PUSH Methodology Worksheet 2.2

Introduction

The purpose of this working document is to act as a guide for performing a risk assessment using the PUSH methodology first presented as *A Practical and Effective Approach to Risk Assessment* at the FFIEC Information Technology Conference in 2007 and 2008 by Mark T. Chapman, CFE CISM CISSP CRISC. (www.ctgi.net, www.phishline.com)

The PUSH approach is named after its four key steps:

- **P**reparation
- **U**niverse Definition
- **S**coring
- **H**itting the Mark

Given the complexity of any reasonable risk assessment process today, it is highly recommended to leverage some automated tool to act as a repository and risk calculator. *Regardless of the specific tool, the most important part of a risk assessment is the **process**.* You process will provide you the information to defend your risk assessment to others (i.e. examiners, auditors).

This document is not a replacement for proper training in risk assessment methods. It is simply a guide that can be used to document a repeatable process. It is not intended to be as formal as auditor "work papers" or as informal as simply plugging numbers into a computer.

Please note that most users of the PUSH method leverage the RiskOptix® Software-as-a-Service platform to provide one place to capture, store, reference, analyze and report information related to managing risks. RiskOptix® has been used in over 100 risk related assessments for financial institutions nationwide and is available from the Wisconsin Bankers Association/FIPCO. There are many good automated tools and formal methodologies in the marketplace. Again, the most important part of the risk assessment is to follow and document an understandable process.

The pages that follow consist of a set of general Methodology steps. Each step is identified by one of four icons that are used to emphasize the nature of the expected results. Those icons are illustrated in the table that follows:

Legend:	
	"Normal" step in the process. Simply review the *Methodology Step* description column and make notes in *Project Specific Details while performing the steps.*
	"Target" step used to identify sources of potential problem areas. These may or may not ultimately be identified as formal risk assessment "observations" or "findings".
	"Future Consideration" step used to identify trends or to make notes of future focus areas. Risk assessment is on on-going process. Take good notes of anything that will make the next assessment round be even more effective.
	"Strength" step used to identify exceptional areas of risk management. These non-indulgent steps can help provide insights into the overall risk profile which is not just about the vulnerabilities.

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Preparation		
	Methodology Steps	***Project-Specific Details***
	Define Purpose, Scope, Goals: • Which business areas will be covered? • What context applies? • Is this a risk assessment, audit or review?	*The purpose of the project is to perform a _____ Risk Assessment to address the administrative, technical, and physical safeguards for a bank of this size and complexity.* *The scope of the risk assessment process needs to ensure that all reasonable foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information.* *The goal is to quantitatively assess the probability or impact of inherent risk while also calculating residual risk based on the effectiveness of the perceived design and execution of controls.*
	Identify the Specific Purpose: • Audit Planning • Budgeting • Compliance • Disaster Recovery • Policy Writing • Risk Management • Remediation • Vendor Selection	*During the preparation phase we identified the approach and the purpose of the risk assessment. The specific purpose for the assessment was to:* 1. *Provide assistance in determining which future projects to perform so as to ensure that areas of highest risk are given a higher prioritization over projects than those with a lower level of risk.* 2. *Establish a sustainable risk assessment methodology that allows the bank to continuously monitor the level of risk.* 3. *Increase compliance with federal regulations related to the safeguarding of customer information.*
	Anticipate the Benefits: • To learn something new • To validate or quantify a concern • To standardize communication of risk • To establish common language and tools • To satisfy regulatory requirements	*The anticipated benefits for this engagement:* • *To establish common language and tools* • *To establish a way to link Risk Assessment to project prioritization.* • *To standardize communication of risk.* • *To improve on existing risk assessment process.*
	Decide to In-source or Outsource: • Confirm that you have the capability in-house. • Engage an external firm with independent,	*We decided that the combined efforts of internal and external resources would make the most sense.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Preparation		
	Methodology Steps	***Project-Specific Details***
	knowledgeable and sufficient resources.	
	Evaluate Automation Options: • Paper • Excel / Word • Specialized Software	*The RiskOptix® software will be used for the risk assessment.*
	Identify Source Documents: • Strategic Plans – is the business changing? • List of Related Projects (Recent and Planned). • Prior Audits/Examinations. • New guidance about threats.	*Here is the list of the most significant source documents for the risk assessment.* • *X* • *Y* • *Z* •
	Earn Management Buy-In: • Identify Motivators • Assign Project Sponsor • Approve Resources	*There is full management buy-in that this is an important strategic and tactical step. Not simply because of compliance, but to help focus and improve the information security posture of the institution.* *Project Sponsor: _____* *Resources Approved: Internal resources, external consultants and an automated tool.*
	Preparation Stage Review: • Are all steps addressed? • Are there any areas that are excluded?	*The preparation stage was completed with no questions about the proper completion of each step.*
	Preparation Stage Potential Observations/Findings: • Are there any potential areas of concern? • The purpose is to make notes. A big concern at this stage may not be an issue in the context of the completed risk assessment. Nonetheless, it is important to document suspected areas of improvement.	*The scope is much more involved than what was performed in the past.* *There is a concern about finding a balance that matches the size and complexity of the institution.*

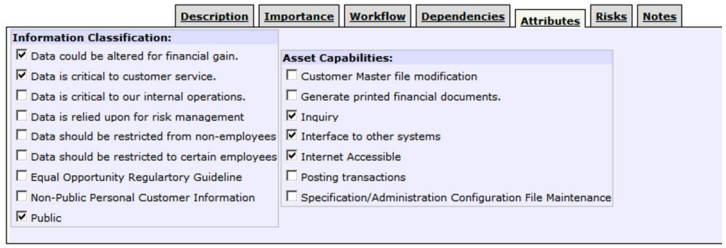
4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

PUSH Methodology Worksheet 2.2

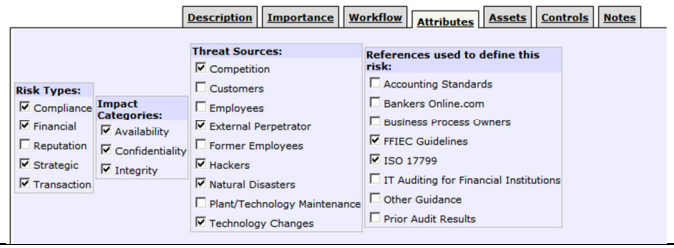
Preparation		
	Methodology Steps	***Project-Specific Details***
	Preparation Stage Potential Areas of Excellence: • Are there noteworthy areas of excellence?	*None identified in the Preparation Stage.*
	Preparation Stage Future Considerations: • Lessons learned? • Future considerations?	*We anticipate that risk assessment will evolve as a continuous improvement process. The only way to get the most out of the risk assessment is to get better at it every time, with more focused scopes, and the ability to include changes.* *For example, adoption of this approach will lead us to always consider future projects and business initiatives.*

Universe Definition		
	Methodology Steps	***Project-Specific Details***
	Define the approach. • "Assets", "Risks" and "Controls" • Granularity • Level of Detail	*The approach will be to assess the Assets, Risks and Controls.* *The level of granularity shows a significant improvement.* *The level of detail shows a significance improvement.*
Asset Universe Definition		
	Asset Universe Granularity. • How many levels of assets do we want to consider? • Where will the asset list come from? • What process will be used to determine the level that is appropriate for the size and complexity of the institution?	1. *We started with the list of Assets from _____.* 2. *We combined the list with the RiskOptix® library.* 3. *All duplicates or irrelevant assets were exported and saved for future reference.* 4. *We reviewed the source documents to ensure appropriate coverage.* 5. *The process carefully considered the appropriateness for the size and complexity of the institution while considering the Scope and Specific Purpose of this particular assessment.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Universe Definition		
	Methodology Steps	***Project-Specific Details***
	Asset Universe Level of Detail. How much information do we want to understand for each asset? This is known as "characterizing" assets. Here is a conceptual example of a simple approach to characterization. Select a set of attributes that are appropriate for the size and complexity of the institution while supporting the risk assessment project scope and specific purpose.  Description | Importance | Workflow | Dependencies | Attributes | Risks | Notes **Information Classification:** ☑ Data could be altered for financial gain. ☑ Data is critical to customer service. ☐ Data is critical to our internal operations. ☐ Data is relied upon for risk management ☐ Data should be restricted from non-employees ☐ Data should be restricted to certain employees ☐ Equal Opportunity Regulartory Guideline ☐ Non-Public Personal Customer Information ☑ Public **Asset Capabilities:** ☐ Customer Master file modification ☐ Generate printed financial documents. ☑ Inquiry ☑ Interface to other systems ☑ Internet Accessible ☐ Posting transactions ☐ Specification/Administration Configuration File Maintenance	1. *We started with the attributes already identified in _____* 2. *We combined the list with the standard attributes from RiskOptix®.* 3. *We disabled any attributes that did not apply to the scope of the project.* 4. *We added additional attributes as appropriate into the database which allows us to filter and sort based on the asset characterization.*
	Do the Asset Universe Granularity and Level of Detail support the Specific Purpose?	*Yes, we believe the number and types of assets and the level of details support the specific purpose of this risk assessment.*
	Are there any potential observations/findings from the process of identifying the asset universe?	*There were several assets that needed to be added to this list. For example, we added _____ to ensure coverage of that important focus area.*
	Identify Future Areas related to Asset Universe.	*In the future, to gain the benefits from continuous improvement the _____areas will likely be expanded to show a higher level of granularity.*
	Are there any areas of particular strength that should be noted for the Asset Universe?	*There was a good understanding of the in-scope assets within the risk assessment.*

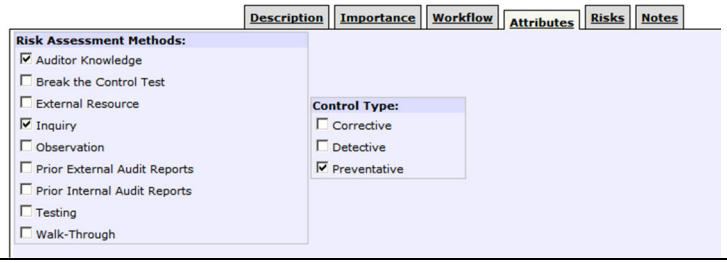
4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Universe Definition		
	Methodology Steps	***Project-Specific Details***
Risk Universe Definition		
	Risk Universe Granularity. • How many levels of risks do we want to consider? • Where will the risk list come from? • What process will be used to determine the level that is appropriate for the size and complexity of the institution?	1. *We started with the list of Risks from _____.* 2. *We combined the list with the RiskOptix® library.* 3. *All duplicates or irrelevant risks were exported and saved for future reference.* 4. *We reviewed the source documents to ensure appropriate coverage.* 5. *The process carefully considered the appropriateness for the size and complexity of the institution while considering the Scope and Specific Purpose of this particular assessment.*
	Risk Universe Level of Detail. How much information do we want to understand for each risk? This is known as "characterizing" risks. Here is a conceptual example of a simple approach to characterization. Select a set of attributes that are appropriate for the size and complexity of the institution while supporting the risk assessment project scope and specific purpose.  	1. *We started with the attributes already identified in _____.* 2. *We combined the list with the standard attributes from RiskOptix®.* 3. *We disabled any attributes that did not apply to the scope of the project.* 4. *We added additional attributes as appropriate into the database which allows us to filter and sort based on the risk characterization.*
	Do the Risk Universe Granularity and Level of Detail support the Specific Purpose?	*Yes, we believe the number and types of risks and the level of details support the specific purpose of this risk assessment.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Universe Definition		
	Methodology Steps	***Project-Specific Details***
	Are there any potential observations/findings from the process of identifying the risk universe?	*We needed to add additional risks to address concepts not covered by the former risk universe. This process happened while examining the related assets and controls. We need to keep this in mind so the risk assessment process is not viewed as linear next time.*
	Identify Future Areas for Risk Universe.	*It will be an ongoing challenge to identify all the different types of potential threats/risks.* *The risk universe definition process included several rounds of merging risks that had similar profiles. Given the relationships between assets and risks, this process helped focus our efforts.* *While this is not a problem, we need to make sure future assessments do not gloss over the importance of identifying specific risk areas. The example we used this time was to make sure we understood any specific risks related to _____.* *In the future, we need to carefully address changes in the asset, risk and control universe (through change management and projects) as well as changes to the threat profile that directly impact the risk universe.*
	Are there any areas of particular strength that should be noted for the Risk Universe?	*There was a good understanding of the in-scope risks within the risk assessment.*
Control Universe Definition		
	Control Universe Granularity. • How many levels of controls do we want to consider? • Where will the controls list come from?	1. *We started with the list of Controls from _____.* 2. *We combined the list with the RiskOptix® library.* 3. *All duplicates or irrelevant controls were exported and saved for future reference.* 4. *We reviewed the source documents to ensure appropriate*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Universe Definition		
	Methodology Steps	***Project-Specific Details***
	What process will be used to determine the level that is appropriate for the size and complexity of the institution?	*coverage.* *The process carefully considered the appropriateness for the size and complexity of the institution while considering the Scope and Specific Purpose of this particular assessment.*
	Control Universe Level of Detail. How much information do we want to understand for each control? This is known as "characterizing" controls. Here is a conceptual example of a simple approach to characterization. Select a set of attributes that are appropriate for the size and complexity of the institution while supporting the risk assessment project scope and specific purpose. 	1. *We started with the attributes already identified in _____.* 2. *We combined the list with the standard attributes from RiskOptix®.* 3. *We disabled any attributes that did not apply to the scope of the project.* *We added additional attributes as appropriate into the database which allows us to filter and sort based on the control characterization.* *The most important was the concept _____ (for example, considering "Automated" controls.)*
	Do the Control Universe Granularity and Level of Detail support the Specific Purpose?	*Yes, we believe the number and types of controls and the level of details support the specific purpose of this risk assessment.*
	Are there any potential observations/findings from the process of identifying the control universe? • Are there any controls that are known to be insufficient or non-existent in the environment? • Use the source documents to see history. • Use the library of controls and other guidance to	*We needed to add additional controls to address concepts not covered by the former control universe. This process happened while examining the related assets and risks. We need to keep this in mind so the risk assessment process is not viewed as linear next time.* *There were several control areas that were identified as missing or*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Universe Definition		
	Methodology Steps	***Project-Specific Details***
	see what is missing.	*deficient. Including, _____.*
	Identify Future Areas for Control Universe.	*In the future, we need to carefully address changes in the asset, risk and control universe (through change management and projects) as well as changes to the threat profile and improvements in control standard-practices that directly impact the control universe.*
	Are there any areas of particular strength that should be noted for the Control Universe?	*There was a good understanding of the in-scope controls within the risk assessment including any missing controls.* *We discussed some areas of obvious strength. For example, _____ is a very strong control for an institution of this size and complexity.*

Scoring		
	Methodology Steps	***Project-Specific Details***
	Choose Input Scale: It is important to define a consistent scale for: • **Asset Importance** – How important is the asset relative to other assets? Do not hesitate to document assets that are of low importance, they will be addressed appropriately in the prioritize & trim step below. • **Risk Impact** – What is the potential impact of the raw, unmitigated, inherent risk? • **Risk Likelihood** – What is the potential likelihood of the raw, unmitigated, inherent risk?	*We choose to use a consistent scale from 1 to 5, with 5 being* to the "largest extent". Examples: • Asset Importance of 1 – lowest importance asset classification. • Risk Impact of 5 – highest inherent risk. • Control Execution of 2 – control may exist, but there are known deficiencies. Where appropriate, the 1-5 may consider financial, strategic, reputation and other scales. The first pass simply used 1, 3, and 5 for low, medium, and high. The scores of 2 and 4 were used to make finer distinctions.

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring		
	Methodology Steps	***Project-Specific Details***

	• **Control Design** (formerly "Control Impact") – How effective is the design of the control against most associated risks?
	  ○ For example, even the most effective "Acceptable Use Policy" would still only have limited effectiveness against the risk of Employee Fraud.
	  ○ Another example is Anti-Virus software. By design, it is thought to be quite effective at reducing the risk of malicious code.
	
	• **Control Execution** (formerly "Control Likelihood") – How effective is the execution or implementation of the control at this particular institution?
	  ○ For example, is there an "Acceptable Use Policy?" Is it reviewed on a regular basis? Is it enforced?
	  ○ Another example is if all desktop machines have Anti-Virus software installed? Do you have centralized management capabilities to prove it?
		The calculations can be used to identify or confirm observations/findings. The most important steps were the process used to identify the scores with appropriate notes added to the risk assessment database.

	Choose Output Scale: RiskOptix automatically computes the following values: • **Mitigation %** - A summary of the strength of controls with respect to applied asset-risk pairs. Here is a simple example: ○ Asset "A" has only one risk associated with it. The risk has an Impact of 5 and a Likelihood of 5. The asset-risk pair has	*We reviewed the results of the calculations in the tool.* *The Mitigation % provides a deeper level of insights than a simple scale of 1-5 while considering the relative number and strength of applied controls.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring		
	Methodology Steps	***Project-Specific Details***
	only one control which has a Design of 4 and an Execution of 4. In this example, the Mitigation % would be AVG(4/5, 4/5) which is 4/5 or 80%. • **Residual %** - A summary of the unmitigated risk due to the strength of controls with respect to the applied asset-risk pairs. It is the inverse of the Mitigation %, or 100% - Mitigation %. In the above example, it would be 100%-80% leaving 20% Residual Risk. Note: 99% is the highest allowed Mitigation%, since nothing is ever 100% mitigated even if every applied control is a Design and Execution of 5.	
	Choose Reporting Scale: The system provides the ability to map Mitigation % to Mitigation Level. This is done using institution and assessment-specific cutoffs based on the asset importance.	*During this assessment, the system showed significant Asset residutal risk exposure by sorting by Mitigation Level.* *From an inherent risk perspective, the system showed* _____.

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring

	Methodology Steps	*Project-Specific Details*
		
Asset Universe Scoring		
	Asset Importance Scoring and Normalizing: ▪ First-pass: Score each item independently. ▪ Second-pass: Normalize the scores by reviewing all universe items with respect to each other. This is meant to be a sanity-check to confirm consistent and reasonable scoring. This is usually easier if one team scored all items. Otherwise, the normalization step will identify risk assessment teams who were inconsistent with the scoring things higher or lower than other areas.	*We carefully scored the Asset Importance on a scale of 1-5 while considering the Asset Characterization and other factors.* *It was one team performing the scoring with individual, sub-group and full-group reviews.* *The normalized result was a reasonable and appropriate mix of low, medium and high importance scores.*
	Asset Universe: Prioritize and Trim. Remove or make note of Low-Importance Assets that can be ignored in the scope of the rest of the risk assessment process.	*We reviewed the low importance assets. In particular, the lowest importance asset was the _____* *We do not have a _____, so no further risk assessment steps will be performed. That said, it is important to keep this asset in the universe since it may be something that is implemented in the future.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring		
	Methodology Steps	***Project-Specific Details***
	Asset Universe Scoring: Are there any potential observations/findings from the process of identifying assets? • Sort by Importance. • Filter by Attributes. For example, do a query for all assets that process, transmit or store non-public personal customer information. • This step is exploratory in nature. Spend some time and look for trends.	*Several potential high importance assets were identified.* _____ *These were noted after association was performed to see the final applied control deficiencies.*
	Asset Universe Scoring: Identify Future Areas	*Refinement of the Mitigation Level Thresholds is a good item to consider for future refinement.*
	Asset Universe Scoring: Exceptional Areas.	*Nothing noted.*
Risk Universe Scoring		
	Risk Impact and Likelihood Scoring and Normalizing: ▪ First-pass: Score each item independently. ▪ Second-pass: Normalize the scores by reviewing all universe items with respect to each other. This is meant to be a sanity-check to confirm consistent and reasonable scoring. This is usually easier if one team scored all items. Otherwise, the normalization step will identify risk assessment teams who were inconsistent with the scoring things higher or lower than other areas.	*We carefully scored the inherent Risk Impact and Risk Likelihood on a scale of 1-5 while considering the Risk Characterization and other factors.* *It was one team performing the scoring with individual, sub-group and full-group reviews.* *The normalized result was a reasonable and appropriate mix of scores.*
	Risk Universe: Prioritize and Trim. Remove or make note of low-impact or low-likelihood risks that can be ignored in the scope of the rest of the risk	*We reviewed the risks areas with low inherent risk.* *Generally, this was used as a trimming step to identify out-of-scope risk areas. These were archived from the system to keep the risk universe clean*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring		
	Methodology Steps	***Project-Specific Details***
	assessment process.	*and relevant to our institution.*
	Risk Universe Scoring: Are there any potential observations/findings from the process of identifying assets? • Sort by Impact and Likelihood. • Filter by Attributes. For example, do a query for all risks related to "Technology Changes" as a basis for a project-specific risk assessment. • This step is exploratory in nature. Spend some time and look for trends.	*Several potential high risk areas were identified.* _____ *These were noted after association was performed to see the final applied control deficiencies.*
	Risk Universe Scoring: Identify Future Areas	*It is helpful to know how to query the database for future risk assessments. For example, if we are considering adoption of new technology, the risk universe can help us identify potential risk areas.*
	Risk Universe Scoring: Exceptional Areas.	*Nothing noted.*
Control Universe Scoring		
	Control Design and Execution Scoring and Normalizing: ▪ First-pass: Score each item independently. ▪ Second-pass: Normalize the scores by reviewing all universe items with respect to each other. This is meant to be a sanity-check to confirm consistent and reasonable scoring. This is usually easier if one team scored all items. Otherwise, the normalization step will identify risk assessment teams who were inconsistent with the scoring	*We carefully scored the Control Design and Control Execution on a scale of 1-5 while considering the Control Characterization Attributes and other factors.* *The Source documents were critical in this process.* *It was one team performing the scoring with individual, sub-group and full-group reviews.* *The normalized result was a reasonable and appropriate mix of scores.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring		
	Methodology Steps	***Project-Specific Details***
	things higher or lower than other areas.	
	Control Universe: Prioritize and Trim. Usually there is nothing to do here from a scoring perspective. From a normalization perspective, you may choose to remove redundant control items from the universe.	*We reviewed the control areas trying to identify redundant items.* *These were archived from the system to keep the control universe clean and relevant to our institution.*
	Control Universe Scoring: Are there any potential observations/findings from the process of identifying assets? • Sort by Execution. This is a typical way to identify control deficiencies. • Filter by Attributes. • This step is exploratory in nature. Spend some time and look for trends.	*Several potential control deficiencies were identified.* _____ *These were noted until after association was performed to see the final applied control deficiencies.*
	Control Universe Scoring: Identify Future Areas	*It is helpful to know how to query the database for future risk assessments. For example, we considered future plans for control implementation and found that there was a scheduled project related to _____ that may not provide the best return on investment.*
	Control Universe Scoring: Exceptional Areas.	*We discussed some areas of obvious strength. For example, the _____is a very strong control for an institution of this size and complexity.*
Association – Assets to Risks		
	Asset-Risk Association: • For each Asset, assign the most relevant risk areas. The idea is to cover the risk universe, not to overstate the obvious. (For example, you could	1. *We started with the associations already identified in _____.* 2. *We combined the list with the standard associations from RiskOptix®.* 3. *We stepped through the Asset-Risk and the Risk-Asset steps to*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring		
	Methodology Steps	***Project-Specific Details***
	relate the risk of "Natural Disaster" with every Asset. A more common-sense approach is to relate it to the physical assets, such as data centers and people with an implied or documented dependency to other assets such as individual servers or applications. • For each Risk, assign the most relevant Assets. This is a cross-check to make sure that Asset-Risk association covers the asset universe.	*provide reasonable coverage of the most relevant relationships as covered on the Audit | Assessment Asset-Risk-Detailed Assessment.*
	Asset-Risk Inherent Risk Detail Review: • For each asset, examine the Risk Impact and Risk Likelihood scores. While most follow the defaults, look for anomalies.	*Under Audit Manager | Assessment | Asset-Risk Detail Assessment, we reviewed the Risk Impact and Likelihoods to see if there was anything that didn't make sense.* *Several adjustments were made.*
	Asset-Risk Association: Are the potential observations/findings related to Asset-Risk Association? • Are there Assets with insufficient risks? • Are there Risks that have not been applied appropriately to Assets?	*We spent significant time as individuals, sub-groups and as a group reviewing the associations. We feel they are appropriate for the size and complexity of the institution.*
	Asset-Risk Association: Identify Future Areas	*There is always room for more refinement. Our approach was to maintain a manageable set of relationships that can be expanded in the future.*
	Asset-Risk Association Scoring: Exceptional Areas.	*Nothing noted.*
Association – Risks to Controls		
	Risk-Control Association: • For each Risk, assign the most relevant Control areas. The idea is to cover the risk universe, not to	1. *We started with the associations already identified in _____.* 2. *We combined the list with the standard associations from*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring		
	Methodology Steps	***Project-Specific Details***
	overstate the obvious. • For each Control, assign the most relevant Risks. This is a cross-check to make sure that Risk-Control association provides appropriate coverage.	*RiskOptix®.* *3. We stepped through the Risk-Control and the Control-Risk steps to provide reasonable coverage of the most relevant relationships. Ultimately, this is covered on the Audit | Assessment Asset-Risk-Control Detailed Assessment.*
	Risk-Control Unapplied Residual Risk Detail Review: • For each Risk and Controls, review the Impact, Likelihood, Design and Execution.	*Several adjustments were made.*
	Risk-Control Association: Are the potential observations/findings related to Risk-Control Association? • Are there Risks with insufficient Controls? • Are there Controls that have not been applied appropriately to Risks?	*We spent some time as individuals and sub-groups reviewing the associations.* *We feel they are appropriate for the size and complexity of the institution.*
	Risk-Control Association: Identify Future Areas	*There is always room for more refinement. Our approach was to maintain a manageable set of relationships that can be expanded in the future.*
	Risk-Control Association Scoring: Exceptional Areas.	*Nothing noted.*
Association – Assets, Risks and Controls (ARC)		
	ARC Review: Review the Asset-Risk-Control (ARC) in the project scope to identify: 1. Risks which have a different Impact/Likelihood against particular assets. 2. Controls which have a different Design/Execution against particular Risks or particular Asset-Risk pairs.	*We individually stepped through the ARC summary steps to provide reasonable coverage of the most relevant relationships.* *The Audit | Assessment Asset-Risk-Control Detailed Assessment was reviewed with an emphasis on the more important assets and the most likely areas of control deficiencies.* *Several adjustments were made.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Scoring		
	Methodology Steps	***Project-Specific Details***
	3. Controls which are Not Applicable (N/A) to a particular Asset-Risk Pair.	
	ARC: Are the potential observations/findings? • Are there Asset-Risk Pairs with insufficient Controls? • Are there Assets with unacceptable mitigation levels? • This is an exploratory step.	*Yes, there were several control deficiencies identified by sorting the ARC Details by Control Execution. This gave us a detailed picture as to the nature of the control deficiencies.* *Further sorts reinforced that the plans for future projects, in particular, the _____, may not have a significant impact on the risk posture of the institution.*
	ARC: Identify Future Areas	*There is always room for more refinement.* *For this risk assessment, there were sufficient control deficiencies identified to provide significant areas of improvement. Future risk assessments may spend more time examining control efficiency. In any case, it is imperative to "use your brain" to look for practical responses. The tool can answer questions about the scoring, but if you simply sort and dump the output you may end up implementing controls that are too specific.*
	ARC: Exceptional Areas.	*Nothing noted.*

Hitting the Mark		
	Methodology Steps	***Project-Specific Details***
	Evaluate Intended Specific Purpose.	*We performed a Risk Assessment to address the administrative, technical, and physical safeguards for a bank of this size and complexity.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Hitting the Mark		
	Methodology Steps	***Project-Specific Details***
	Did the risk assessment process fulfill the Purpose, Scope and Goals?	*We ensured that all reasonable foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information.* *We quantitatively assess the probability or impact of inherent risk while also calculating residual risk based on the effectiveness of the perceived design and execution of controls.*
	Write the "Final Report".	*Done.* *There are three components.* *1. Executive Summary.* *2. Methodology Document (this document).* *3. Printed report from RiskOptix®.*
	Track Actions Over Time	*The live RiskOptix® database can be used to track changes to the risk profile over time. It can be used for multiple risk assessments with very different purposes.*
	Evaluate Project Effectiveness • Discoveries • Trends • *Actions* (proposed, planned or completed) • What did you learn through the process? • What unexpected benefits did you realize? • How did you keep the process from getting too detailed or out of control? • How can you improve the process next time? • These reports and charts look scientific and absolute - how did you handle the inherent subjectivity? • Did you achieve your objectives?	*We discovered the details in the observations.* *We learned a new, more comprehensive process for risk assessment that helps manage the complexities of risk assessment. It is difficult to go from theory to actionable information. We feel this approach was a significant improvement and recognize how we can continue to gain benefits in the future.* *We understand that this is a risk assessment, not an audit. The results could be used to identify areas that need the level of review of an audit.* *Yes, we achieved our objectives.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com

Hitting the Mark		
	Methodology Steps	***Project-Specific Details***
	Additional Considerations • Risk Tolerance • Trending • Monitoring • Monte Carlo Simulations • Surveys • Testing	*These are interesting future considerations. Some of the areas, such as Tolerance, Trending and Surveys may be used in the future.* *Others, such as Monte Carlo simulations, seem to be beyond what is appropriate for the size and complexity of the institution.*

4721 South Biltmore Lane | Madison, WI 53718
tel.800.722.3498 | fax.608.661.9382 | www.fipco.com