EXAMPLE

RISK ASSESSMENT

INFOSIGHT

www.InfoSightInc.com

FOR FINANCIAL INSTITUTIONS

Example Risk Assessment

Definition of Terms

The following section provides definitions to the variables used in the risk assessment:

- **Vendor Management Risk Categories** – The areas of Vendor Management risk within the Bank.
- **Inherent Risk** – The risk associated with the nature and complexity of each Vendor Management Risk Review Category.
- **Likelihood** – The chance of a risk materializing determined through both objective and subjective evaluation.
- **Impact** - One or more consequences (in tangible and intangible terms) that are foreseen if a risk is not mitigated.
- **Preliminary Risk –** The overall risk after consideration of inherent risk, likelihood of occurrence, and impact; without taking into consideration internal controls.
- **Residual Risk** – The remaining risk after the assessment of controls has been performed.

Risk Assessment Methodology

The methodology defines six different phases as described below:

- **Phase 1** – Determination of Vendor Management Risks and Vendor Management Review Risk Areas
- **Phase 2** – Determination and Measurement of Inherent Risk
- **Phase 3** – Determination and Measurement of Likelihood
- **Phase 4** – Determination and Measurement of Impact
- **Phase 5** – Determination and Measurement of Preliminary Risk
- **Phase 6** – Determination of Residual Risk

Each phase is described in detail in the following sections:

Phase I – Vendor Management Risk Categories

Vendor Management risks should be identified with stakeholders representing Vendor Management Risk functions. For the purposes of this take away example, the risks are those associated with the function outsourced, the service provider, and the technology used:

- Risks pertaining to the function outsourced include:
  - Sensitivity of data accessed, protected, or controlled by the service provider;
  - Volume of transactions; and
  - Criticality to the financial institution's business.
- Risks pertaining to the service provider include:
  - Strength of financial condition;
  - Turnover of management and employees;
  - Ability to maintain business continuity;
  - Ability to provide accurate, relevant, and timely Management Information Systems (MIS);
  - Experience with the function outsourced;
  - Reliance on subcontractors;
  - Location, particularly if cross-border (See Appendix C, Foreign-Based Third- Party Service Providers); and
  - Redundancy and reliability of communication lines.
- Risks pertaining to the technology used include:
  - Reliability;
  - Security; and
  - Scalability to accommodate growth.

Phase 2 – Determination and Measurement of Inherent Risk

Inherent risk is defined as the risk associated with the nature and complexity of each Vendor Management Risk Category. This example assumes that Inherent risk is measured on a scale of 1 through 3 as noted below:

1. Low (1)
2. Medium (2)
3. High (3)

Phase 3 – Determination and Measurement of Likelihood

Likelihood is the chance of a risk materializing through both objective and subjective evaluation. This examples uses a scale of 1 through 5 with the values defined below would be an appropriate method to measure likelihood.

- Rare (1) – conditions and events necessary for the risk to materialize are minimal to non-existent and have never occurred.
- Unlikely (2) – conditions and events necessary for the risk to materialize exist and a few risks have occurred.
- Moderate (3) – conditions and events necessary for the risk to materialize exist and some risks have occurred.
- Likely (4) – conditions and events necessary for the risk to materialize exist and several risks have occurred.
- Almost Certain (5) – conditions and events necessary for the risk to materialize exist and many risks have occurred.

"It was a calculated risk, and we forgot to carry the one."

Phase 4 – Determination and Measurement of Impact

Impact is reflected in one or more consequences (in tangible and intangible terms) that are foreseen if a risk is not mitigated. The consequences of a risk materializing can be classified as Operational, Reputational, Strategic, Compliance, and Interest/Liquidity/Price. The value assigned for impact is defined as the sum of one or more consequences for each Vendor Management Risk Category divided by five.

Impact = (O+R+S+C+I)/5

- Operational (1)
- Reputational (1)
- Strategic (1)
- Compliance (1)
- Interest/Liquidity/Price (1)

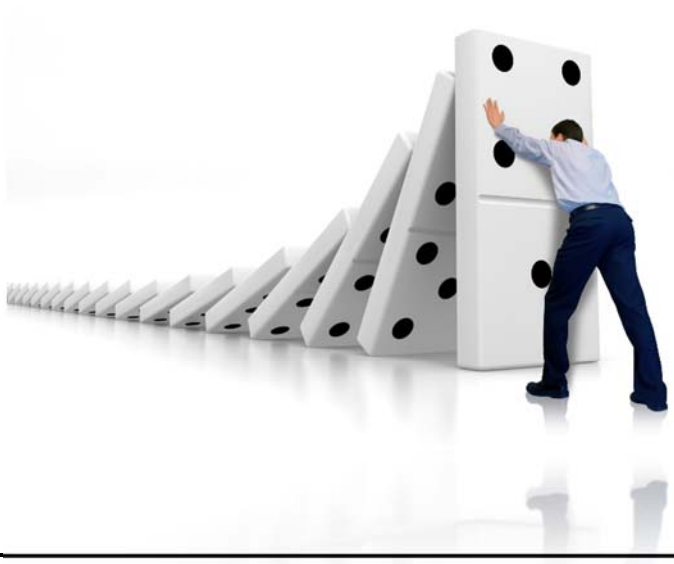
Phase 5 – Determination and Measurement of Preliminary Risk

Preliminary risk is the overall risk after consideration of Inherent risk, Likelihood of occurrence, and Impact without taking into consideration internal controls. The value assigned to Preliminary Risk is the sum of Inherent Risk plus the Likelihood value multiplied by the Overall Impact value not taking into consideration the effect of controls in place.

Preliminary Risk = IR + [Likelihood x (O+R+S+C+I/5)]

The following scale classifies Preliminary Risk as high, medium, and/or low:

- Low (1 - 2)
- Medium (3 - 5)
- High (6 - 8)



Risk Areas	Inherent Risk	Likelihood	Impact	Residual Risk	Risk Ranking		Operational	Reputational	Strategic	Compliance	Interest Rate/Liquidity/Price
Vendor Management Risk Categories							O	R	S	C	I
Sensitivity of data accessed, protected, or controlled by the service provider;											
Volume of transactions											
Criticality to the financial institution's business											
Strength of financial condition											
Turnover of management and employees;											
Ability to maintain business continuity											
Ability to provide accurate, relevant, and timely Management Information Systems (MIS);											
Turnover of management and employees;											
Systems Reliability											
Systems Security											
Systems Scalability											

Definitions:

IT Risk Categories - The areas of IT risk within the Bank

Inherent Risk - The risk associated with the nature and complexity of each IT Risk Review Category.

Likelihood – The chance of a risk materializing determined through both objective and subjective evaluation.

Impact - One or more consequences (in tangible and intangible terms) that are foreseen if a risk is not mitigated.

Preliminary Risk – The overall risk after consideration of inherent risk, likelihood of occurrence, and impact; without taking into consideration internal controls.

Residual Risk – The remaining risk after the assessment of controls has been performed.

Formulas:
Impact = (F+R+C+O+S)/5

Preliminary Risk = IR + [Likelihood x (F+R+C+O+S/5)]

Residual Risk = Preliminary Risk since the scope for 2014 changed

Inherent Risk Legend:

LOW = 1
MEDIUM = 2
HIGH = 3

Risk Ranking Legend:

LOW = (1-2)
MEDIUM = (3-6)
HIGH = (6-8)

Likelihood:

Rare = 1		Likely = 4
Unlikely = 2		Almost Certain = 5
Moderate = 3		