The scope of the risk management process needs to be defined to ensure that all relevant processes are taken into account in the risk assessment. In addition, the boundaries need to be identified. Information about the organization should be collected to determine the environment it operates in and its relevance to the risk management process.

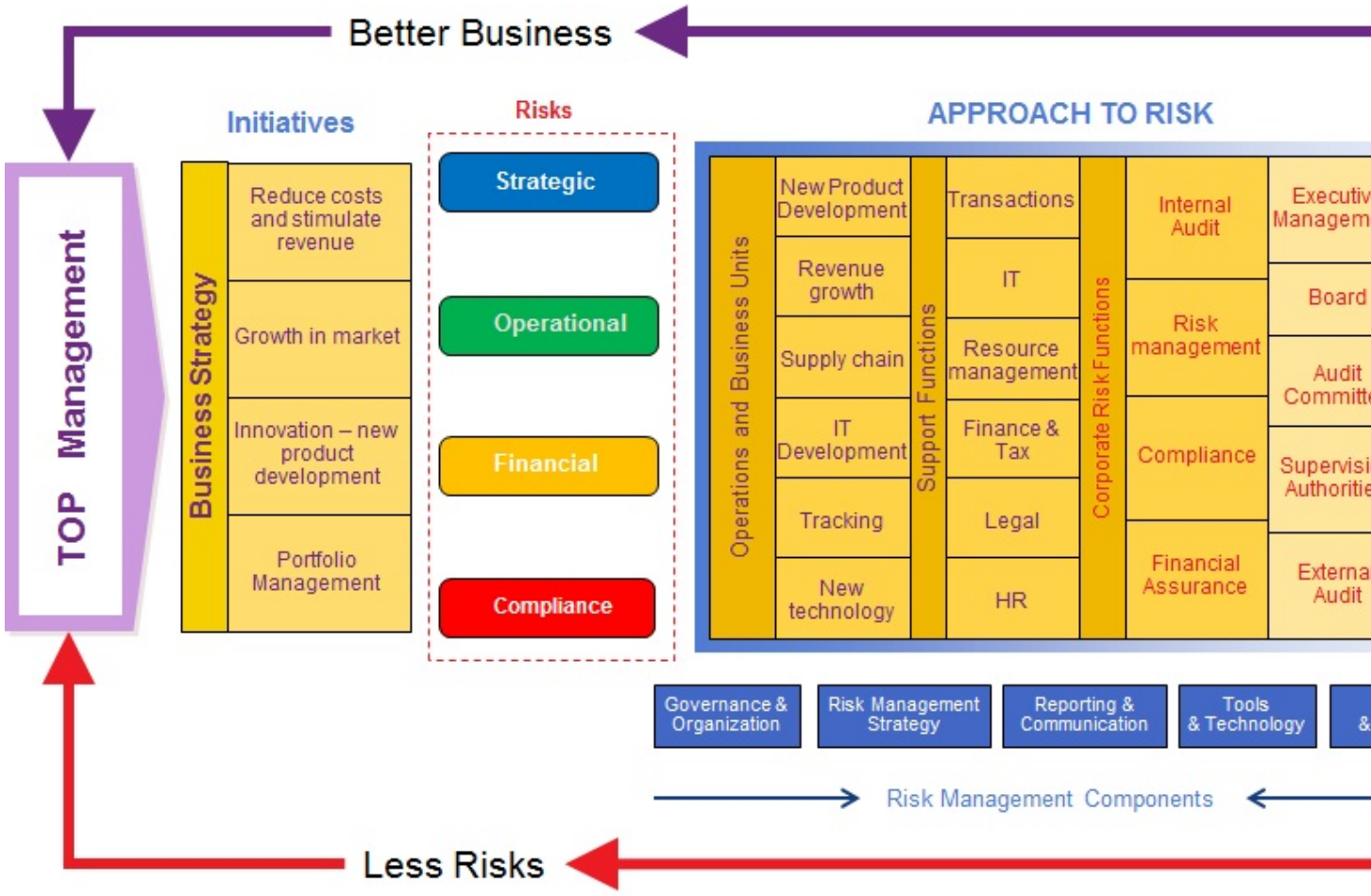
In this process, the following area need to be addressed:

- The organization's strategic business objectives, strategies and policies;
- Business processes;
- The organization's functions and structure (including IT);
- Legal, regulatory and contractual requirements applicable to the organization;
- The organization's policies;
- The organization's overall approach to risk management;
- Physical and information assets;
- Locations of the organization and their geographical characteristics;
- Constraints affecting the organization;
- Expectation of stakeholders;
- Socio-cultural environment;
- Interfaces (i.e. information exchange with the environment and B2B partners);
- GRC - Governance, Risk and Compliance optimized function;
- Data privacy and protection risks;
- General / Industriy compliance regulations - PCI DSS, SOX, Basel II, GDPR - EU General Data Protection Regulation, ASF Norm 6, NBR/Transfond, MCSI, ISO 37001:2016 - Anti-bribery management systems, Pharma regulations, ...
- DORA - The Digital Operational Resilience Act is a regulation (no. 2022/2554) adopted by the European Union in December 2022 to govern the cybersecurity of financial entities, such as banks and credit institutions.

Governance and Responsibilities

- Which functions are responsible for assessing and responding to risks in the organisation?
- What are their reporting lines?
- What are their relative responsibilities?
- To what extent do the different functions involved in risk identification/management work to a common agenda?
- To what extent do the different functions connect their risk related activities?

Our Approach To Risk



Risk Advisory and Compliance best practices

The six main best practices for risk management & compliance should be followed:

1. Clear ownership of risk & compliance within the company;
2. Appropriate internal mechanisms to discuss/communicate risk & compliance issues;
3. Formal process to identify risks specifically relating to corporate objectives and compliance requirements;

4. Active board-level involvement in managing risk and compliance;
5. Specific policy governing communications on risk & compliance with major investors and other external stakeholders;
6. Effective **GRC** - Governance, Risk and Compliance function.

Some of compliance rules we provide advisory / audit services

1. Rule **ASF no. 4/2018** on the management of operational risks generated by information systems used by authorized / licensed / registered entities, regulated and / or supervised by the Financial Supervisory Authority;
2. Regulamentul **BNR nr.3/2018** privind monitorizarea infrastructurilor pieţei financiare şi a instrumentelor de plată din **16.aug.2018** ;
3. **EBA GUIDELINES** ON BANKING INTERNAL GOVERNANCE - 21/03/2018
4. **PCI - DSS**, Requirements and Security Assessment Procedures - version 3.2.1 / May 2018
5. **POLITICA DE SECURITATE** A INFORMAŢIEI APLICABILĂ SISTEMELOR DE PLĂŢI ŞI SISTEMELOR DE DECONTARE OPERATE DE BANCA NAŢIONALĂ A ROMÂNIEI - Versiunea 2.0 din **13 martie 2018**;
6. CERINȚE PENTRU CERTIFICAREA TEHNICĂ ŞI ADMINISTRAREA PARTICIPANȚILOR ÎN SISTEMUL **SENT** AL TRANSFOND versiunea 01 revizia 00 / **10. 12.2018**

7. CERINTE pentru certificarea tehnica a participantilor la sistemele **ReGIS-Safir** din **13 martie 2017**
;

8. **NIS DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 ;**
9. **GDPR** - REGULATION (EU) **2016/679** of **27 April 2016** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
10. **PSD 2** - Payment services Directive (EU) 2015/2366;
11. **EBA GUIDELINES** ON THE SECURITY OF INTERNET PAYMENTS - 19 December 2014;
12. The Digital Operational Resilience Act (DORA) is a regulation (no. 2022/2554) adopted by the European Union in December 2022 to govern the cybersecurity of financial entities, such as banks and credit institutions.