Governance, Risk & Compliance (GRC)

AEC

How Old Are Your Risks?

Do you still remember when the Heartbleed vulnerability appeared, and your organization was at risk? Today, Huawei and ZTE technologies may result in a similar risk. Both of the cases mentioned above present a risk, and therefore, an obvious question arises, i.e. how is your risk analysis dealing with this situation? Is it able to integrate the newly identified threat, so you in your tomorrow's report you could see how much higher is the risk of the infrastructure under your management being unavailable or wiretapped? No? Then your risk analysis is definitely not flexible enough.

One of our long-standing customers contacted us in connection with the Huawei technology threat campaign. Within a short period of time, the company was supposed to reflect the said threat in its risk analysis. Our customer wanted to satisfy the authorities and simultaneously, to find out whether this threat has to be dealt with as a priority when compared to other threats. First, our consultants analysed the company's current risk information management methods and incorporated the thread. Then, they focused on the process weak points, such as regular asset lists updates, missing links between the individual assets, and definition of individual user responsibilities within the risk management process. The first key finding for the customer resulted from the risk analysis output and led him to a conclusion that the current threat put in context of the whole organization is not the most serious one and that it can be solved later in time. The second finding was then our recommendation to implement an integrated GRC management system eliminating any weaknesses in the risk management process and allowing for flexible responses to the emerging risks. Over the course of six months, we deployed this new technology at the customer's and integrated the entire risk management process into it. The customer started to like the new approach to risk management so much that the company decided to extend the GRC system to become its audit and GDPR compliance tool as well.

The GRC tool has proven to be suitable not only when it comes to covering the information asset and risk management processes, but also for other activities related to the company management. Due to this tool, the company is sharing and using the information stored in it across multiple departments, updating the data regularly, and saving costs by streamlining all activities.

www.aec.cz

Governance, Risk & Compliance (GRC)

Solution Description

GRC tools for organization governance, risks and compliance are comprehensive solutions providing companies with support for increasing the level of security. Information assets database and a sophisticated information risk management process are the core of this tool with other areas of governance, such as compliance management, supplier relationship management, security vulnerability and incident management etc. built upon it.

In addition, the GRC tools come with a wide range of integration options, thus keeping the data updated and comprehensive. However, scope of our delivery never targets only the GRC tool implementation. Our first objective is to focus on process review and improvement. We realize that a quality process is the base for data transformation into valuable outputs.

Benefits of Our Solution

- We are reviewing and optimizing information security management processes.
- Implementation of the system helps to improve quality of the processed data.
- Up-to-date and interconnected data together with process automation enable timely response.
- Which means optimization of information security management costs.
- We will create a central location for storing and sharing information in your company.
- Our solution supports collaboration between individual departments.

When to start considering GRC implementation?

If your organization is subject to one of the following regulations:

- GDPR
- ISMS
- ZoKB
- PCI DSS

If you have technology or processes implemented in any of the following areas:

- Vulnerability Management System – VMS
- Security Information and Event Management – SIEM
- Identity Management System – IDM
- Configuration Management Database – CMDB
- Business Continuity Management – BCM
- Disaster Recovery Planning – DRP
- Risk management
- Internal audit

Reference

Our customers with implemented GRC tool include for example:

T-Mobile Czech Republic

Komerční banka

AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283