Deloitte.

Operational risk management

Azerbaijan International Insurance Forum 2015

Tural Hajiyev 2-3 July, 2015

Content

1. Importance of operational risk management

Expected benefits from operational risk management

Increased transparency

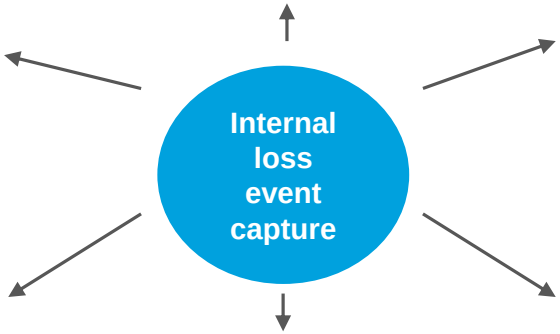
- Identifies key sources & costs of risks
- Facilitates escalation of issues
- Enables prioritization of activities

Customer service

- Supports customer service

External stakeholders

- Demonstrates that operational risks are under control



Regulatory compliance

- Complies with regulatory requirements
- Enables future progression to more advanced

Financial benefit

- Cost identification and reduction
- Supports cost / benefit analysis of improvements / controls

Internal stakeholders

- Improves understanding of risk losses
- Enables oversight of losses
- Validates control effectiveness and enables corrective action

Examples of most frequent sources of operational risk

2. Operational risk fundamentals

Operational risk management process

Key focus of our seminar

Identification and assessment

- Involvement of all staff
- Loss reporting, SCSA, new product approval
- Qualitative and quantitative assessment

Monitoring and control

- Monitoring of Key risk indicators
- Results: identification of trends in operational risk profile

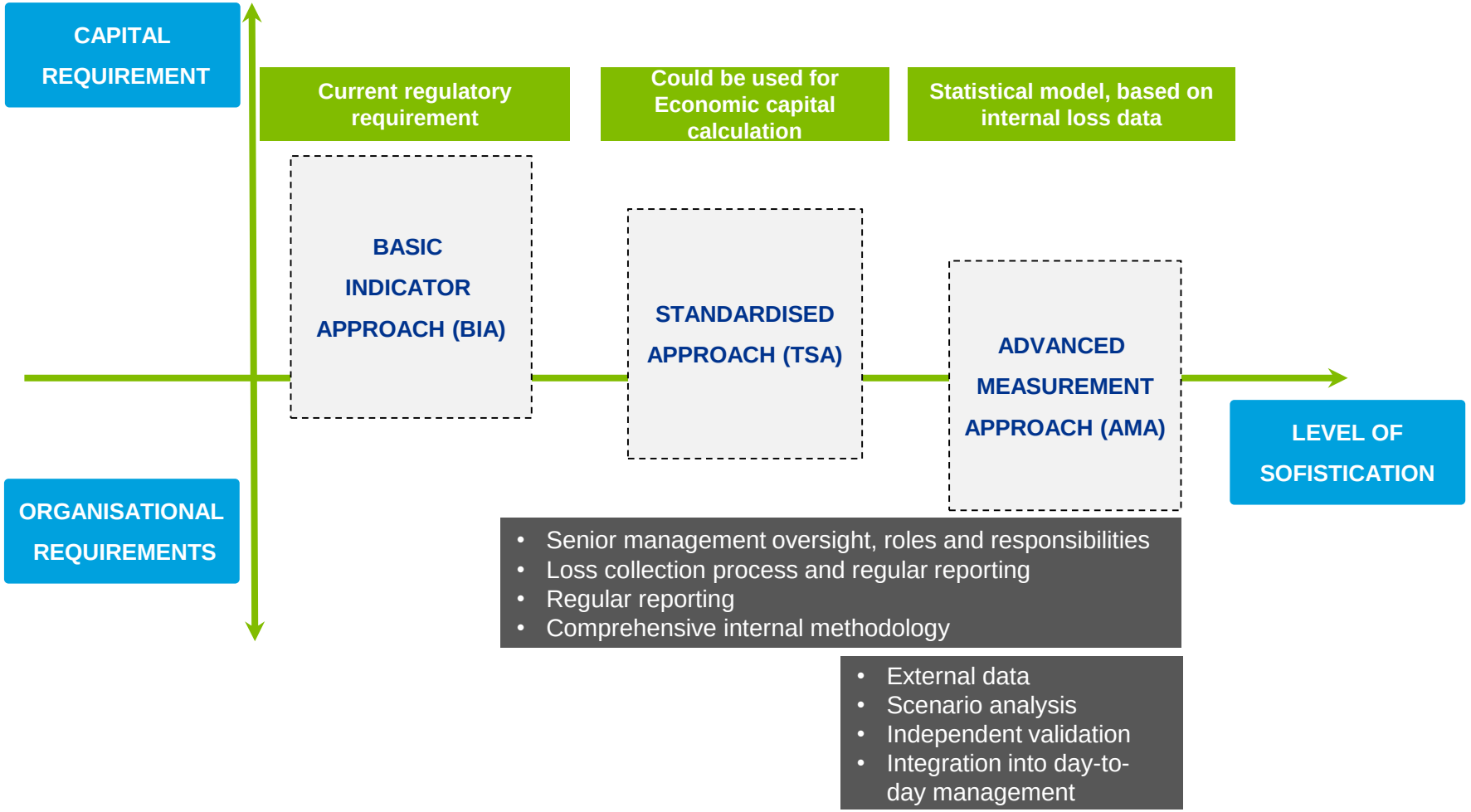
Risk mitigation

- Acceptance
- Minimization
- Avoidance
- Risk transfer

Reporting

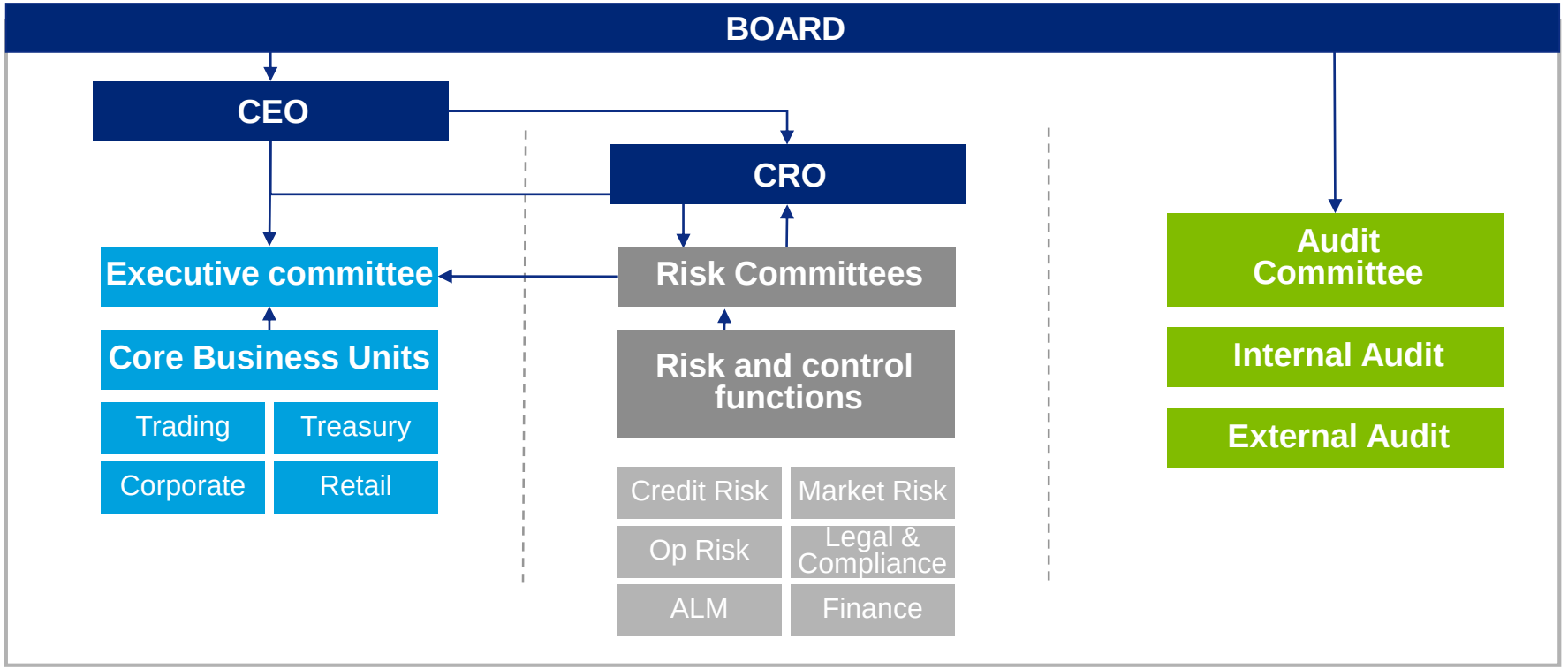
- Unified reporting system
- Timely and comprehensive reports
- Reconciliation with , initial sources

Operational risk management approaches (Basel requirements)



The «three lines of defense» model

Example



1st Line: Primary risk management

2nd Line: Challenge and risk control

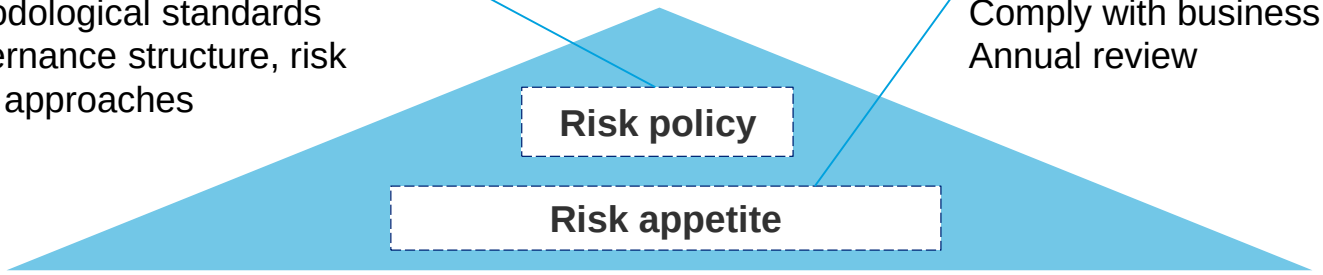
3rd Line: Assurance

Risk governance framework

Policies and tools: necessary elements for operational risk management framework

Overall methodological standards
Includes governance structure, risk management approaches

Comply with business strategy
Annual review



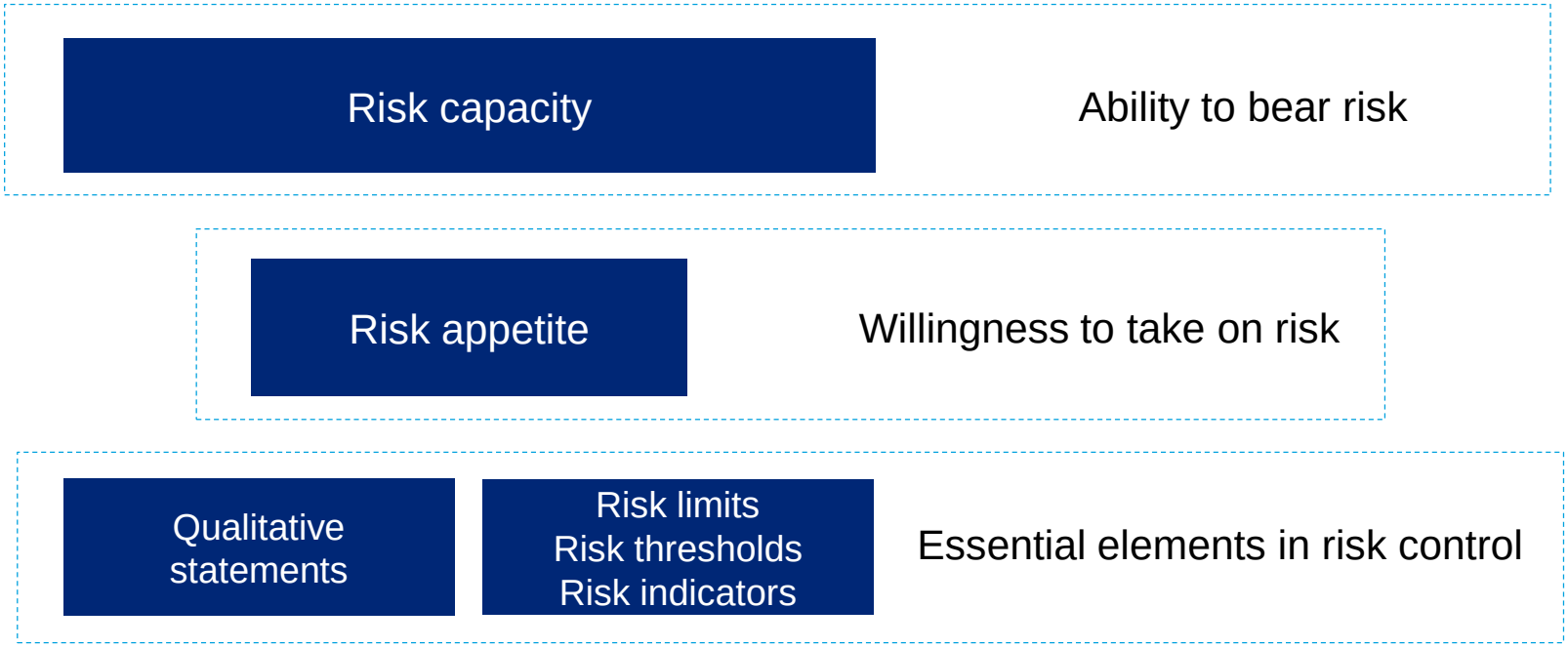
Org_structure	Organizational structure	Job descriptions
Loss data	Description of internal loss collection process	
Risk assessment	RCSA methodology	New product approval process
KRIs	List of KRIs	Monitoring and control regulation
Capital calculation	Methodology for regulatory and economic capital calculation	
Risk mitigation	BCPs, insurance policy, risk mitigation database	
Reporting	Reporting workflow	Reporting templates
Data and Systems	Loss Database, IT-tools	

What is an Operational risk policy?

Risk policy outlines an organization's risk management strategy and objectives for a given risk class. It encompasses the following areas:

What is a Risk appetite?

- Risk appetite reflects **the amount of risk taking that is acceptable to an organization.**
- Risk appetite refers to the organization's attitude towards risk taking.
- Risk appetite is a function of the organization's capacity to bear risk.
- Risk appetite can also be viewed as **assigned or allocated risk capacity.**



Example of Risk appetite articulation via qualitative statements

One approach to articulating risk appetite involves a series of qualitative statements detailing the specific risks that a business is or is not prepared to tolerate

Examples of Risk appetite statements

- Business has zero risk appetite for fraudulent activity
- Business has a low operational risk appetite.
- Business has a very low appetite for reputational risk exposure. The business will always need to take all steps to minimize the likelihood of adverse reputational impact

"+" Advantages

- Easy to define
- Useful in areas where quantification may be an issue

"-" Disadvantages

- No figures, difficult to measure
- Not easy assessment of the relative significance of actual breaches
- Complicated aggregation
- Incompleteness

Example of Risk appetite articulation via quantitative methods: thresholds

Thresholds could be set according to traffic lights:

- **«green» range** acceptable;
- **«amber» range** may be tolerated
- **«red» range** unacceptable

Thresholds examples

- Yearly (or quarterly) loss amounts;
- Number of operational risk events;
- Size of any one single operational loss;
- Degree to which operational loss levels or the number of operational risk events can increase in a given year;

"+" Advantages

- Facilitates monitoring
- Permits assessment of relative significance of breaches
- Permits aggregation and comparison
- Flexible

"-" Disadvantages

- Method of deriving may be subjective, some areas may find it difficult to define and relate to threshold

Example of Risk appetite articulation via quantitative methods: key risk indicators

Key risk indicators (KRIs) are:
1) Parameters that are assumed to be **highly predictive** regarding changes in the risk profile;
2) Designed to **monitor the development** of significant risks.

Examples of KRIs (for staff turnover level)

1) **below 24% – No risk.**;
2) **above 24% – Potential risk.** HR should monitor actively, establish causes and actions
3) **above 28% – Risk.** Action and escalation with explanatory report required.

"+" Advantages

- Easy to monitor, quick view of overall performance against target
- Tailored to different parts of the business
- Flexible. Can be adjusted to provide the "right level" of Board oversight

"-" Disadvantages

- Requires in-depth knowledge of risk areas process
- May be difficult to derive or establish in some risk areas and operational processes
- Does not permit assessment of relative significance of breaches across different KRIs
- Does not permit aggregation of risk appetite

Example of Risk appetite articulation via quantitative methods: limits

Limits may be set by the Board for operational risk outcomes:

Examples of operational risk limits

- **aggregate limit –** total annual operational risk losses, arising from both expected and unexpected events, is not to exceed (tbd) USD;
- **single event limit –** no single unexpected operational risk loss in a single year should exceed (tbd) USD

"+" Advantages

- Provide an overall measure of acceptable outcome in any one year or other timeframe
- Single event limits provides clear direction on levels of acceptable/ unacceptable exposure
- ELs can be tied in to the budget process
- Facilitates monitoring

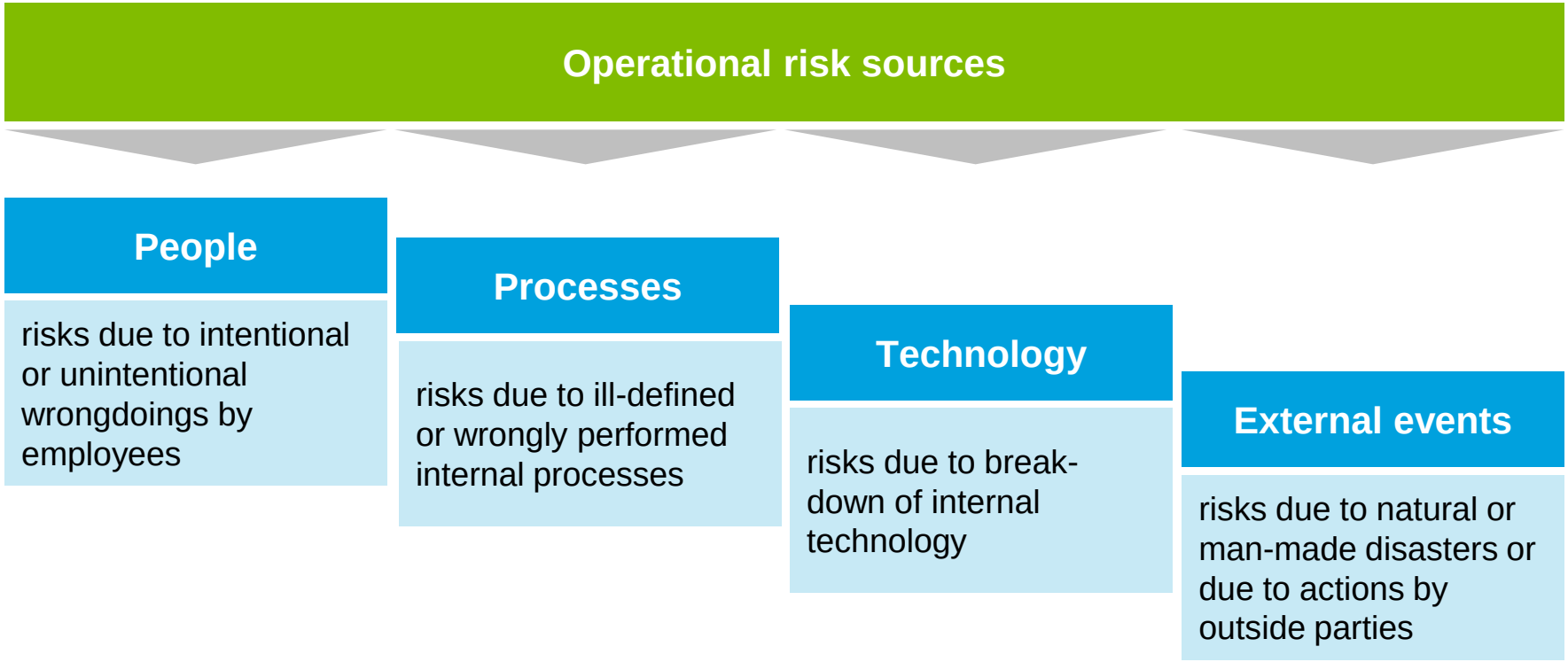
"-" Disadvantages

- Dependent on Board and senior management having defined overall appetite for risk and being able to attribute an acceptable volatility to operational risk

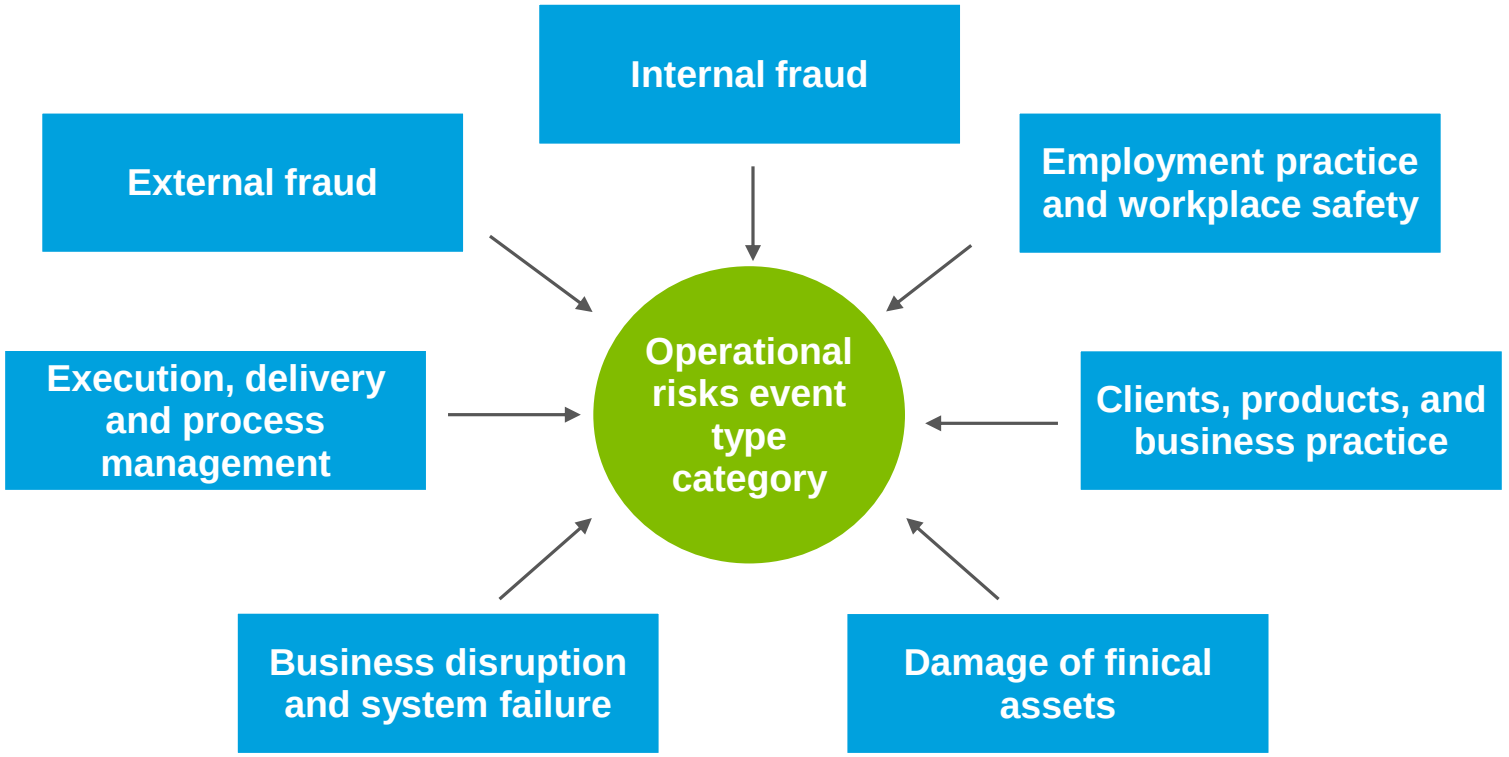
3. Operational risk definitions and language

Operational risk definition and cources

Operational risk is usually defined as the risk of loss resulting from inadequate or failed internal **processes, people and systems** or from external events. This definition includes legal risk, but excludes strategic and reputational risk



Operational risk categories, Level 1 (Basel II framework)



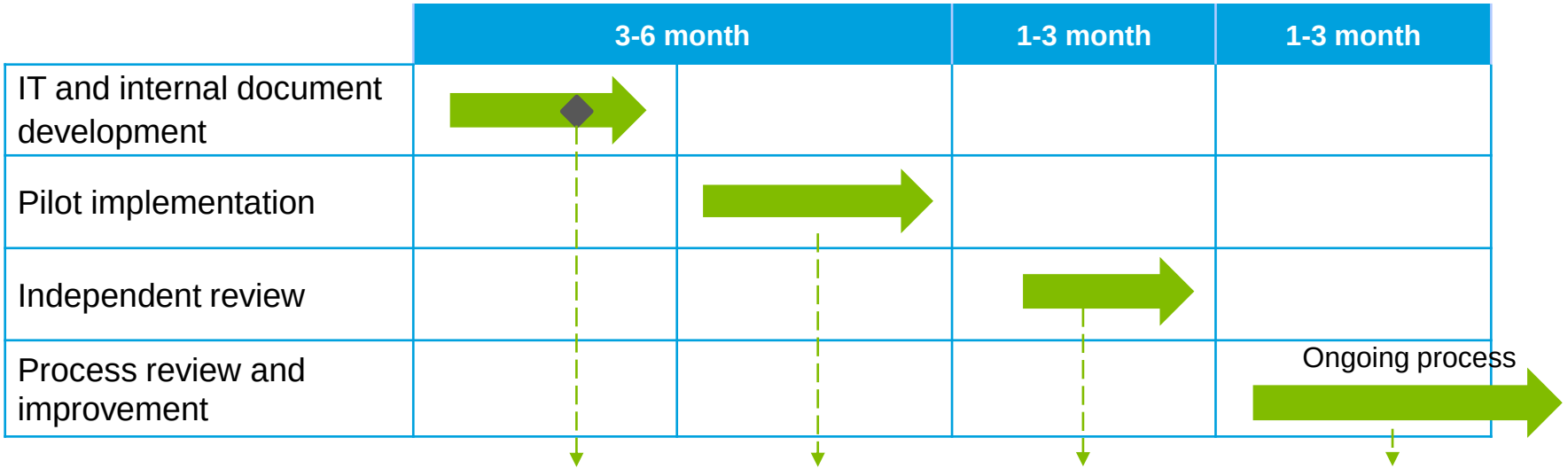
It is important to develop internal description and sup-categorization of operational risk, based on classification, provided by regulator

Classification of operational risk loss

Actual losses (due to real operational risk event)		Potential losses
Direct	**Indirect**	
Direct impact on net profit	Are not reflected directly in the P&L, iindirectly affect the financial result	Loss to occur in the future, with a certain degree of probability
• Decrease in asset value • Undrawn profit • Write-off of tangible assets • Recourse, transaction loss • Fines • Recovery costs, etc.	• Loss of potential profits • Additional labor cost • Suspension of activities Loss of customers loss of reputation	

4. Internal loss events

What practical steps are necessary for implementation?



- MS Excel and/or Access software
- bespoke operational risk software
- Internal documents
- Training materials

- Briefing of senior management
- Business unit workshops facilitated by risk management

- Internal auditor or external consultant review to provide assurance that loss data collection is focused on key risk events and is robustly implemented,

- Refinement and assurance of loss data and supporting process

Internal loss database requirements

A robust operational risk framework requires development of a database to capture loss events attributable to the different categories of operational risk (people, processes, systems and external events).

Next slides provides an example breakdown of data fields that a bank could apply when collating internal loss data. Bank may consider initiating the collection of operational risk loss data using the key fields below and develop the fields of data further as the process matures

Internal loss database structure (1/2)

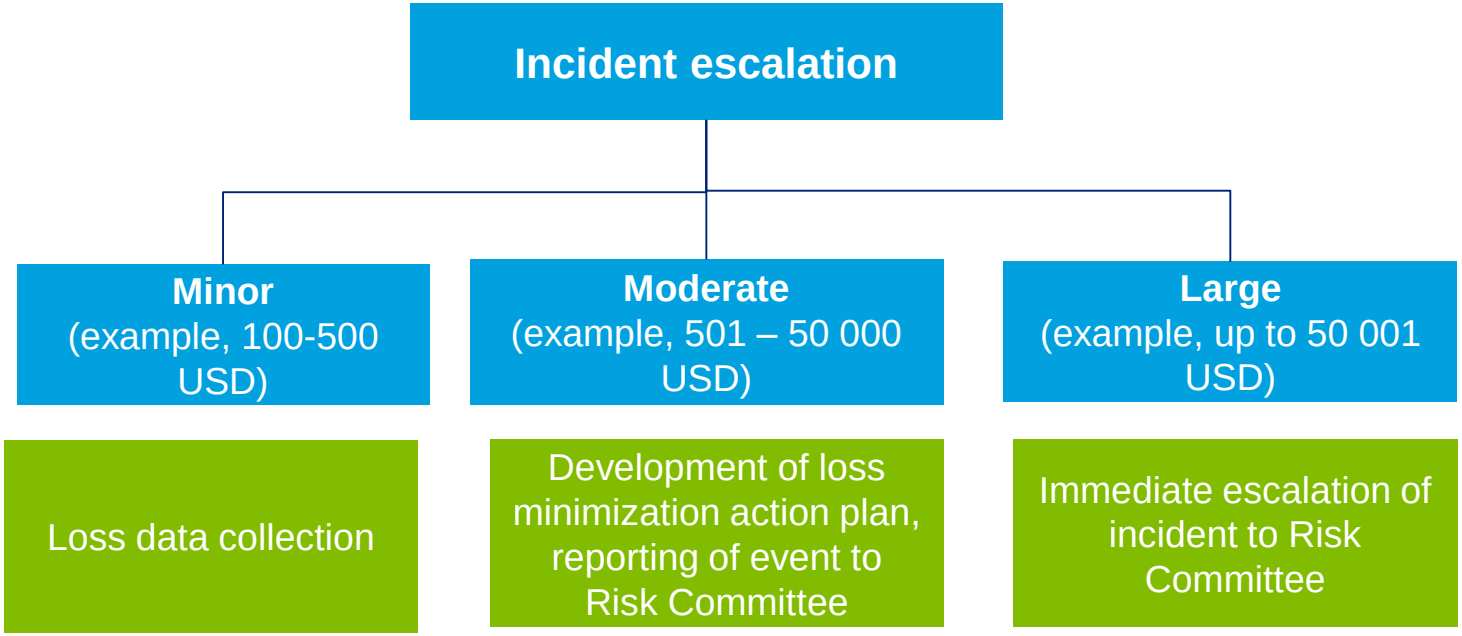
Data fields	Description
Reported by	Name of person reporting the incident
Incident owner	Name of person who has overall accountability for the management of the incident
Business line	Business line in accordance with standard or internal classification
Date of incident DD/MM/YY	Date the incident occurred
Reporting date MMM/YY	Month and year the incident was reported
Method of detection	How the incident was identified (a free text field)
Incident type	Risk type (actual loss, potential loss)
Incident open/closed	Open or closed status

Internal loss database structure (2/2)

Data fields	Description
Total cost to date	Total costs incurred to date (once closed this should be total cost of the incident)
Maximum potential loss	Maximum potential amount that could be lost if the incident had or were to occur – if applicable (could be used for scenario analysis)
Incident description	Description of the incident
Incident cause	Cause of the incident (new risk, control failure, other)
Incident cause categorization	People, processes, systems or external events
Actions	Remedial actions taken (or to be taken) since incident occurred. NB: should include actions to be taken to recover lost funds as well as actions to be taken to enhance the control environment
Actions due date DD/MM/YY	Due dates for the action listed in previous column to be completed
Actions complete? Yes/no	Whether actions are complete

Loss event thresholds and escalation process

Example



! **Basel:** A bank must have an appropriate de minimis gross loss threshold for internal loss data collection, for example €10,000. The appropriate threshold may vary somewhat between banks, and within a bank across business lines and/or event types. However, particular thresholds should be broadly consistent with those used by peer banks.

Principles of collection of operational risk events, which need to be articulated across organization

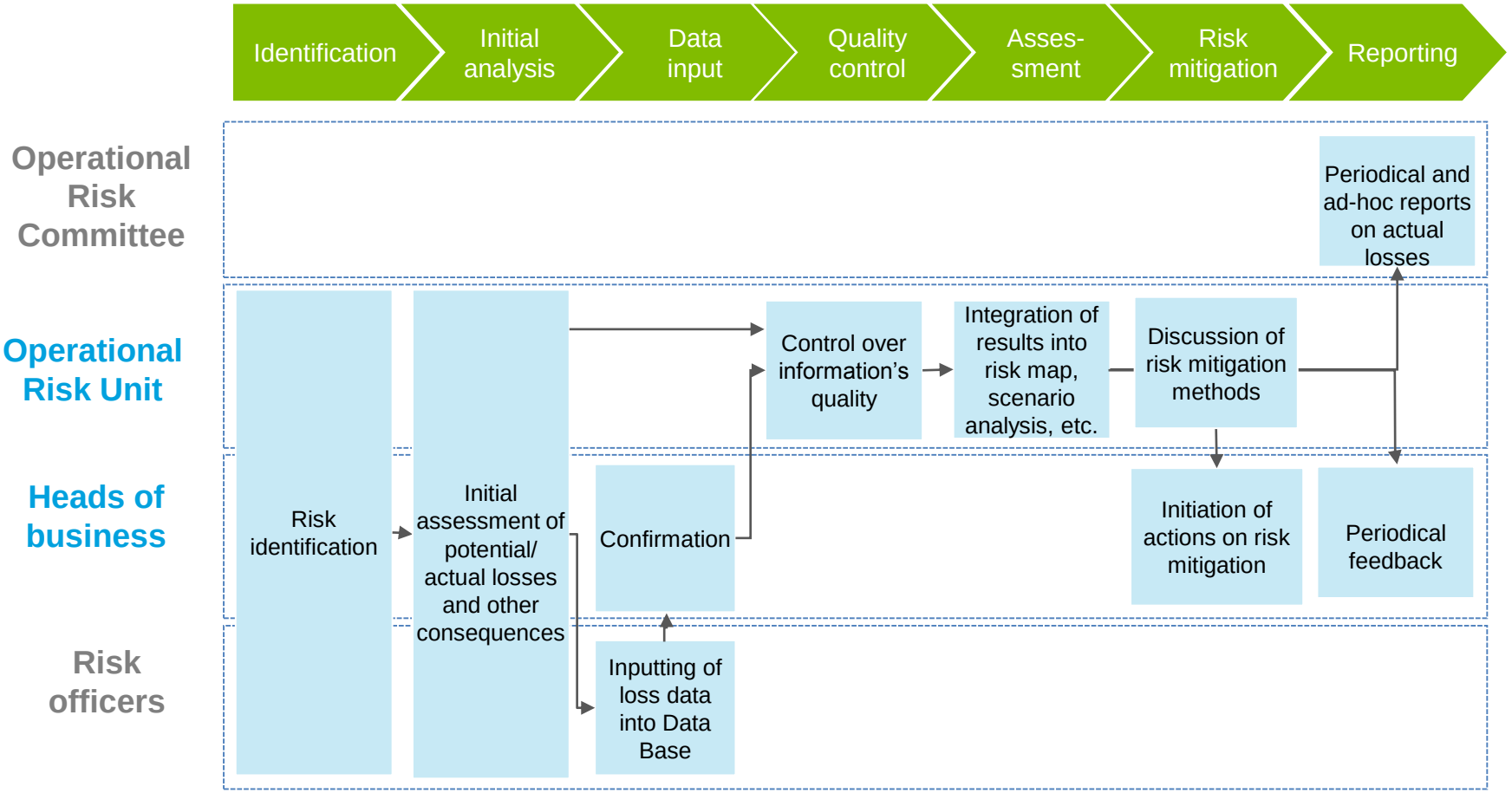
Head of business unit is responsible for control of timely loss reporting process and development of mitigation actions

Operational risk report must be drawn up detailed that its content was clear to employees that are not directly involved in the business process

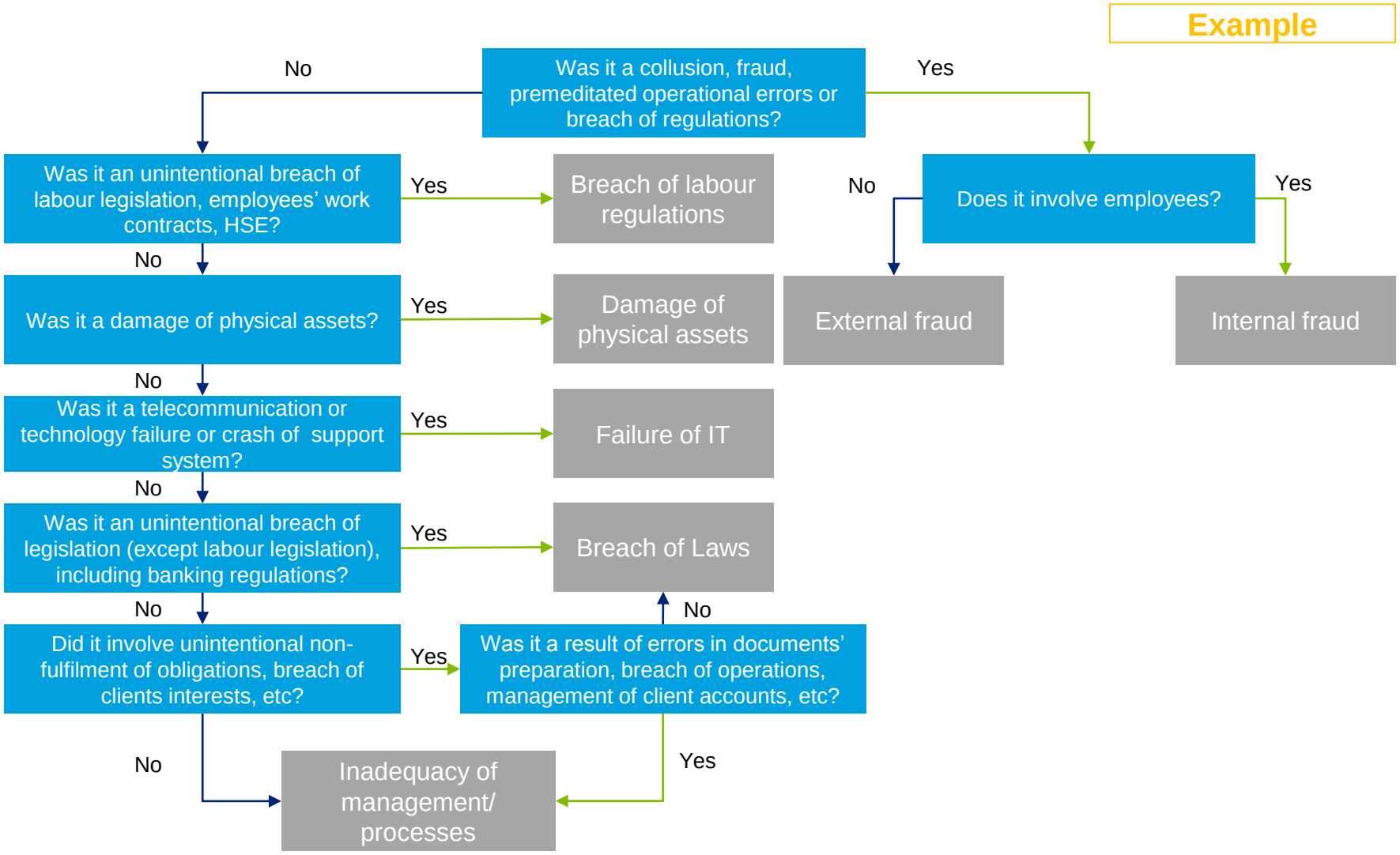
Operational risk contact person is responsible for completeness of operational risk reports of his/her unit

The purpose of reporting - not to shift the responsibility for mitigation of identified risks to operational risk unit, but to establish an effective operational risk management process

Process of internal loss collection



Operational risk classification algorithm



Typical mistakes during reporting of operational risk events

Common error	Consequence
Providing incomplete information on the event	Additional time in the investigation and clarification of details

Each report should include following information:

1. What is the reason for risk event?
2. What actions have been taken to minimize the negative effects?
3. **Which actions will be taken to prevent the recurrence of risk event?**
4. How the event has been identified, how regular are these checks?
5. What are the actual and potential consequences? In the report it is important to clarify what the consequences were realized, and what are the potential consequences

Collection of operational risk events form centralized units, sources of information

Data on cases of violations of information security

from IT-security department

Accounting information

from accounting and financial department

IT fraud cases

from IT-security department

Data on claims of supervisory authorities

from the unit responsible for the collection and coordination of supervisory authorities claim

Data on IT failures and breaches

from the division responsible for legal support activities

Data on IT failures and breaches

from the unit responsible for information technology support activities

Data on the problem credits exposure (default cases)

from the unit responsible for problem exposure handling