Deloitte.

Business risk consulting
Integrated governance, risk and compliance

Table of contents

Why governance, risk and compliance	3
Governance, risk and compliance – in harmony	4
Overview and key iGRC challenges	5
iGRC	6
Our experience indicates that...	7
The Risk Intelligent Enterprise™ framework	10
Assessing iGRC capabilities	11
A Maturity Model for risk intelligence	12
High-level risk intelligence accelerators	13
Risk intelligence map	14

Why governance, risk and compliance

- Both private and public sector executives are under pressure today to increase their understanding of Governance, Risk and Compliance (iGRC) issues—and their ability to respond to them.
- They are expected to deliver against a range of key performance indicators (KPIs), including profitability, customer satisfaction, revenue growth, market share, market value and brand awareness. At the same time they face escalating demands for information from outside stakeholders, regulatory bodies, analysts and the media.
- To help keep tabs on complexity, keep regulators at bay, keep stakeholders informed and continue to deliver performance against KPIs, a well-planned and responsive iGRC structure is crucial.
- If not properly established, executives will remain in reactive mode, continually distracted by the latest crisis and unable to take a proactive role in shaping risk management in order to increase the value of the organisation.

> "If you embrace iGRC wholeheartedly and take an integrated, enterprise approach, it's going to cost less than a collection of fragmented processes"

- Instead of paying lip service, in response to external pressures, the internal organisation must adapt to apply best business principles to manage risk. When this is achieved, expenditure falls too. *"If you embrace iGRC wholeheartedly and take an integrated, enterprise approach, it's going to cost less than a collection of fragmented processes,"* says Lee Dittmar, Deloitte's global leader for governance, risk and compliance consulting.

Governance, risk and compliance – in harmony

iGRC is how the organisation is governed to optimise results, by managing risks and seizing opportunities, while staying compliant.

Compliance

The effect of uncertainty on business objectives; risk management is the coordinated activities to direct and control an organisation to recognise opportunities while managing negative events

Governance

The culture, policies, processes, laws, and institutions that define the structure by which organisations are directed and managed

Risk management

Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements

Overview and key iGRC challenges

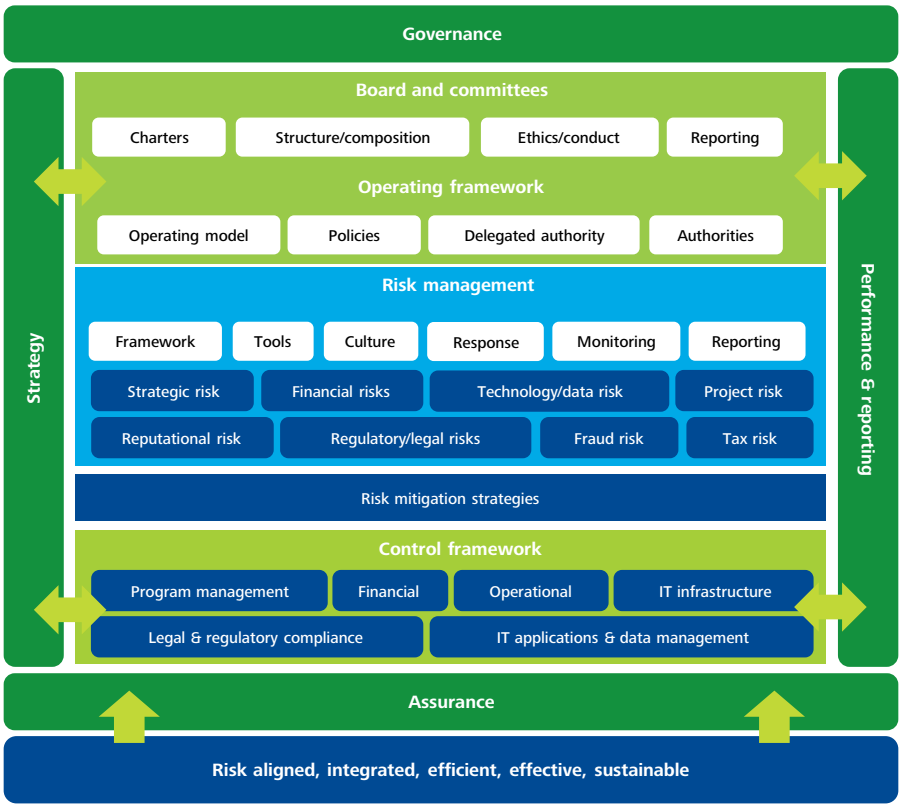
iGRC is more than a clever definition. It brings all of the control strands together providing an integrated repository in which (i) enterprise risks, can be documented, quantified, prioritised and managed (ii) governance procedures, such as, board and management activities, oversight structures, strategy setting, performance monitoring and reporting can be determined and (iii) that there is a documented controls environment for the evaluation, monitoring, and reporting of the controls that facilitate compliance with regulatory requirements as well as corporate policies and procedures.

Governance

- Assessing board effectiveness
- Assessing governance structure and effectiveness
- Regulatory overburden
- Governance over decision making
- Integrated risk and governance
- Effectiveness, delegation and control within the organisation and across the value chain
- King 3 compliance

Risk management

- Defining risk appetite
- Improving the alignment between risk and management decision making on both operational and strategic level
- Linking risk and remuneration
- Enhancing risk information
- Scenario planning
- Defining and establishing a risk culture
- Defining a relevant and complete risk universe



Control

- Identifying and monitoring critical controls
- Establishing a controls culture
- Establishing a balance between cost and control

Assurance

- Multiple assurance providers and assurance mapping
- Balance between risk based auditing and assurance over core business processes
- Multiple assurance providers and assurance mapping
- Balance between risk based auditing and assurance over core business processes

iGRC

iGRC is about integrating and aligning an organisations approach to managing risk within the context of an overall governance model, through appropriate control mechanisms, to support and achieve its strategic objectives

iGRC achieves the following results:

Value creation and preservation and assurance

Protection and creation of company value through identification and management of risks and future opportunities.

Simplify standardisation, centralisation and taking out complexity

iGRC integrates, streamlines and leverages common Governance, Risk Management and Compliance processes and increases knowledge sharing and coordination across the organisation's functions in order to optimise existing efficiencies and effectiveness.

Stakeholder confidence

iGRC assists the Board and management by enabling compliance with Corporate Governance standards.

Reduce costs on sustainable basis

Lowering cost on a sustainable basis by cutting and optimising spend on compliance activities through efficient and effective utilisation of resources, by applying the – assess once, test once, satisfy many principles inherent in integration.

Our experience indicates that...

Organisations that are rethinking their existing risk management approach and assessing their risk management capabilities are better positioned to manage the current economic difficulties.

Challenges being faced	How Deloitte can help?
Governance • Assessing board effectiveness • Assessing governance structure and effectiveness. • Regulatory overburden • Integrated risk and governance • Effective delegation and control within the organisation and across the value chain • Consequences of 'Apply or explain' of King III Report on Corporate Governance • Understanding and implementation of the Code for Responsible Investment in South Africa (CRISA) • Roles and responsibilities of Directors	• Identify, implement and advise on governance compliance requirements (King III) • Assessing governance structure (e.g. clarity over roles and responsibilities) • Define governance framework and minimum standards for subsidiaries, operating companies and business partners (e.g. Joint Ventures) • Communication of governance throughout the organisation (e.g. assisting design and implementation of policy framework, identifying key decisions and aligning delegated authority and defining key roles, responsibility and accountability) • CRISA assessments/training and implementations • Board induction and orientation • Continuing Board development and learning
Risk • Improving alignment between risk and management decision making on both operational and strategic level • Defining risk appetite • Linking risk and remuneration • Intelligent risk reporting • Scenario planning • Defining and establishing a risk culture in order to implement risk framework (obtain buy in and ownership of risk management processes) • Defining a relevant and complete risk universe	• Assess, Develop, Implement and Monitor Framework and Policy for management of risk that is aligned to the business strategy and is consistent with business risk appetite and culture. Assist organisations in becoming Risk Intelligent (Risk Governance, Risk Infrastructure and Risk Ownership) • Facilitate definition and implementation of risk appetite framework and metrics • Developing Key Risk Indicators and linking them to the performance measures • Support identification of key risks (strategic, process and Programme risks) using Risk Intelligence Maps, scenario identification and analysis and Risk Analytics • Quantification of risks to determine the Total Cost Of Risk(TCOR)™ • Selection and development of risk management tools and applications • Assessment of the risk culture and defining common risk management processes

Challenges being faced

Controls/value-based compliance

- Identifying and monitoring critical controls as well as establishing controls culture
- Identifying and interpreting emerging legislation, trends impacting ones business
- Alignment with the culture change towards compliance maturity
- Developing and implementing compliance frameworks e.g. Anti-bribery and corruption control

How Deloitte can help?

- Ensure control environment is compliant, effective, efficient and sustainable
- Understand and document key business processes
- Designing and implementing controls to support your compliance framework
- Regulatory compliance (legal universe, gap analysis and control assessments)
- Compliance risk management (compliance maturity assessment and gap analysis) and (compliance framework i.e. manual policies and procedures; monitoring and reporting tools and training)

Assurance

- Multiple assurance providers and assurance mapping
- Balance between risk based auditing and assurance over core business finances
- Multifaceted role of auditors
- Auditing control culture and behaviours
- Use of technology throughout the assurance cycle
- Providing assurance over the extended enterprise e.g. contracts/relationships
- Stakeholder expectations

- Assurance mapping – identifying key risks/processes and assurance providers. Combined assurance
- Assist management in developing assurance processes (e.g. controls self assessment)
- Provision of cost effective assurance – internal audit, CRC, CR assurance, ABC etc.
- Provision deep subject matter specialists (e.g. Treasury, Tax,) – genuine risk based auditing
- Use of technology - data interrogation
- Assurance reporting (e.g. audit committee reporting and external)
- Internal audit effectiveness review – assessment of current internal audit practice vs. good practice
- Helping to articulate the value of assurance
- Assurance of risk variation and tolerance which includes residual risks

Challenges being faced

Project Risk

- Weaknesses in the framework to manage your project risks
- Lack of adequate project controls and processes
- Failure of project management professionals to deliver on projects
- Systems projects finished behind schedule, over budget or failing to meet objectives

Sustainability

- Reporting requirements
- Leadership buy-in, accountability, roles and responsibilities
- Sustainability strategy integration and alignment
- Stakeholder inclusiveness
- Governance
- Sustainability assurance readiness
- Data quality
- Skills
- Forward looking information
- Systems and technology

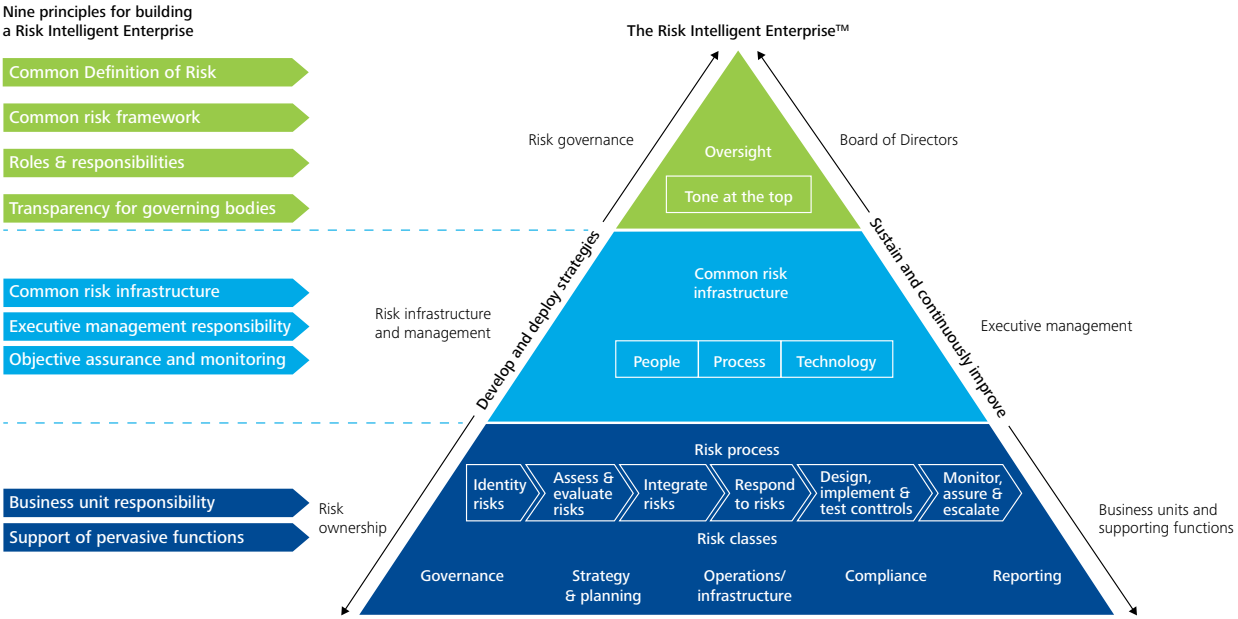
How Deloitte can help?

- Project risk services typically begin with a project risk assessment
- Project audit services provide an independent evaluation and verification of key aspects of the project management and lifecycles controls, with an emphasis on risk management assessment
- Project advisory services -evaluate program or project management office controls providing the right balance of coaching, facilitating and training services from both a project and program office perspective
- Point-in-time risk assessments and project oversight and proactive risk monitoring

- Integrated reporting gap analysis
- Strategy analysis through a sustainability lens using the Sustainability Enterprise Value Map (SEVM) tool
- Sustainability risk and opportunity management
- Sustainability policy and procedure review and/or design
- Sustainability training
- Sustainability culture assessment
- Stakeholder engagement management
- Data analysis and scenario building
- Sustainability due diligence
- Sustainability Assurance
- Internal audit support
- SHE legal compliance audits
- Environmental liability reviews

The Risk Intelligent Enterprise™ framework

The Risk Intelligent Enterprise approach offers a practical framework, or roadmap, for enabling directors and management to focus simultaneously on value protection and value creation. Deloitte's framework and insights are based on Nine fundamental principles of a Risk Intelligence program.



Assessing iGRC capabilities

Inadequacies in risk management and risk oversight continue to be cited by the marketplace as principal contributors to the current economic crises. With today's heightened awareness of risk in a dynamic environment, organisations are rethinking their existing risk management approach and assessing their risk management capabilities.

The concept of effectively and efficiently managing risks to both existing assets and for future growth, which we call Risk Intelligence, is at the core of our approach to assisting organisations with their risk management programs. Simply put, companies create value by taking risks and lose value by failing to manage them. A Risk Intelligent Enterprise™ recognises this dual nature of risk and devotes sufficient leadership both to risk-taking for reward and to the protection of existing assets. Identifying the organisation's top of mind risks can help executives improve their ability to understand, prevent, quickly detect, correct, escalate, and manage risk issues in an efficient and cost effective manner.

Deloitte uses an accelerated approach to help organisations assess their capabilities to manage risks and also to identify and assess risks in the organisation. By following this approach, organisations will be better positioned to both mitigate and manage their risks. This Risk Intelligence Accelerator approach comprises a two-step process to efficiently address client needs. Either of these steps can be performed independently, if needed.

Assess risk management capabilities using the Risk Intelligent Diagnostic and Maturity Model.

Assess risk management capabilities using the Risk Intelligent Diagnostic and Maturity Model

Principles for building a Risk Intelligent Entreprise	Primary owner	Responsability	Key duty	1. Initial	2. Fragmented	3. Top-down	4. Integrated	5. Risk intelligent
Key roles, responsibilities and authorities management are clearly delineated within the organisation	Board of Directors	Risk governance	Discharge risk management responsibility for oversight	The Board has not set the tone for managing risks and culture of risk awareness does not exist in the enterprise	The Board sets the tone for managing risks, but a culture of awareness exists in silos	The Board sets the tone for managing risks and demonstrates a culture of risk awareness, but it has not been embraced broadly	The Board sets the tone for managing risks and established a culture of risk awareness which is widely adopted and understood throughout the enterprise	The Board sustains and strengthens the risk intelligent tone and promotes a risk intelligent culture

Before investing in iGRC improvement initiatives, organisations need to understand their current capabilities.

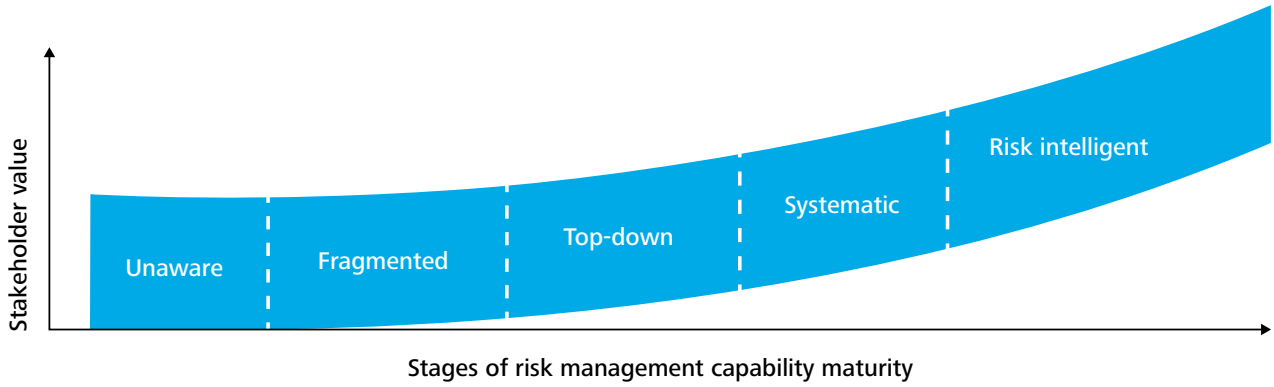
Deloitte has the Risk Intelligent Diagnostic and Maturity Model, which is based on fundamental principles for building a Risk Intelligent Enterprise™.

The tool is used with boards, executives and risk owners across the organisation to help:

- Gain insight into their current risk management capabilities, benchmark them against leading risk management practices and determine whether they have the capabilities to manage risks intelligently
- Identify opportunities to advance their level of risk management on the Risk Intelligent Maturity Model
- Assist with the development of a roadmap to improve risk management practices

A Maturity Model for risk intelligence

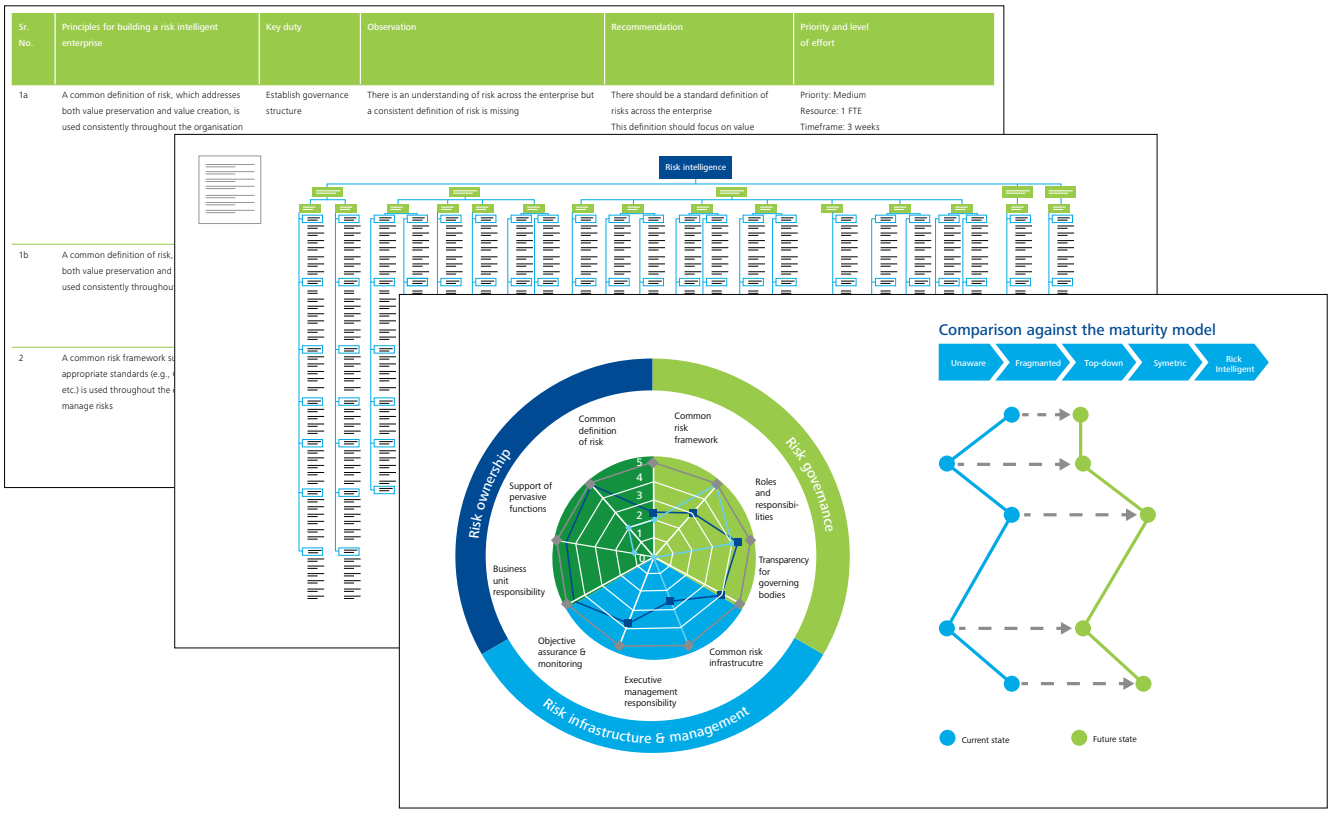
Deloitte's risk intelligence Maturity Model has been built based on our nine principles of a risk intelligence enterprise. Below is an illustrative example of our Maturity Model.



Stages of risk management capability maturity

Unaware	Fragmented	Top-Down	Systematic	Risk intelligent
• Depends primarily on individual heroics, capabilities, and verbal wisdom	• Independent risk management activities • Limited focus on the linkage between risks • Limited alignment of risk to strategies • Disparate monitoring & reporting functions	• Common framework, program statement, policy • Routine risk assessments • Communication of top strategic risks to the board • Executive/Steering committee • Knowledge sharing across risk functions • Awareness activities • Formal risk consulting • Dedicated team	• Coordinated risk management activities across silos • Risk appetite is fully defined • Enterprise-wide risk monitoring, measuring, and reporting • Technology implementation • Contingency plans and escalation procedures • Risk management training	• Embedded in strategic planning, capital allocation, product development, etc. • Early warning risk indicators • Linkage to performance measurement/ incentives • Risk modeling/ scenarios • Favorable benchmarking

High-level risk intelligence accelerators



Risk intelligence map

Governance, risk management and compliance

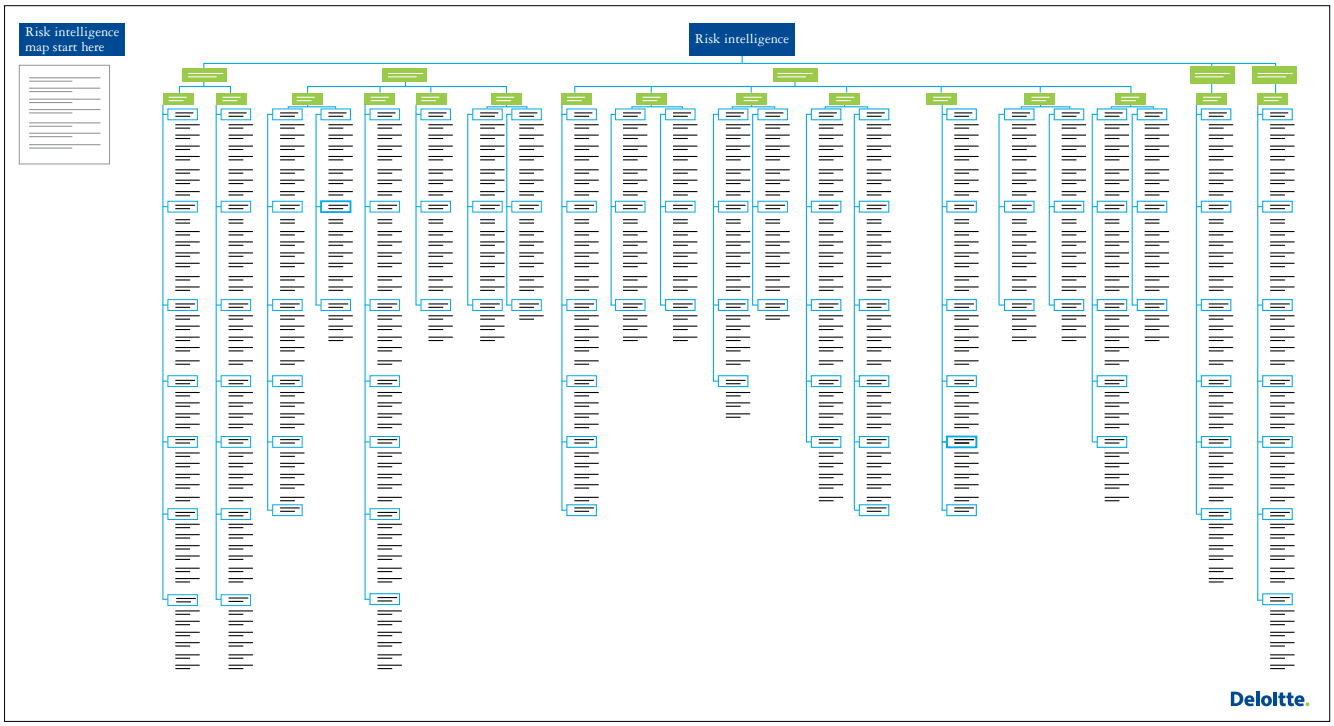
Governance

- Inadequate management oversight of cloud adoption
- Failure to evaluate and monitor usage of cloud

Risk management

- Inadequate analysis of incremental risks introduced by cloud
- Lack of independent assessment of cloud solution
- Insufficient expertise in auditing cloud environment

Compliance



Contacts

Business Risk

Laurent Berliner
Partner - Business Risk Leader
+352 451 452 328
lberliner@deloitte.lu

Mathieu Brizard
Senior Manager - Governance, Risk & Compliance
+352 451 453 096
mbrizard@deloitte.lu

Jean-Philippe Peters
Directeur - Business Risk
+352 451 452 276
jppeters@deloitte.lu

Jérôme Sosnowski
Directeur - Business Risk
+352 451 454 353
jsosnowski@deloitte.lu

Advisory & Consulting

Joël Vanoverschelde
Partner - Technology & Enterprise Application Leader
+352 451 452 850
jvanoverschelde@deloitte.lu

Thierry Flamand
Partner - Actuarial & Insurance Solutions
+352 451 454 920
tflamand@deloitte.lu

Tax

Raymond Krawczykowski
Partner - Tax Leader
+352 451 452 500
rkrawczykowski@deloitte.lu

Audit

Sophie Mitchell
Partner - Audit Leader
+352 451 452 481
somitchell@deloitte.lu

Stéphane Césari
Partner - Audit
+352 451 452 487
scesari@deloitte.lu

Martin Flaunet
Partner - Audit
+352 451 452 334
mflaunet@deloitte.lu

Justin Griffiths
Partner - Audit
+352 451 452 692
jugriffiths@deloitte.lu

Georges Kioes
Partner - Audit
+352 451 452 249
gkioes@deloitte.lu

Johnny Yip Lan Yan
Partner - Audit
+352 451 452 489
jyiplanyan@deloitte.lu

Deloitte Luxembourg
560 rue de Neudorf
L-2220 Neudorf
Grand Duchy of Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu