



Definition of the IT internal audit Strategic plan using a risk-based approach

The ever-increasing complexity of information and communication technology (ICT) and security risks presents new challenges for an organisation's internal controls function, including Internal Audit (IA).

Recent regulatory developments in the financial sector such as the CSSF Circular 20/750 implementing EBA Guidelines on ICT Security and Risk Management emphasize the importance of the internal audit function to provide independent assurance on the control environment effectiveness to the management body.

In this context, effective information technology internal auditing requires thorough planning coupled with nimble responsiveness to quickly changing risks. Following a risk-based approach, an organisation's IA plays a critical role in helping review and provide independent assurance that ICT and security-related activities are compliant with organisation's policies, procedures, and external requirements.

Supervisory authorities (in Luxembourg and Europe) monitor closely how organisations cover their ICT risks when defining their multiannual internal audit plan using a risk-based approach.

How Deloitte can help?

With the help of Deloitte's ICT security and risk expertise and practiced methodologies, we support organisations in building and delivering a strategic multiannual IT internal audit plan that is based on a comprehensive risk assessment.

How does it work?

Deloitte supports organisations' internal audit functions in developing a risk model and IT internal audit plan in alignment with (i) applicable regulatory requirements, (ii) market-leading best-practices, and (iii) complexity of organisations' ICT operating model.

We have developed a comprehensive ICT and security risk management framework that addresses a broad range of ICT and security risks. Leveraging this framework and our expertise in this field, we assist organisations with the challenge of defining a customized ICT security and risk management universe that is aligned with the organisations own context; taking into account specific risks the organisation is exposed to, the organisations' size and environment, regulatory landscape, existing operational audit plan, etc.

Careful consideration of an organisations' specific environment allows us to develop an actionable and manageable ICT and security risk universe, and related IT audit plan.

Our approach and methodology

Through analysis of organisations' environment and the development of a customized risk model and universe, Deloitte helps organisations identify the key risks that IT internal audit should further understanding and have a role in mitigating. We propose the following phased approach for the development of your organisation's IT internal audit plan requirements:

- understand the organisation environment and its IT activities
- develop the ICT and security risk universe, and assess and prioritize its risks
- Define the IT audit plan

We support organisations in building and delivering a strategic IT internal audit plan.



Contact us:

Stéphane Hurtaud
Partner
Risk Advisory
shurtaud@deloitte.lu

Onur Ozdemir
Director
Risk Advisory
oozdemir@deloitte.lu

Roland Bastin
Partner
Risk Advisory
rbastin@deloitte.lu

Laurent Berliner
Partner
Risk Advisory
lberliner@deloitte.lu

Asmaa Ouraini
Manager
Risk Advisory
aouraini@deloitte.lu

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500[®] companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.