of each risk assessment means. It allows risk assessments to build off each other, facilitating meaningful year-over-year comparisons and department-to-department comparisons that help gauge changes in inherent or residual risks. It ultimately allows the institution to better align strategic objectives and attain goals.

> Risk management must be part of the institution's culture. Otherwise, it's just going through the motions.

OPTIMISM BIAS: THE ENEMY OF OBJECTIVITY AND CONSISTENCY

Every person brings her own background and experiences, and those influence her risk assessment decisions. While these experiences can bring valuable insights, they can also color decisions in a negative way. One of the most common problems is a phenomenon known as optimism bias.

> Being aware of the existence of potential biases can go a long way towards minimizing their impact.

Optimism bias, also known as unrealistic or comparative optimism bias, is a person's belief that he is less likely to experience a negative event compared to others. For example, when it comes to the risk of a fire, people might think it's unlikely because they haven't experienced one before, haven't experienced one in this location, or haven't seen or heard of many fires from friends or news reports. These may be accurate and logical statements, but these perceptions are also distorting risk scores. A fire can happen to anyone.

Optimism bias can creep into a risk assessment whether it's performed by a single person or a group of people. Being aware of the existence of potential biases can go a long way towards minimizing their impact. Common forms of optimism bias to be aware of include:

- **Rule of thumb.** We think bad things happen to other organizations because they don't follow the rules. We tell ourselves that since we follow the rules, we have less risk. Rule of thumb bias makes us compare ourselves with the negative elements that come to mind instead of making an overall comparison.
- **Singular focus.** It's natural that we know more about our organization than we do about others. Since those firsthand experiences feel more real, we tend to generalize when it comes to others and focus on our own feelings and experiences. This can cause us to neglect the reality of the average organization. This singular focus on self can be avoided by actively working to take a broad view of risks and thinking globally. Risk discussion from guidance also helps minimize the effects of singular focus in risk assessments.
- **Interpersonal distance.** Perceived risk differences depend on how far or close any particular risk is to the individual making the risk determination. The further the distance, the more vagueness gets introduced into the determination process. Read up on peer institutions that have dealt with situations to remind your team you're not immune to their problems.
- **Expected outcome.** This is when risk assessors are influenced by the goals of the organization. The result is that the assessor sees what he wants to see instead of the actual risks. Make sure assessors know they won't be penalized for honesty.

Optimism bias can also affect control scores. It's perfectly natural for us to feel that we have more control over situations than we might realistically expect. Sometimes that perceived control is real. Other times it's not. Imagine a passenger riding shotgun with a friend who just bought a brand-new sports car. The passenger is gripping the dashboard with white knuckles and begging his friend to slow down while zipping down on a windy road. The driver responds by praising the car's superb handling. The difference here is perspective. The passenger doesn't have any control over the situation. The driver is impressed by how well the

car handles curves and the gas pedal's responsiveness. If the driver and passenger were to stop and switch positions, the tables may turn.

When assessing controls, consider the viewpoint of both the proverbial driver and the passenger. The truth is probably somewhere in between.

AVOIDING COMMON MISTAKES

When conducting a risk assessment, the role of the assessors is to rate risks and controls as accurately as possible. Some people make the mistake of confusing a risk assessment with a job performance review. They don't want to give a bad grade so they err on the side of optimism. Assessors must be reminded that their job isn't to push for organizational objectives or to make people look good. The job is to form as complete a risk picture as possible so the institution can make smarter, more informed decisions.

Another common mistake is letting the goals of the organization bias the risk assessment to paint a picture others want to see. The role of a risk assessor is not to fulfill the goals or desires of the organization. It shouldn't be based on expected outcomes. That denies management the opportunity to be aware of issues and take appropriate steps to accept or remediate the risk.

Other times risk assessors avoid showing too many "red" rankings and aim for "green" because they fear getting someone in trouble. This is a mistake. It can't be said enough: Risk assessments are not performance reviews. Risk is a part of business, and different parts of the organization will have different degrees of risk. Having a high initial or residual risk rating does not necessarily mean that someone is doing a poor job. Just think of cybersecurity. The inherent risk of a breach when there are no controls is extraordinarily high. Pretending it isn't won't help the institution make smarter cybersecurity decisions. It will only give it a false sense of security. The same is true of controls and residual risk. Even with controls in place, sometimes risk remains high.

It can't be said enough: Risk assessments are not performance reviews.

APPLYING RISK ASSESSMENT KNOWLEDGE

Now that we know how a risk assessment should work, let's look at a few real-world examples to understand how one institution might assess a few common risks and controls. We'll address Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets and Control (BSA/AML/OFAC), protecting sensitive customer data, compliance and cyber risks.

In conducting this exercise, we'll use a 5-point scale using the terms catastrophic, significant, moderate, minor and insignificant to measure risk and its potential impact. Control effectiveness will be measured on a three-point scale for impact (very important, important and not important). Probability and effectiveness will be measured on a five-point scale with the terms certain, likely, possible, unlikely and remote.

BSA/AML/OFAC

Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets and Control (BSA/AML/OFAC) are critically important to any financial institution. The FFIEC recommends financial institutions conduct a BSA/AML risk assessment every 12 to 18 months or when new products or services are introduced, existing products and services change, or higher-risk customers open or close an account. The steps are the same as with every other kind of risk:

1. **Identify BSA/AML/OFAC risks with relevant risk controls**
2. **Assign impact and probability to each BSA/AML/OFAC risk to understand each risk's potential effect on the organization**
3. **Assign and prioritize controls for each BSA/AML/OFAC risk to manage risk mitigation**
4. **Define residual risk for BSA/AML/OFAC, for a deeper dive into the total risk and a more consistent risk assessment**

When assessing BSA/AML/OFAC, identify potential risk categories by looking at the institution's products, services, customers, transactions, and geographic locations as well as the regulations that must be followed. There's no shortage of areas to asses, including funds transfers, foreign correspondent accounts, and Know Your Customer.

In this case, let's look at the risk of failing to file suspicious activity reports (SARs).

Risk: Failing to file timely SARs.

Event Impact: Catastrophic. Failing to file suspicious activities reports and other BSA violations are a common source of enforcement actions. Falling short can have tremendous regulatory repercussions.

Probability: Possible. Just because you tell staff to do something, that doesn't mean they'll do it. Without a structure in place to ensure that reports are filed in a timely fashion, it's entirely possible something will fall through the cracks.

Inherent risk. Catastrophic. While the probability is only moderate, the potential consequences are so dire that the risk remains very high.

Fortunately, there are a variety of controls that can reduce the risk of a financial institution failing to properly file SARs.

- **Policies and procedures**
- **Training**
- **Regular audits**

Let's look at policies and procedures.

Control: Policies and procedures

Impact: Important. Well-drafted policies and procedures spell out the specific steps that should be taken and assign roles and responsibilities. They provide an important roadmap to ensure that every report is properly filed.

Effectiveness: Moderate. There is always a chance that someone doesn't follow the policies and procedures. Assessments have shown occasional lapses.

Residual risk: Minor. This strong control will go a long way towards reducing risk.

When combined with other controls, including training and regular audits, the residual risk can fall even further. It depends on the institution.

[1] Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase. BSA/AML Risk Assessment-Overview. https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_005.htm Accessed 11/16/2017.

PROTECTING CUSTOMER DATA

Protecting customer's sensitive data is more than just a sacred duty. It's a regulatory requirement. A Gramm-Leach-Bliley Act risk assessment should identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information and assets.

Unauthorized access comes in many forms. In this case, let's consider the risk that an employee will successfully access or misuse data.

Risk: Employee unauthorized access or misuse or sensitive consumer information.

Event Impact: Catastrophic. It's a violation of federal law and could result in reputational damage to the institution.

Probability: Possible. With no controls it's easy enough to access data, but the average employee isn't likely to try to steal data.

Inherent Risk Rating: Moderate-High (4). While there is a lot of opportunity to steal data, the vast majority of employees aren't looking to commit a crime.

Now let's look at the controls the institution has in place to mitigate this risk. There are a variety of controls designed to limit unnecessary access to data and protect data. They include:

- **Access restrictions based on job responsibilities.**
- **Requiring individual identification and authentication for desktop log-on.**
- **Formal policies that define password parameters & rules (no Post-its with passwords on monitors).**
- **Requirements for periodic review of access rights.**
- **Termination protocols and checklists.**
- **Secure disposal measures to properly dispose of consumer information when no longer needed.**
- **Requirement for acknowledgement and acceptance of confidentiality/non-disclosure agreements before permitting access to confidential data or systems.**

Each of these controls should be individually reviewed and risk assessed. Then an aggregate residual risk score should be calculated. To better understand how this works, let's assess the first control by impact and probability.

Control: Access restrictions based on job responsibilities.

Impact: Important. The fewer people who have access to data, the safer the data is, and this control limits who has access. However, there will still be many people with access to the data and logging into someone else's account to access data remains a possibility.

Effectiveness: Moderate. It's very hard to log in without access, assessments have shown.

Residual risk: Minor. With the controls in place, it's less likely that employees will be able to misuse data since sensitive data since fewer people will have it. Additional controls are necessary to reduce risk further.

COMPLIANCE

Ask any financial institution about its top challenges and compliance is almost certain to make the list. From new regulations to managing existing rules to tracking exam and audit findings, managing compliance is an increasingly onerous and risky task.

Risk: Exam or audit finding fall through the cracks and aren't properly addressed in a timely fashion.

Event Impact: Catastrophic. Regulators will not be happy if identified problems aren't actively addressed. Failing to properly manage them can result in regulatory action.

Probability: Likely. With the increasing number of audits generating more and more findings, it's very possible that a finding could be lost in the shuffle.

As with most risks, there are a variety of controls that can reduce the risk exposure. They include:

- **Policies and procedures**
- **Automated tracking system**
- **Board reporting**

Let's assess an automated tracking system as a control.

Impact: Very important. An automated system ensures that every audit and exam finding is logged and tracked with someone assigned responsibility for follow through. It can provide reminders that actions are necessary and make it obvious which findings have been addressed and which are on their way.

Effectiveness: Likely. An automated system will very likely ensure that audit and exam findings are not forgotten. Human error remains a small factor, as sometimes people fail to properly use the system, but training can further increase the probability of proper usage.

Residual risk: Insignificant. An automated tracking system greatly reduces the risk of failing to correct the errors that auditors and examiners identify.

CYBER RISK

Cybersecurity is a top concern for every financial institution. From reputational harm to regulator wrath, the cost of a breach is high.

Risk: Hackers aim a cybersecurity attack at the institution's systems.

Event Impact: Catastrophic. The consequences of unauthorized access into the institution's systems are incredibly severe. Private customer data could be stolen or changed. Funds could be stolen. The institution could be locked out of its system. It could be a nightmare.

Probability: Certain. Cyber criminals are constantly looking for new victims and testing systems for vulnerabilities to exploit. It's a certainty that there are intruders trying to get into the network on a regular basis.

Inherent Risk Rating: Catastrophic. Not only is it likely that cyber criminals are trying to access the system, but if they got in it would cause tremendous damage.

Now let's look at the controls the institution has in place to mitigate these risks. After all, going offline isn't a viable option in the modern business world. There are a variety of network security protocols and controls designed to prevent and/or detect unauthorized access and cybersecurity incidents. They include:

- **Anti-virus software on desktops, servers, and host, with patches obtained from secure sites.**
- **Anti-malware software installed on critical servers and on end-point devices, with signatures updated nightly.**
- **Defense in-depth program, including intrusion detection/intrusion prevention systems.**
- **Semi-annual threat and vulnerability testing and attack and penetration tests.**
- **Centralized monitoring via security incident and event management (SIEM).**
- **Perimeter firewall systems.**

Let's assess the first control by impact and effectiveness.

Control: Anti-virus software on desktops, servers, and host, with patches obtained from secure sites.

Impact: Very important. Anti-virus software should be quite effective in protecting systems, but there is always the possibility that there's an attack from a new virus that hasn't been discovered yet. Also, every machine must be patched for this to be effective. One machine could leave the whole network exposed.

> It's not about being alarmist or giving friends a passing grade. It's about shaking off biases and looking at each control with a practical eye.

Effectiveness: Possible. New viruses are being developed all the time and there are many states actively working to access systems, yet assessments how shown this control to regularly work.

Residual risk: Significant. Even though there are a great many of well-thought out controls to limit the possibility of a cyberattack, risk still remains due to the evolving nature of cybersecurity threats.

This score is not an indictment of the IT department. IT should be praised for everything it does to protect the institution. Without its efforts, it's almost guaranteed that the institution would have been hacked by now. Instead, the risk assessment lets the board and management know that it needs to continue to invest heavily in cybersecurity. If the assessment indicated low cyber risk, the board and management might feel free to reallocate resources to another area of the institution, and in a world of rapidly advancing cyber threats, that's a mistake.

This exercise should be repeated for other areas of cyber risk, including the vendor management program. Take the time to not just identify potential risks, but also controls such as:

- **A centralized vendor risk management program designed to address the adequacy of information security practices of third parties.**
- **Due diligence requirements prior to third-party engagement.**
- **Enhanced due diligence for moderate-high, high, and critical vendors.**
- **Defined data protection standards for third-party vendors with authorized access to data.**

Be realistic in how effective these controls will be in the real-world environment and how likely they are to work. Acknowledge that when it comes to cyber risk, there are few guarantees. Look at each control individually and make a gut call. It's not about being alarmist or giving friends a passing grade. It's about shaking off biases and looking at each control with a practical eye.

The takeaways from the sample assessments are clear. Inherent risk is often high. Some controls are more effective than others. Residual risk can often be lowered through a combination of controls.

CONCLUSION

The goal of a risk assessment is not to eliminate risk. It's to align an institution's risk exposure and management with its risk tolerance and goals. The information gleaned from a well-executed risk assessment gives management and the board valuable insights that help it make better decisions that contribute to the safety and soundness of the institution while allowing it to make the most of potential opportunities.

Risk is a continuum. Therefore, there are no right or wrong risk or control scores. Scores are simply information, just like a customer's credit score. If an institution decides that an activity poses too much risk or that its controls are insufficient for managing those risks, then it can decide to discontinue the activity or consider new controls just like it would decide whether or not to extend a loan based on a credit score. No institution wants its rating agency to adjust credit scores just to make a loan a slam dunk. It wants to know the truth so it can make an accurate credit decision.

The key to creating reliable risk assessments is consistency and awareness of potential biases. Management will be able to better utilize the information from risk assessments if the scoring process for the compliance and information technology risk assessment are consistent. Every institution has different objectives, risk tolerances and circumstances. Risk assessors should be encouraged to consider these unique attributes while also looking outside the institution to recognize risks and opportunities that are likely to impact similar organizations. Risk assessment must be an ongoing process, one where assessors are empowered with a broad base of knowledge and encouraged to think critically. When everyone is on the same page and aware of the same potential hang ups, risk assessments are far more likely to accurately represent risk and contribute to business success.

About Ncontracts

Ncontracts® is a leading provider of risk management software and services to financial institutions. While we started with our industry-leading vendor management platform, our portfolio offerings have evolved to feature enterprise risk management, business continuity risk management, findings management, and cybersecurity management. More than 800 financial institutions use Ncontracts to manage risk more efficiently and effectively using our integrated suite of software and services.