protiviti®
Global Business Consulting

Diving into SAP S/4HANA: Sitting down with Jocie Kasdorp with BDR Thermea

by Simon Knaapen, Senior Manager

Recently, I sat down with Jocie Kasdorp, the Group Risk and Compliance Manager at BDR Thermea Group, for an interview. BDR Thermea Group is the parent company operating internationally with brands Baxi, De Dietrich, Remeha, and more. BDR Thermea is a global player with market-leading brands in more than 100 countries. Last year, they achieved a revenue of over €2.1 billion and employ over 6,500 people.

BDR Thermea Group has an internal control framework that is guided by their code of conduct. They work with the three-lines of defense model. Jocie has been with the company for 3 years and has 25 years of experience in finance, compliance and risk management. In her current role, she is responsible for the second line function, including the content and execution of the internal control framework, including enterprise risk management and policy compliance.

At BDR Thermea Group they have reinforced the second line function with a Single Point of Contact (SPOC) Community where a single person locally is dedicated to internal controls in each market. They are close to the business and as such well positioned to understand and mitigate risks in the local businesses. Their dual reporting line into Group Risk and Compliance provides them with support and independence.

The internal control framework is also applied for the SAP S/4HANA implementation. Protiviti has been assisting with the SAP S/4HANA implementation, specifically around security access. We have set up role-based access control (RBAC), based on solid segregation of duties (SoD) principles, and SAP GRC Access Control. Jocie feels strongly that role-based access is critical to the S/4HANA control environment, and we worked together to strengthen and apply specific controls for SAP S/4HANA. This being an area of expertise for our firm, we were natural partners from the beginning.

> "There always has to be the interaction between the business, risk management and the technical consultants," said Jocie. "The business knows their processes and what needs to be done, but then there is the question: does it create an unacceptable risk? And if so, how do we avoid or mitigate that risk without disrupting the business."

BDR Thermea Group set straightforward, but not necessarily easy to achieve SAP security access goals:

- Provide users with the lowest amount of access required to be able to perform their functions.
- Segregation of duties (SoD) strongly reinforced in the system. This is achieved by setting up BDR specific SoD ruleset that was built together with Protiviti. The authorization roles were analyzed against that ruleset. Automate controls, where possible.
- Structured and consistently applied SAP security & authorization processes.

- Where risk remediation is not possible, mitigate the risks on the role and user level, documenting the control in GRC. The risk mitigation, which may be country specific is identified through collaboration between business process experts in collaboration with SAP technical experts.
- Governed emergency access control (also known as 'firefighter'), for incidental access requirements and/or blocking situations.

The plan is to rollout SAP S/4HANA globally to the entire organization, which will be done incrementally per country over the next few years. First to implement was Italy, which came with some initial growing pains, which were exacerbated by a remote go-live. This first rollout was a greenfield project, meaning the authorization concept was built from scratch. This provided flexibility but also uncertainty in the security access within the project. During the build of authorization concept, we followed the principle of streamlining the processes, in line with the blueprint for the SAP S/4HANA project.

The project in Italy went live remotely, due to covid restrictions. The core team was in The Netherlands, while the users were in Italy. The remote nature of this go-live added an extra dimension of complexity.

The philosophy is to provide users with the minimum access needed to complete their jobs supported with emergency and governed access with the so-called firefighter role. In the case of a blocking situation, users have the option to use this emergency access.

Lessons learnt from the first roll-out were applied to the subsequent roll-outs — making them much smoother from a security access perspective. BDR Thermea Group has now rolled-out to their head office in The Netherlands and France. The authorization concept initially built was reusable in the subsequent roll-outs — resulting for an efficient and successful go-live from a SAP security perspective.

Looking to the future, the risk and compliance team at BDR Thermea Group hopes to integrate their service management tool ServiceNow with SAP GRC Access Controls. By doing so, every SAP access request is scanned on critical access and/or SoD conflicts. By doing this, BDR Thermea Group prevents SoD conflicts in SAP S/4HANA before they occur. This has the added advantage of improving the user experience, with a single-entry point for all access requests. Furthermore, they are working to automate an increasing number of controls. The Protiviti Assure controls tool has been instrumental in identifying the gaps and highlighting focus areas.

According to Jocie, internal control is the responsibility of everyone within the business. SAP security access control provides a solid foundation for us to build upon.

Interested in learning more about Protiviti's SAP services? Contact Simon Knaapen at **simon.knaapen@protiviti.nl** or Niels Willeboordse at **niels.willeboordse@protiviti.nl**