FRM Part II

Operational Risk And Resilience

INTRODUCTION TO OPERATIONAL RISK AND RESILIENCE

Learning Objectives

After completing this reading you should be able to:

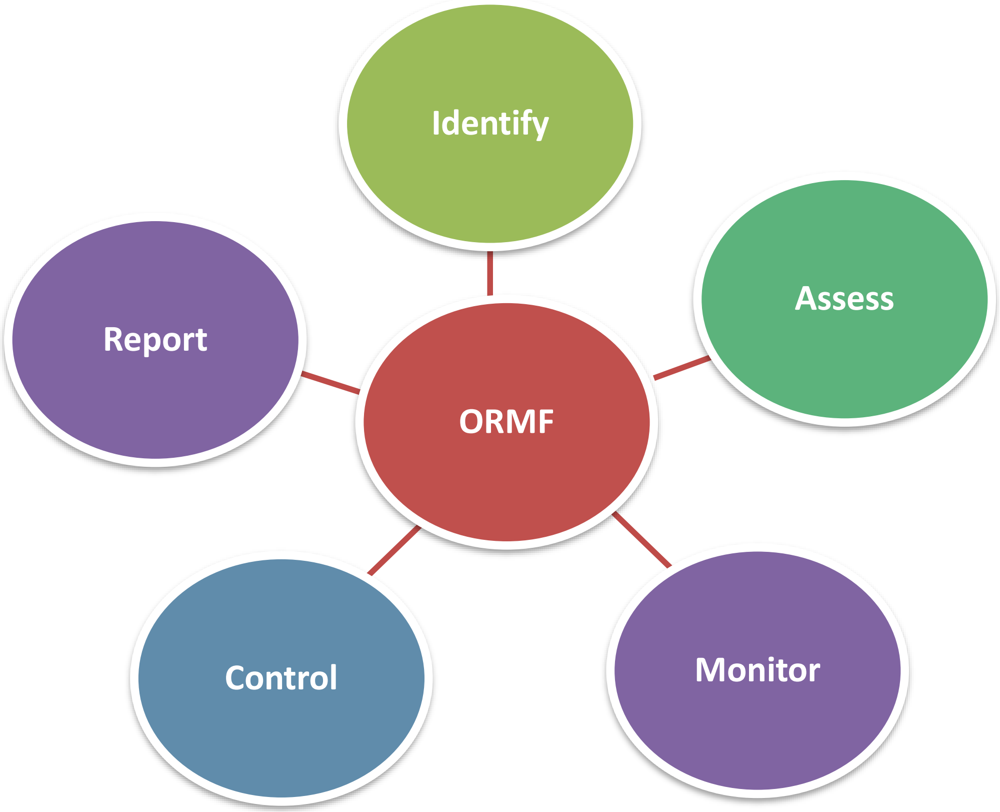
- ✓ Describe an **operational risk management framework** and assess the types of risks that can fall within the scope of such a framework.
- ✓ Describe the **seven Basel II event risk categories** and identify **examples** of operational risk events in each category.
- ✓ Explain **characteristics** of **operational risk exposures** and **operational loss events**, and **challenges** that can arise in managing operational risk due to these characteristics.
- ✓ Describe **operational Resilience**, identify the elements of an operational resilience framework, and summarize regulatory expectations for operational Resilience.

Operational Risk Management Framework

Describe an operational risk management framework and assess the types of risks that can fall within the scope of such a framework.

Operational Risk Management Framework (ORMF):

- **A system of processes, controls, and practices** designed to help organizations manage risks associated with their operations.
- **Designed to identify, assess, monitor, control, and report** operational risks across all areas of the business.



Operational Risk Management Framework

Types of Risks that Fall Within the Scope of this Framework

System failure

Arises when systems that are integral to the operations of a company fail due to hardware, software, or connectivity issues.

Human error

Poor decision-making and careless mistakes can lead to compliance violations, customer service issues, and financial losses.

Fraud and unethical activity

Employees or external parties can engage in unethical activities such as **bribery**, **insider trading**, and **embezzlement**.

Regulatory violations

If a company fails to comply with applicable laws and regulations, they may be subject to **fines** or other **penalties**.

Outsourcing risks

When outsourcing services to third-party vendors, companies need to ensure that these vendors are **reputable** and **trustworthy**.

Basel II Event Risk Categories

Describe the seven Basel II event risk categories and identify examples of operational risk events in each category.

- Basel II is a set of international banking regulations created to **strengthen** the banking system and make it more resilient to shocks.
- One of the **core elements** of Basel II is the seven event risk categories, which help banks identify and manage potential risks.

Basel II Event Risk Categories

- 75% of the **frequency** of operational risk events are concentrated in four categories: EF, EPWS, CPBP, and EDPM.

		Acronym		Frequency	Severity
1	Internal fraud	IF	Unauthorized employee activity	2%	2%
2	External fraud	EF	Theft and fraud, hacking damage	30%	9%
3	Employment practices and workplace safety	EPWS	Contract termination issues, discrimination	15%	5%
4	Clients, products, and business practices	CPBP	Client misinformation, complaints, and product misspecification	22%	52%
5	Damage to physical assets	DPA	Destruction of equipment, natural disasters, losses	1%	1%
6	Business disruption and system failures	BDSF	IT breakdown, outages	2%	5%
7	Execution, delivery, and process management	EDPM	Processing errors, missing documentation	28%	27%

Basel II Event Risk Categories

- Three event types—EF, CPBP and EDPM—are enough to explain **86**% of the severity.

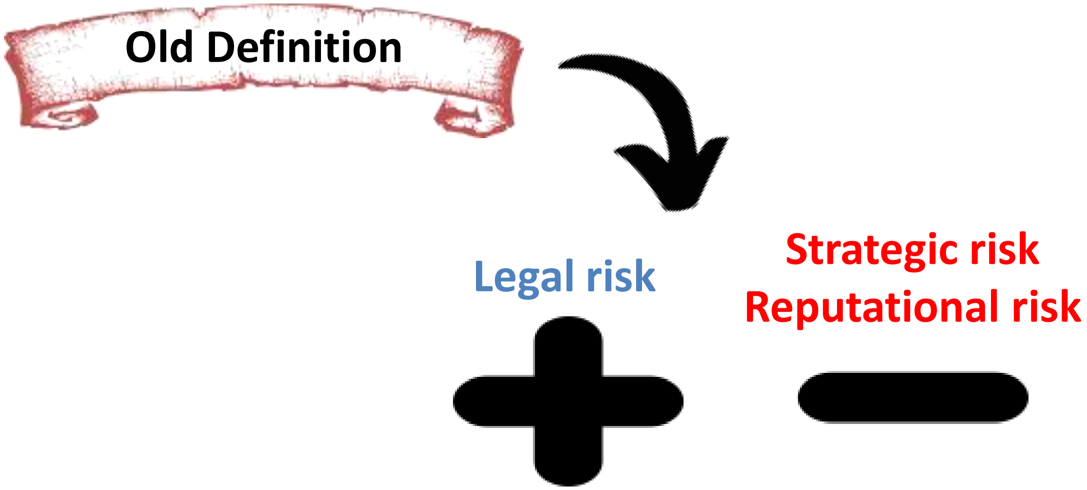
		Acronym		Frequency	Severity
1	Internal fraud	IF	Unauthorized employee activity	2%	2%
2	External fraud	EF	Theft and fraud, hacking damage	30%	9%
3	Employment practices and workplace safety	EPWS	Contract termination issues, discrimination	15%	5%
4	Clients, products, and business practices	CPBP	Client misinformation, complaints, and product misspecification	22%	52%
5	Damage to physical assets	DPA	Destruction of equipment, natural disasters, losses	1%	1%
6	Business disruption and system failures	BDSF	IT breakdown, outages	2%	5%
7	Execution, delivery, and process management	EDPM	Processing errors, missing documentation	28%	27%

Operational Risk Exposures and Operational Loss Events

Explain characteristics of operational risk exposures and operational loss events, and challenges that can arise in managing operational risk due to these characteristics.

Operational Risk

- “The risk of loss resulting from **inadequate or failed internal processes**, **people**, and **systems**, or from **external events**.”
- This age-old definition **includes legal risk** but excludes **strategic and reputational risk**.



Old Definition

Legal risk

+

Strategic risk

Reputational risk

−

- **BCBS** revised the definition, stating, "Where appropriate, strategic and reputational risks **should be considered** by banks’ operational risk management."

Operational Risk Exposures and Operational Loss Events

Operational Risk

Legal Risk

- •Arises from a failure to comply with laws and regulations.
- •Can include **regulatory fines, penalties,** and **other legal actions** against the company.

Reputational Risk

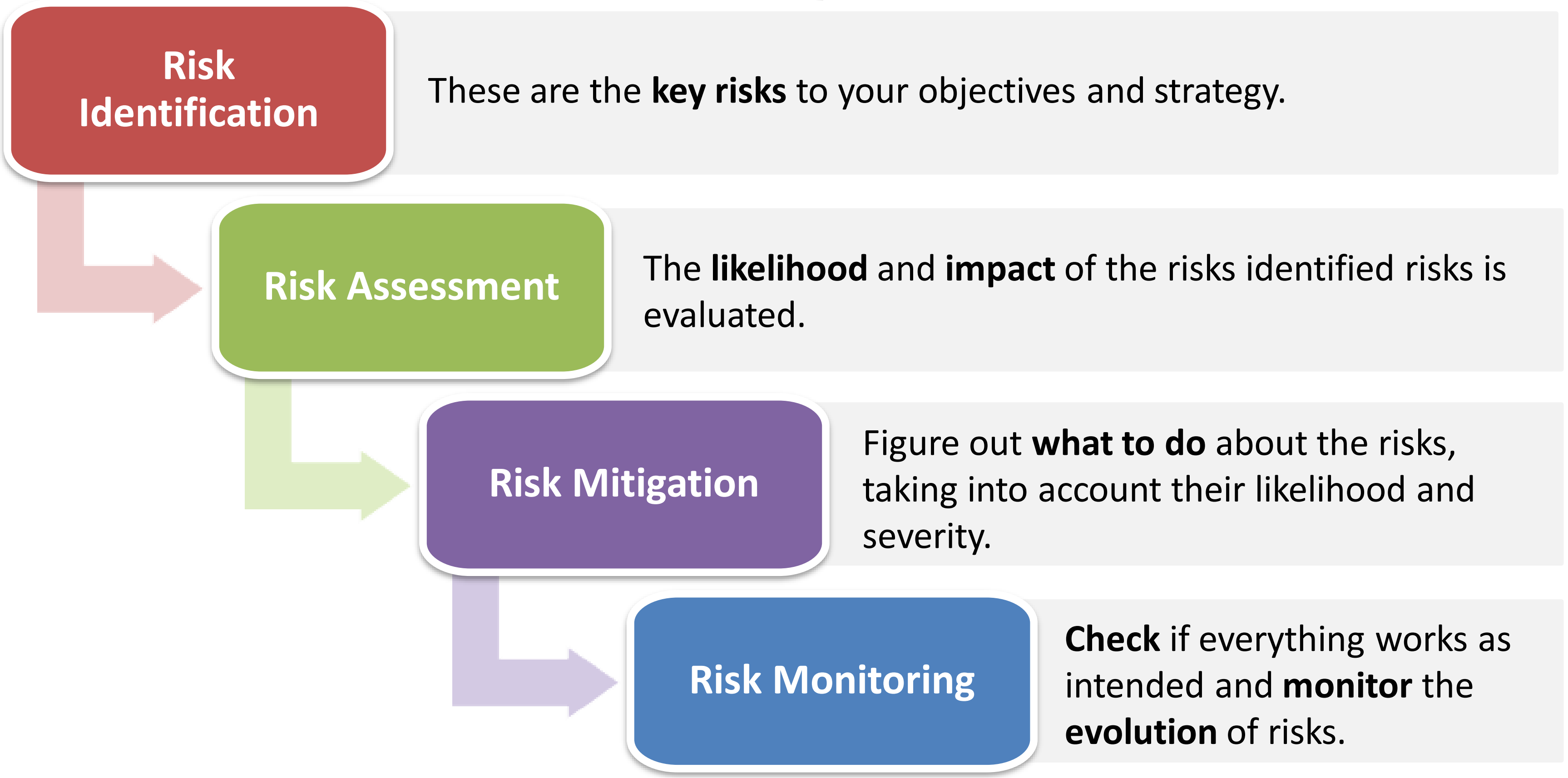
- •Potential for loss of business or damage to a company's image due to **poor decisions** or **unethical behavior** by its employees.

Strategic Risk

- • Risk of losses due to **wrong decisions** or **failed execution** of a given strategy.

Operational Risk Exposures and Operational Loss Events

Risk Management Process: Four Actions



Risk Identification

These are the **key risks** to your objectives and strategy.

Risk Assessment

The **likelihood** and **impact** of the risks identified risks is evaluated.

Risk Mitigation

Figure out **what to do** about the risks, taking into account their likelihood and severity.

Risk Monitoring

Check if everything works as intended and **monitor** the **evolution** of risks.

Operational Risk Exposures and Operational Loss Events

Characteristics of Operational Risk Exposures and Operational Loss Events

Heterogenous

- Operational risk is **varied and multifaceted.**
- Has different sources, effects, and distributions of losses.
- For example, external fraud incidents can range from cyber-attacks to stolen credit cards.

Idiosyncratic

- Some risks are **specific** to a firm.
- Risk management strategies such as avoidance, hedging, and insurance can reduce operational risks.
- But are **not enough to completely eliminate** them.

Heavy-tailed

- Operational risk has a "heavy tail" distribution curve.
- **Extreme losses are more probable than predicted** by a normal distribution.
- Due to difficulty in forecasting very **unusual events.**
- **"Black swan" events**—low-probability but high-impact occurrences—can lead to significant unanticipated losses.

Operational Resilience

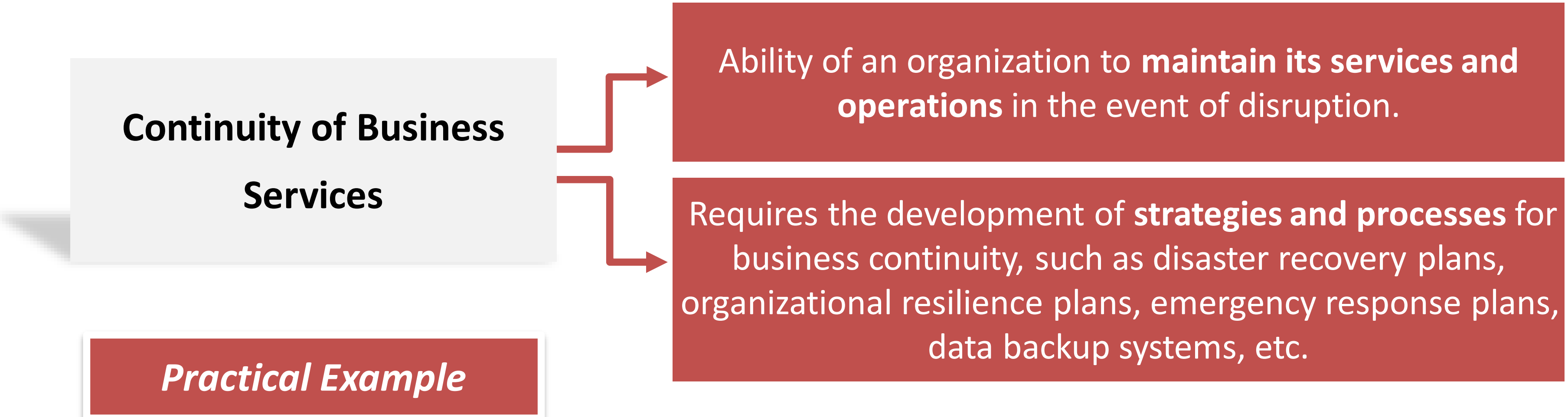
Describe operational resilience, identify the elements of an operational resilience framework, and summarize regulatory expectations for operational Resilience.

Operational Resilience

- An organization's capacity to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions to survive and prosper.
- Involves **assessing current processes, systems, policies, procedures, and resources** to identify potential risks or weaknesses that may lead to business interruptions.
- Its goal is to **build a proactive plan of action** that allows the organization to be resilient in the face of increasingly severe and unpredictable stressors or shocks.
- Involves **implementing strategies** such as regular risk assessments, regular reviews of existing processes and systems, and developing response plans.
- Organizations must **understand their critical operations** to identify potential **areas of vulnerability** and develop measures that will help them survive any disruption.

Operational Resilience

Elements of An Operational Resilience Framework



Continuity of Business Services

Ability of an organization to **maintain its services and operations** in the event of disruption.

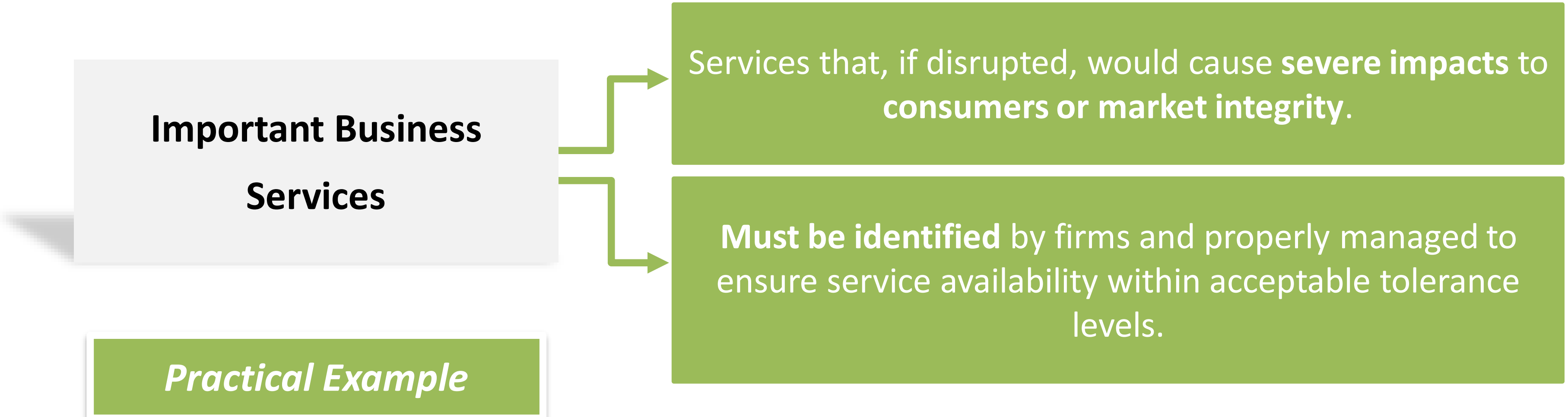
Requires the development of **strategies and processes** for business continuity, such as disaster recovery plans, organizational resilience plans, emergency response plans, data backup systems, etc.

Practical Example

An **emergency backup system** that provides **redundant resources and IT infrastructure** to ensure the continued functioning of core banking services during a crisis. It would include reliable **online backups**, automated failover to **alternative servers**, **cloud hosting** for storing customer data, **regular backups** on encrypted media, **secure access**, and **offsite server replication**. All of this would help keep banks operational even in the face of major disaster.

Operational Resilience

Elements of An Operational Resilience Framework



Important Business Services

Services that, if disrupted, would cause **severe impacts** to **consumers or market integrity**.

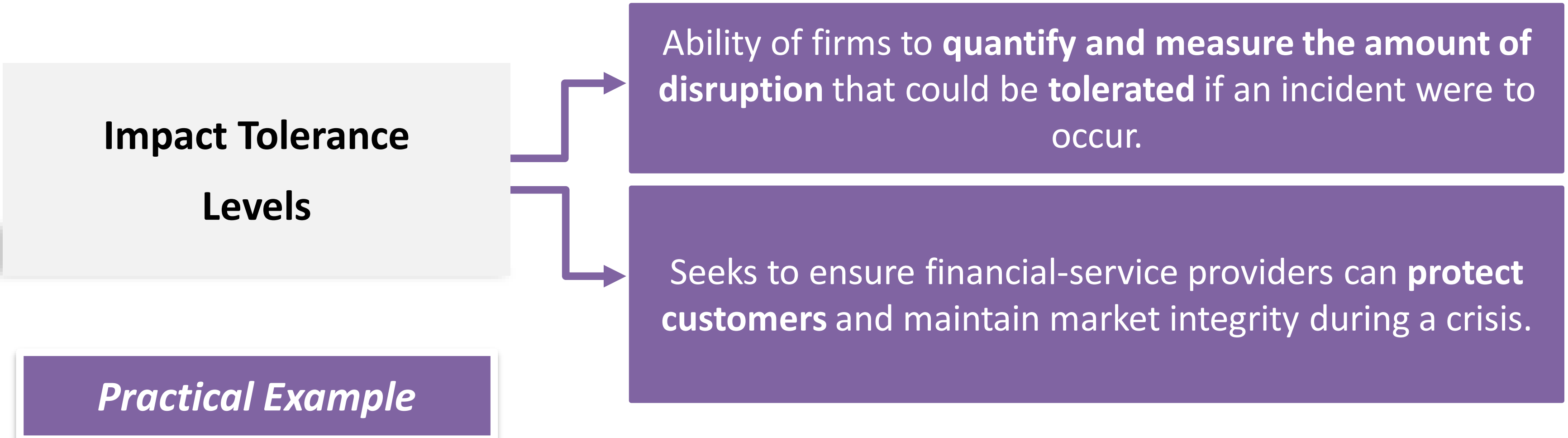
Must be identified by firms and properly managed to ensure service availability within acceptable tolerance levels.

Practical Example

If a bank establishes that one of its important business services is provision of **ATM machines** for cash withdrawals, it must ensure customers have constant access to their money through functioning hardware and software, regularly stocked ATMs (with cash), and secure machines. Additionally, it also needs updated technical support for any user issues.

Operational Resilience

Elements of An Operational Resilience Framework



Impact Tolerance Levels

Ability of firms to **quantify and measure the amount of disruption** that could be **tolerated** if an incident were to occur.

Seeks to ensure financial-service providers can **protect customers** and maintain market integrity during a crisis.

Practical Example

The amount of fluctuation a bank can handle in terms of its **risk-weighted assets**. For example, **Central Banks have set limits** for what they consider to be acceptable fluctuations in these assets, which vary depending on the region and other factors. Banks must maintain **required ratios of capital to assets**, with some facing stricter requirements for depositor protection. They must also have **appropriate liquidity** to absorb losses without disrupting operations.

Operational Resilience

Elements of An Operational Resilience Framework

Management of Disruption

Involves managing disruptions effectively so as to **minimize their impact** on an organization's business operations.

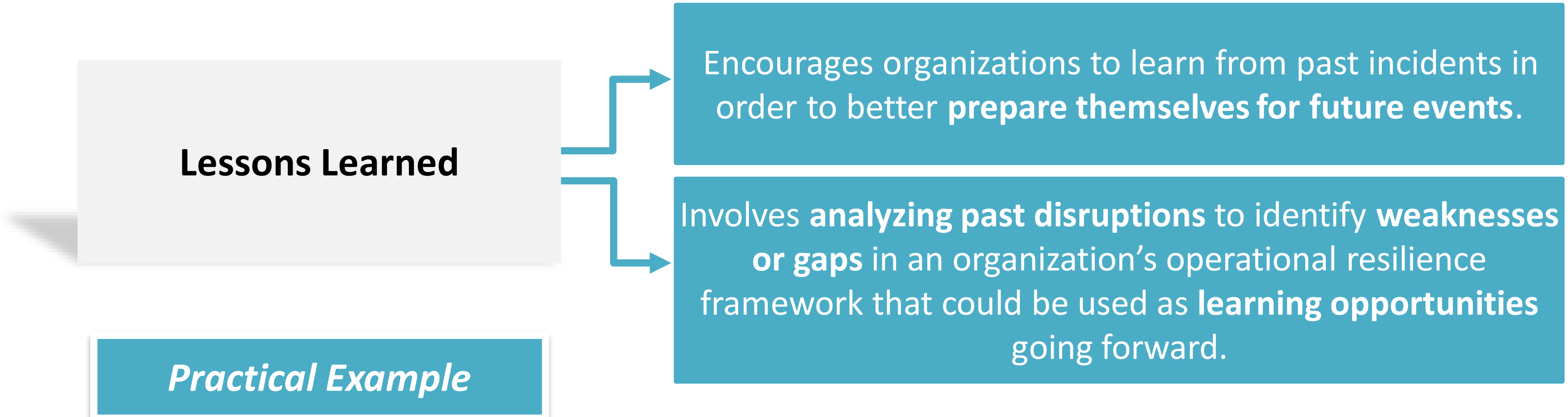
Strategies for managing disruptions can include setting up a **crisis management team**, and developing **incident response plans**, creating **early warning systems**, and conducting **regular reviews of processes**.

Practical Example

If a bank happens to experience a **massive data breach**, it may take quick action by **notifying customers**, issuing new cards and passwords, and providing step-by-step instructions on how to protect their information. The bank may also implement protective measures such as **multi-factor authentication**, additional encryption layers, and regular security reviews.

Operational Resilience

Elements of An Operational Resilience Framework



Lessons Learned

Encourages organizations to learn from past incidents in order to better **prepare themselves for future events**.

Involves **analyzing past disruptions** to identify **weaknesses or gaps** in an organization’s operational resilience framework that could be used as **learning opportunities** going forward.

Practical Example

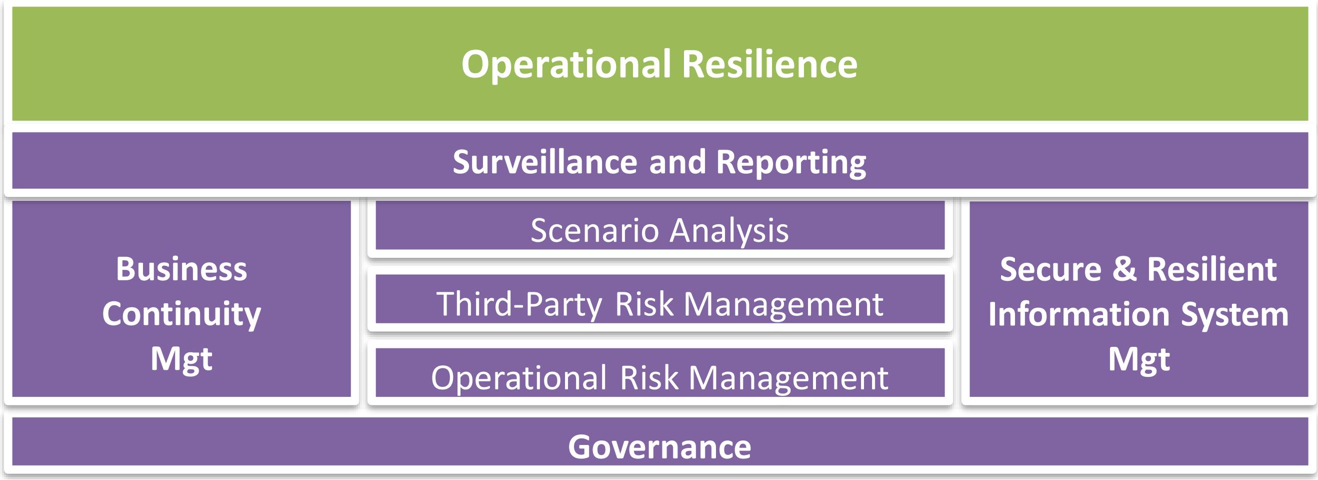
In case of **employee fraud**, a bank must institute **corrective measures** such as regular fraud checks, tighter controls, vigilant access grants, anti-fraud programs, monitoring of user activity, and background checks on staff.

Operational Resilience

Regulatory Expectations for Operational Resilience

U.S. Regulation

- The Federal Reserve released new standards in 2020, stressing the necessity of **embedding operational Resilience within a holistic enterprise management system**.
- This guidance promotes:
  - Establishment of **tolerance impact levels** for essential business services
  - Encourages organizations to consider operational Resilience as a **critical outcome** of an effective Operational Risk Management Framework (ORMF).


Operational Resilience
Surveillance and Reporting
Business Continuity Mgt
Scenario Analysis
Third-Party Risk Management
Operational Risk Management
Secure & Resilient Information System Mgt
Governance

Operational Resilience

Regulatory Expectations for Operational Resilience

BCBS Regulation

Governance

- Banks should use a **comprehensive, risk-based approach** to ensure the alignment of their governance framework with the delivery of operational resilience objectives.

Operational Risk Management

- Banks should have a **strong integrated control environment** in place to identify, assess, monitor and control operational risks across all business activities.

Business Continuity Planning and Testing

- Banks should **systematically identify and prioritize potential threats**, and regularly test and review their contingency plans to ensure that they are fit for purpose.

Operational Resilience

Regulatory Expectations for Operational Resilience

Mapping Interconnections

- Banks must be able to **pinpoint and track the connections** between internal systems and processes as well as external parties that support critical operations.

Third-Party Dependency

- Banks must implement **robust due diligence procedures** to manage relationships with third parties in order to minimize potential disruption or service degradation.

Incident Management

- Banks should develop **comprehensive plans** to address incidents that could disrupt the delivery of critical operations.

ICT including Cybersecurity

- Banks must ensure their **ICT systems are secure** by proactively monitoring them, continuously evaluating **security controls** and regularly testing procedures to protect against cyber threats.

FRM Part II

Operational Risk And Resilience

INTRODUCTION TO OPERATIONAL RISK AND RESILIENCE

Learning Objectives Recap:

- ✓ Describe an **operational risk management framework** and assess the types of risks that can fall within the scope of such a framework.
- ✓ Describe the **seven Basel II event risk categories** and identify **examples** of operational risk events in each category.
- ✓ Explain **characteristics** of **operational risk exposures** and **operational loss events**, and **challenges** that can arise in managing operational risk due to these characteristics.
- ✓ Describe **operational Resilience**, identify the elements of an operational resilience framework, and summarize regulatory expectations for operational Resilience.