Risk Management: Appetite, Assessment & Beyond

Graham Cameron & Tuck Goh

Disclaimer

- All third party information featured in the presentation slides remain the intellectual property of their respective originators. All use of information is done under the fair use copyright principal, and we do not assert any claim of copyright for any quotation, statistic, fact, figure, data or any other content that has been sourced from the public domain. We do assert a claim of copyright for our compilations of presentation slides, their unique scope and style, HTML, database design, look and feel, and back-end code. Upon viewing any page under this presentation you consent to the disclaimer with regard to the accuracy of any materials or slides as presented.

Risk

What is “Risk”?

- uncertainty
- opportunity

Common definition:

Risk is that which could harm or prevent the achievement of objectives, the known and sometimes unknown factors that arise.

Risk Management

Definition:

Risk management is the process of identifying, assessing, and managing the risks that an organization faces.

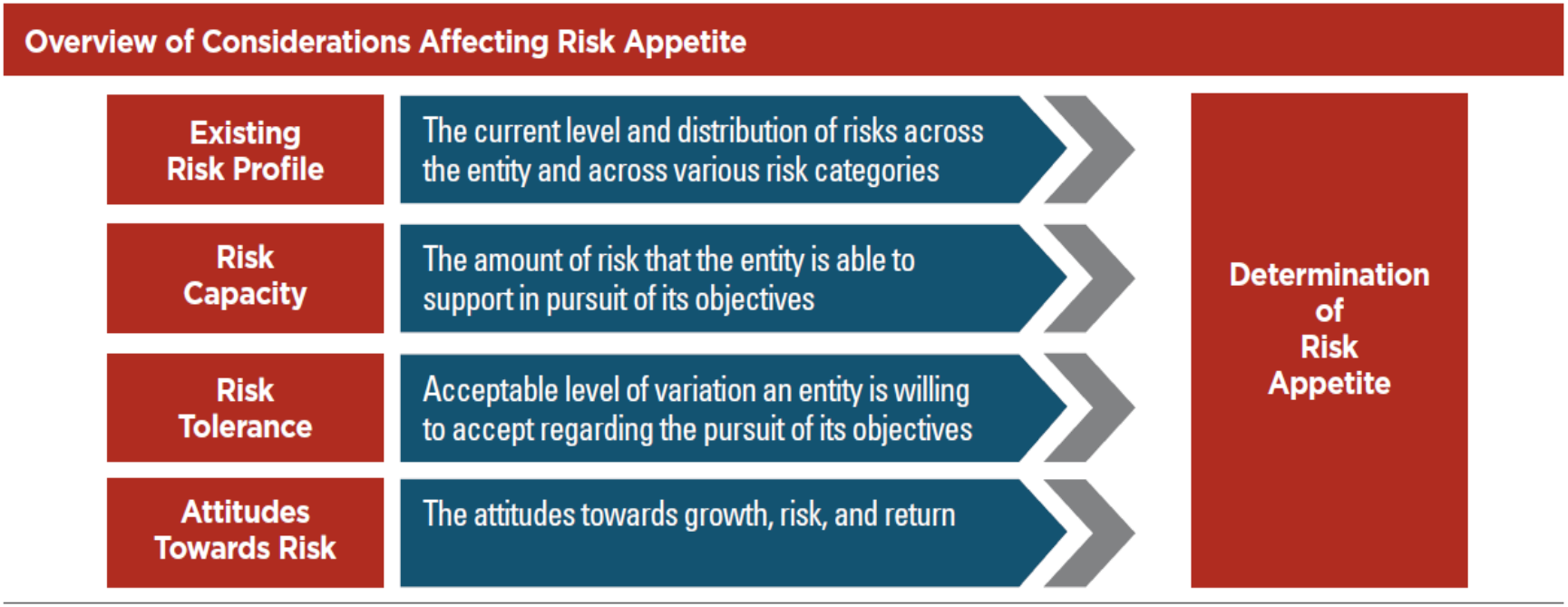
- As the outcomes of business activities are uncertain, they are said to have some element of risk. These risks include strategic failures, operational failures, financial failures, market disruptions, environmental disasters, and regulatory violations.
- While it is near impossible for companies to remove all risk they face, it is important that they properly understand and manage the risks that they are willing to accept in the context of executing the business strategy.

Risk Appetite

COSO's Enterprise Risk Management — Integrated Framework defines risk appetite as follows:

The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. … Risk appetite guides resource allocation. … Risk appetite [assists the organization] in aligning the organization, people, and processes in [designing the] infrastructure necessary to effectively respond to and monitor risks.

Defining Risk Appetite



Common Risk Types

- **Credit Risk:** When anyone lends money to another party, there is always a risk that the loan will not be repaid, either in full or in part.
- **Operational Risk:** The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events
- **Market Risk:** This is the risk of suffering a loss due to changes in the market, such as movements in interest rates.
- **Liquidity Risk:** A bank will always need to have sufficient funds available to meet the withdrawal demands of its depositors.
- **Regulatory Risk:** This is the risk of material loss, reputational damage or liability arising from the failure to comply properly with the requirements of regulators.

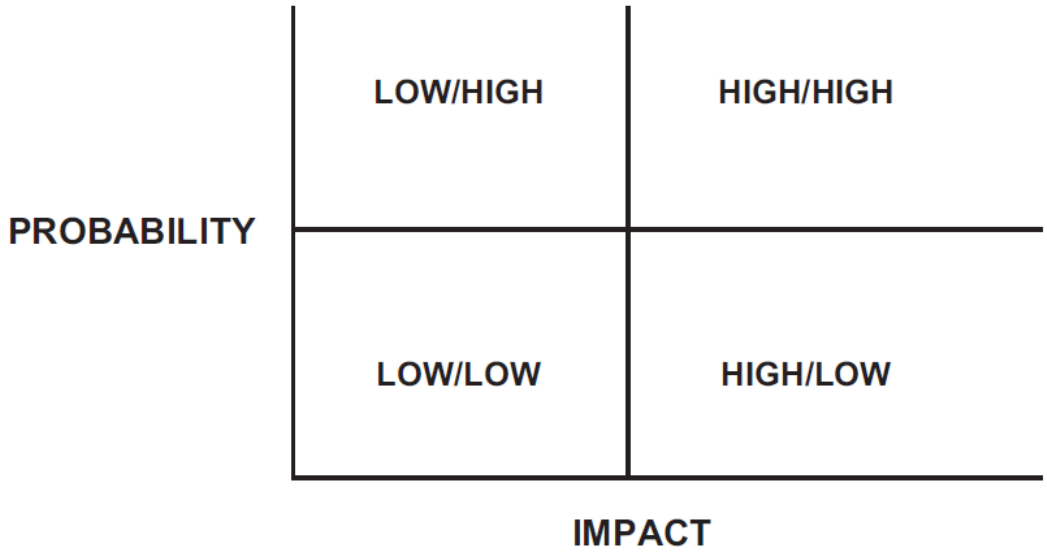
Risk Identification

It is vital that the management of risk is a proactive process, therefore, rather than waiting for the risk event to occur and the organization then deciding how to deal with it, the business must be constantly appraising both its internal and external environments to identify any risks that it may be facing. The process of risk identification must produce a clear understanding of what these risks are.

Risk Assessment

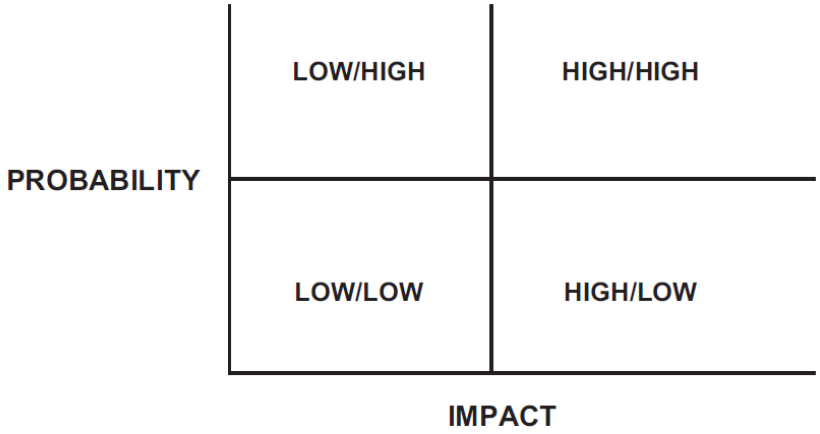
Once the business is clear about the risks it faces, decisions then have to be taken as to how likely is it that these risks will occur and if they do occur, what is their likely effect on the business.

Having assessed the probability and impact of the risk, the organization can move on to decide how best to mitigate the risks.



Risk Mitigation

Having identified and assessed the risks, we now need to come to a decision – what are we going to do to mitigate the risk? This again links to the impact and probability matrix..



- High probability/high impact - these are the risks to avoid
- Low impact but high probability – these risks must be controlled
- High impact but low probability - this type of risk would be managed by risk transference
- Low impact/low probability – generally these risks are accepted by organizations.

Risk Treatment Options

Risk avoidance

This is where the risk is such a threat to the business that it must simply be avoided. In other words the risk event is beyond the organization's current risk appetite.

Risk sharing

This is where the overall risk is reduced to an acceptable level by the organisation sharing the risk with another party, such as through a joint venture, which is when two or more organizations collaborate to deliver a product or service. By doing so they are sharing the risks associated with the venture.

Risk Treatment Options

Risk transfer

This is where the risk is transferred to another party who accepts the risk. Risk transference can apply to the risk itself or the financial consequences of the risk. An example of risk transference in financial services is when security companies are hired to transfer cash around the organization and it is the security company which accepts the associated risks.

Risk acceptance

There are times when an organization will feel that although risks are present they are worth accepting, possibly due to the potential resultant benefits. The consequences of the risk may be low, or the likelihood of the risk event occurring is low.

Operational Risk

The Basel Committee

The Basel Committee is a “club” of leading industrial countries including the Unites States, Spain, Japan, Germany, France and the United Kingdom.

The Committee formulates broad international financial services supervisory standards and guidelines in the expectation that individual regulatory authorities will implement them.

What is Operational Risk?

The Basel II Committee defines operational risk as:

"The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."

Basel I

1

Investors deposit money with a financial institution and in return receive interest for depositing the money

2

The money deposited by investors is used to lend to customers in the form of loans, mortgages, etc.

3

A financial institution must hold capital reserves to protect the depositors in the event of the institution becoming insolvent

4

The level of capital to be held is determined by the requirements of Basel Committee

Basel II Approaches for Operational Risk

	Basic Indicator Approach (BIA)	The Standardized Approach (TSA)	Advanced Measurement Approach (AMA)
Basis of Calculation Defined by	Regulator	Regulator	Self
Calculation Basis	15% of Group Income	12% to 18% of Income According to Business Line	Internally Developed Model
Standards	General Risk Management Standards	As BIA + Qualitative Criteria	As TSA + extra Qualitative & Quantitative Criteria

Operational Risk Categories

Operational Risk is broken down into the following categories:

1. Internal Fraud
2. External Fraud
3. Employment, health and security practices at work
4. Practices with clients products and business
5. Damage to physical assets
6. Interruption of business and failures in systems
7. Execution, delivery and management of processes

Operational Risk Profiling

- Understand the business
- Assess the risks
- Identify the potential causes and controls
- Evaluate the controls
- Measure the risk (likelihood and impact)
- Create action plans for improvement
- Monitor the risk

Operational Risk Event

A specific, identified occurrence of an operational risk regardless of whether the event ultimately gives rise to an actual loss.

A risk event can materialize as a loss, an unexpected gain or a near miss resulting from inadequate or failed processes within one of the risk categories. Commonly, the Basel II Operational Risk categories are used:

- Internal Fraud
- External Fraud
- Employment, health and security practices at work
- Practices with clients products and business
- Damage to physical assets
- Interruption of business and failures in systems
- Execution, delivery and management of processes

Types of Operational Risk Event

- Loss – operational risk event where a loss has been incurred

- Near Miss – an event where an actual gain or loss might have occurred but did not, due to corrective action and/or good fortune

- Gain – operational risk event that results in an overall positive direct impact as a result of good fortune

- Issue – an inadequate or failed process that has been identified but has not resulted in an immediate threat or potential loss

Why Identify, Capture and Manage Op Risk Events?

- Identify and assess the internal control environment and make any required enhancements

- Test and validate the effectiveness of the Op Risk management framework

- Learn from previous mistakes to help drive and shape process/control enhancements and prevent further occurrences

- Collect data to assist in capture, forecast and budget of expected losses.

Key Risk Indicators (KRI's)

•KRI's are linked to each key risk

• The ongoing monitoring of these key risks established an ongoing mechanism for review and update

• Where adverse trends are identified is the risk managerial action may be required, as well as review of the risk profile

•Examples of KRIs are:
• HR resource adequacy levels
• IT Critical incident resolution time
• Number of payment errors

Information Risk

The risk of unauthorized disclosure, corruption, unauthorized modification or loss of information

Examples:

• Sending or arranging to receive messages known to be infected, or containing files infected with a virus unless specifically requested by IT staff.

• Disclosure of confidential information to someone not authorized to access/know that information.

Examples of Breaches

- Improper disposal of confidential information (i.e. placing it in a regular trash can)

- Installation of unapproved software on Company computer systems without IT authorization

- Failure to follow “Clean Desk Policy”

Why is Operational Risk Management important…….

- Prudent and sound business practice
- Lower operating losses
- Competitive advantage
- Promotes financial stability
- Corporate Governance

Technology Risk

Agenda

- What is Technology Risk (TR)?
- Law, Regulation, Industry standards
- Who's risk is it? Roles and Responsibility
- Technology Risk Program
- Risk Treatment/Response
  - Cost/Benefit - Risk Reward
- What's next
- Summary – Takeaway

What is Technology Risk?

- Industry/common definition (or myths…)
- TLG's definition
  - Securing consumer data (Confidentiality and Integrity)
    - Who's risk is it? (or who assume the risk) – identifying the risk owners/ownership
    - What is at risk? Value of asset/process
  - Availability of service
- What is yours?

Risk = Likelihood * Impact

Risk = Probability * Impact

Risk = Probability * Velocity * Impact

Risk = Probability * Consequences

Risk = Threat * Vulnerability * Cost

Risk = FICO score

Risk = (Probability * Impact)/Control

Risk = Are you confused yet?

Law, Regulation, Industry Standard

- Law, Regulation, Industry Standard (Privacy, Security)
  - Financial
    - Gramm Leach Bliley Act, FFIEC, PCI DSS
  - Feds/Gov
    - NIST, HIPAA/HITECH
  - Industry Standards
    - ISO, SIG
- Framework
  - Cobit, COSO, ITIL, ISO.
- These are the **bare minimum** or industry accepted practice that you can use as guidance when performing assessment/gap analysis

Who's risk is it?

Roles and Responsibility

- Responsibility/Role assignment (example: RACI)
- Business, CIO, CTO, IT GRC, Information Security
- Risk Assessor – where do you see yourself in the lifecycle of risk management in your company?

Technology Risk Program

- 3rd party (IT) Assessment
  - 3rd party = vendor, supplier, business partners.
- Technology Risk Indicators – TRI (Key Risk Indicator)
- Enterprise Technology Risk Assessment
- Fraud investigation

3rd party (IT) Assessment

- Checklist
  - Gap analysis, assessment planning, **NOT for assessment**
- Define scope – be very specific
- Define constraints
  - time, resources, money
- Assumption
- Risk rating – rank and help prioritize review
  - Attestation reports?
  - Risk events?
  - Last visit/assess?
- Periodic assessment, one-off

3rd party (IT) Assessment (cont'd)

- Identify Goals and Objectives of your assessment (simplify and clarify)
  - TR v2 - Prepare risk statement(s) that would reference back to your goals or objectives
- Quantify the potential lost at a very high level (if possible)
- Create/'borrow' template to guide the evaluation process
- Remember it is an 'Assessment' not an 'Audit'

Risk Treatment/Response

- Cost/Benefit or Risk/Reward Analysis
- Risk owner/ownership
  - RACI
- Action Plan
- Avoid/eliminate, mitigate, transfer, accept
  - Avoid: Process change/re-architecture
  - Mitigate: Control
  - Transfer: Supplier/professional (email, cloud)
  - Accept: Cost/benefit analysis

What's next?

- Enhancement: 3rd party (IT) Assessment v2
  - Codification of risk statement
  - Scoring
- New: Cyber security (offense vs. defense)
- New: Threat matrix

TLG's Philosophy

Compliance ≠ Security

Risk ≠ Control

Trust but verify – Professional Skepticism

Simplify and Clarify

Gap Analysis/Checklist: Miles wide and inch deep

Risk Analysis: Miles/inch wide and miles/inch deep

Assessment not Audit

Summary - Takeaway

- Understand your business, vision, goals, operation
  - What is Technology Risk
  - Perform Gap Analysis
    - Compliance
    - Industry practice
- 3rd party (IT) assessment
  - How safe is your data once it leaves your control?
- Simplify and Clarify

Further Reading

COSO:
- Enterprise Risk Management Framework
- ERM – Understanding & Communicating Risk Appetite

Basel Committee on Banking Supervision:
- Principles for Sound Management of Operational Risk

Federal Reserve System:
- Operational Risk Management

Federal Trade Commission:
- Safeguarding Customers' Personal Information (FTC)

Federal Financial Institutions Examination Council (FFIEC):
- IT Handbook InfoBase

Information Systems Audit and Control Association (ISACA):
- RiskIT

BITS:
- BITS Publications: Security, Vendor Management, Data Governance, Fraud.

www.risk.net
www.theirm.org

Questions?

Thank you.

Graham Cameron, Chartered Banker, CRMA
gcameron@santanderconsumerusa.com
www.linkedin.com/in/grahamcameron76/

Tuck Goh, CISA, CISM, CISSP
tlgoh@santanderconsumerusa.com
www.linkedin.com/in/tuckgoh