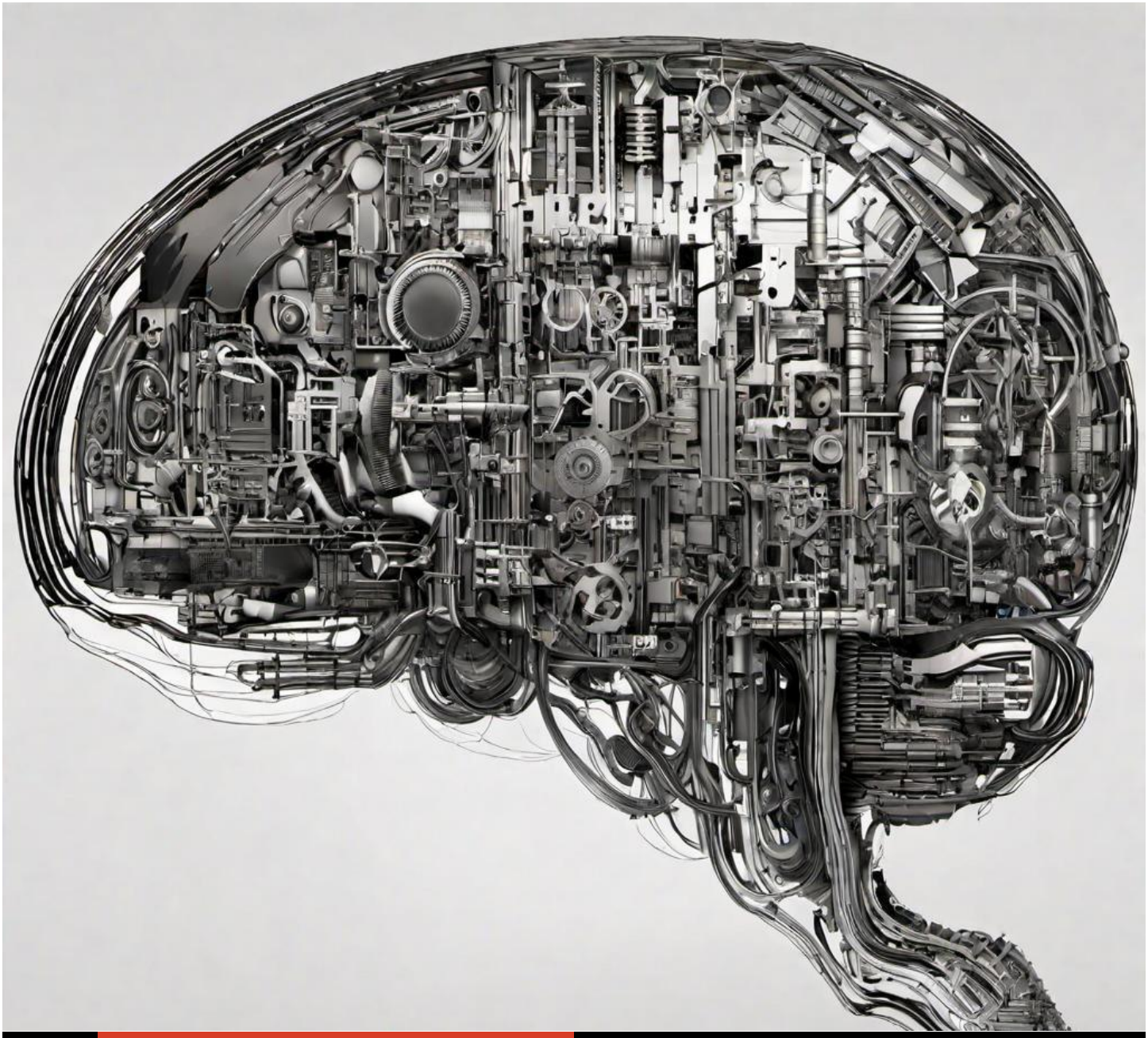


IT RISK ASSESSMENTS

CHADLY MOUKOURI NGAMI

2023

WWW.CHADLYMN.EU

chadlymoukouri@hotmail.com

IT RISK ASSESSMENTS: A PROCESS FOR YOUR CIO OR CISO.

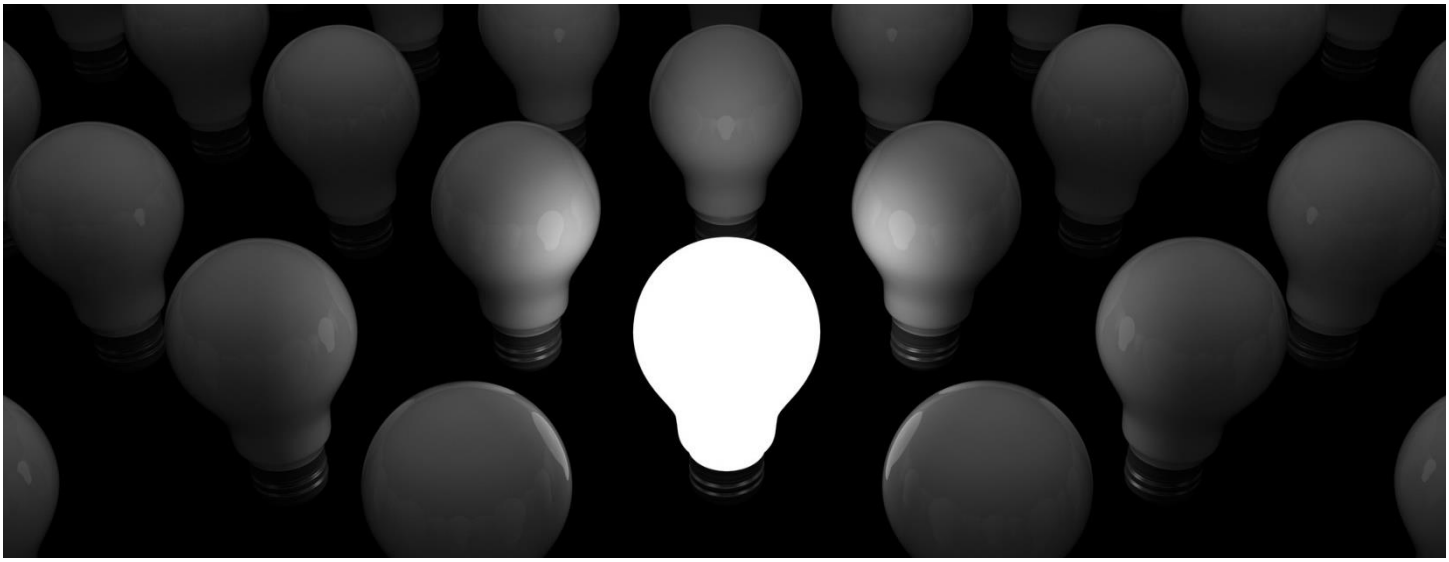
IT risk assessments prioritize critical information assets, highlight connections between cyber threats and risks, and map key controls to known threats. Compliance with regulations and adherence to frameworks is demonstrated by assessing IT risk. Finally, IT risk assessments provide leaders with a foundation for decision-making, including the establishment of security investment priorities.

Our focus is on exploring the best practices for conducting an IT risk assessment and breaking down six steps to identify and quantify risk.

How to Conduct Your Next IT Risk Assessment with Best Practices

Success is achieved through the following best practices:

Integrate industry-leading control guidance into your security risk assessment framework.
Ensure that the IT risk assessment is integrated with the operational and enterprise risk assessment programs.



Coordinate business risks with relevant threats, controls, and assets. Create a security risk tolerance that is in line with the organization's goals and objectives.
To enhance the organization's long-term security posture against real-world threats, align enterprise risk with security operations (SecOps). A criticism of traditional enterprise risk assessments is that they aren’t always as grounded in real-world threats to assets as SecOps usually is — but it doesn’t have to be this way!

A six-step approach to IT risk assessment:

Following these six key steps will help you identify and quantify residual risk — ultimately helping risk owners make informed decisions and enabling leaders to make appropriate risk management investments.

I- **Familiarize yourself with the business.** Understanding the impact of security on the organization's progress towards its business objectives, as well as considering risk management in the context of business outcomes, is part of this.

II- **Examine the impact of business.** An BIA allows stakeholders to determine the criticality and impact levels for each asset.

III- **Acknowledge the significance of data in reducing risk.** Understanding the organization's goals and objectives will determine which data is most crucial. This information can be used to classify data down to the asset level.

IV- Exa**mine data that is not regulated.** Despite the importance of regulated data, it's important to consider other information that poses risks for the business. Trade secrets are a type of data that is not typically regulated, but their loss would have significant consequences.

V- **Determine your security risk.** Take into consideration the impact and likelihood of risks on critical assets. These risks could be financial, reputational, regulatory, or other. Identify the most effective key controls for reducing these risks. Assess the strength of controls in place to manage those risks, and determine any residual risk that remains after taking existing controls into account. Develop risk treatment plans to address any risk that is beyond the leaders' risk appetite. And keep in mind, the risk is not static. The control environment can experience improvements or degradation as new assets are acquired or deprecated, and subsequent controls testing demonstrates improvement or degradation.

VI- **Contextualize risk in a financial sense.** The quantification of risk involves the loss of revenue, regulatory fines, reputational damage that depresses sales and share prices, and impaired performance of the organization.

Effective management of IT risks.

IT risk assessment focuses on critical information assets, threats, risks, and controls, while also informing security investment priorities and supporting compliance. Compliance management software supports IT risk assessments by providing the means to track performance and guide risk-based decisions, support IT risk management, monitor progress against plans, and create a meaningful basis for leaders’ investment decisions in security and compliance.