Achieving DORA Compliance:
Top GRC Vendor Evaluations

Introduction to DORA and GRC

To effectively navigate the complexities of DORA compliance, organizations are increasingly turning to **Governance, Risk, and Compliance (GRC) tools**. These tools provide a comprehensive approach to managing risks, ensuring regulatory adherence, and fostering a culture of compliance within an organization.

Recognizing the importance of selecting the right partner to assist with DORA compliance, we have conducted an evaluation of **six leading vendors in the GRC space**. This evaluation aimed to identify the vendor that offers the most suitable solutions and expertise to help organizations achieve and maintain compliance with DORA. By leveraging the capabilities of these tools and partnering with the right vendor, businesses can streamline their compliance efforts, enhance operational resilience, and mitigate the risks associated with non-compliance.

Our evaluation of vendors in the GRC space for DORA compliance revealed that **different vendors scored differently in various areas critical to achieving compliance**. This highlights the importance of understanding the specific requirements and nuances of DORA and selecting a vendor that excels in the areas most relevant to your organization.

The evaluation process conducted by Deloitte assessed vendors based on several key areas of DORA compliance, including:

1. Third-Party Risk Management

2. Business Continuity Management

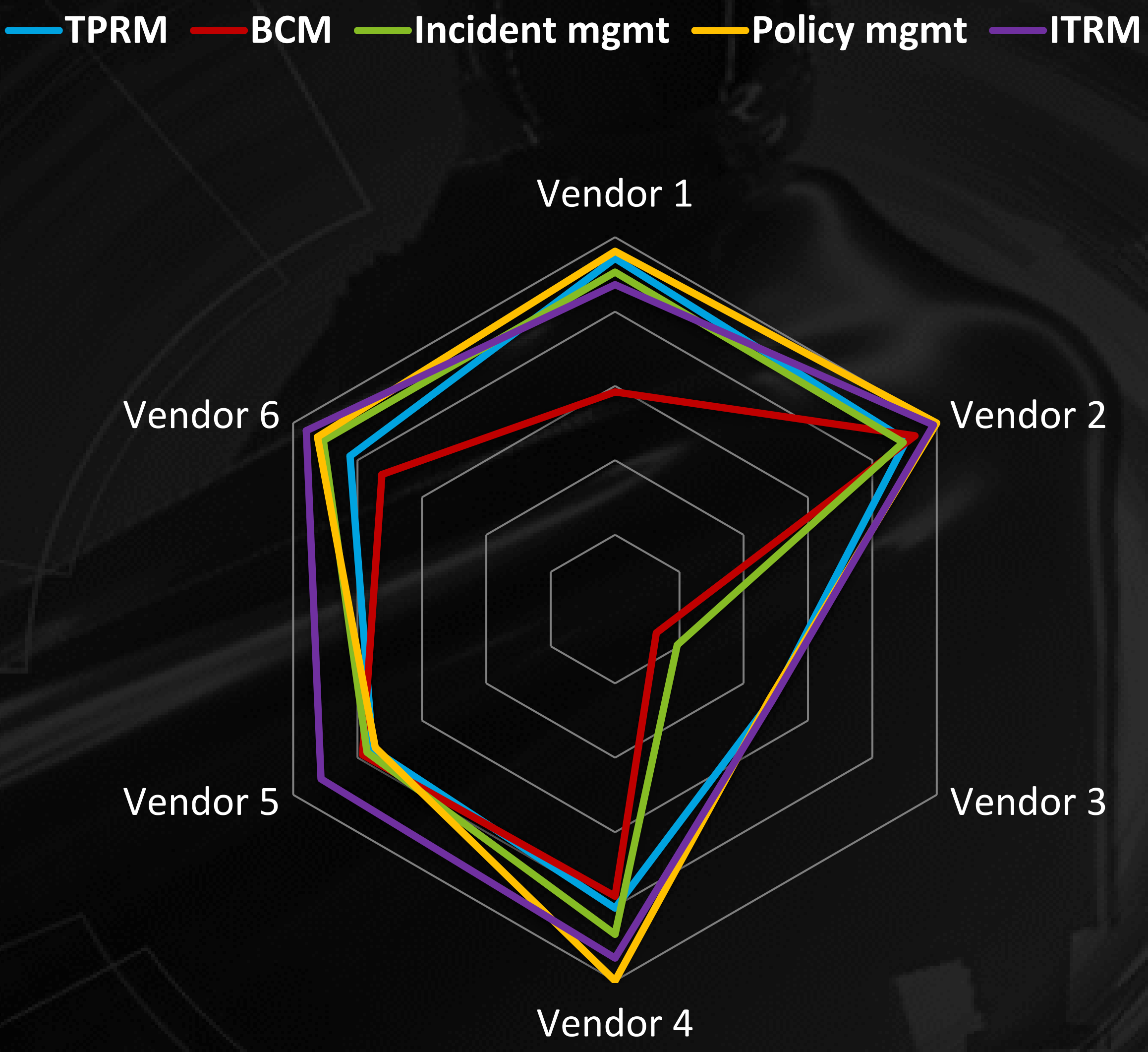
3. Incident Management

4. Policy Management

5. IT Risk Management

Introduction to DORA and GRC

Our evaluation of vendors in the GRC space for DORA compliance revealed varying performance levels across different critical areas of compliance. This underscores the necessity of understanding the specific requirements and nuances of DORA to select a vendor that excels in the areas most relevant to your organization. Below, we provide detailed data on how each vendor scored in key compliance areas, helping you make an informed decision.



It is important to note that while some vendors may excel in certain areas, they may have room for improvement in others. Therefore, organizations seeking a GRC vendor for DORA compliance should carefully evaluate their specific needs and prioritize the areas that align most closely with their requirements.

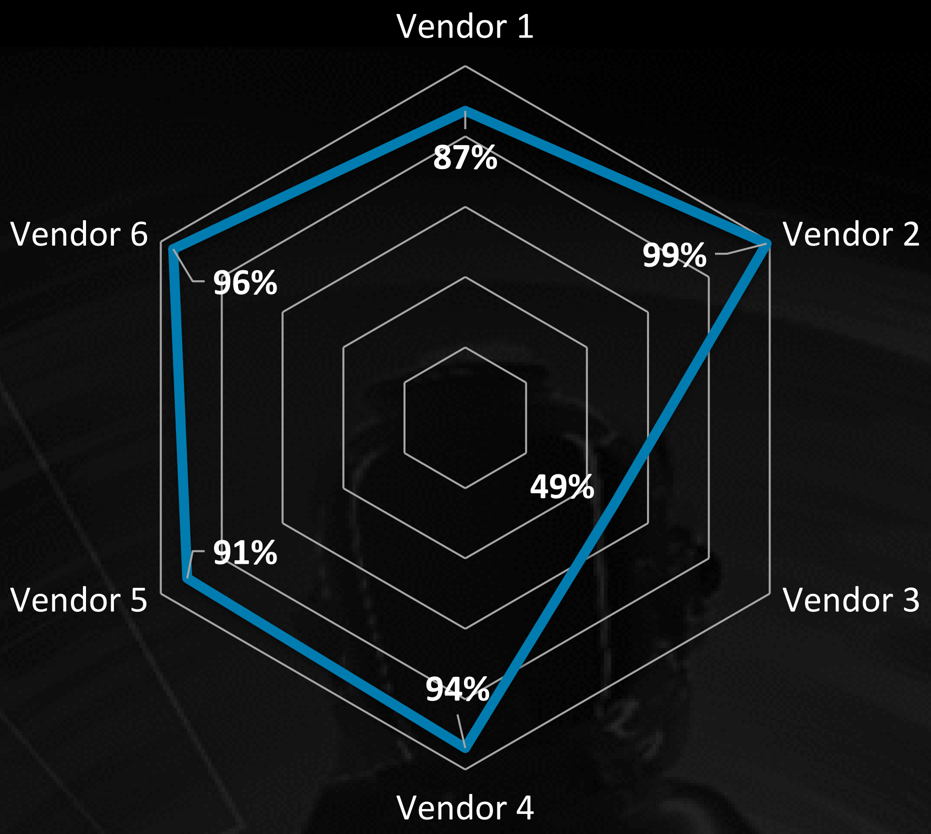
By understanding the strengths and weaknesses of different vendors in relation to the various areas of DORA compliance, organizations can make informed decisions when selecting a partner. This ensures that the chosen vendor can effectively address the specific challenges and regulatory demands posed by DORA, ultimately enhancing operational resilience and compliance.

> **"To effectively navigate the complexities of DORA compliance, organizations are increasingly turning to Governance, Risk, and Compliance (GRC) tools."**

1. Third-Party Risk Management

Within the **Third-Party Risk Management (TPRM)** area, the vendors were evaluated on their ability to effectively manage and mitigate risks associated with third-party relationships. This involved assessing their processes for due diligence, vendor selection, contract management, and ongoing monitoring to ensure compliance with DORA’s requirements.

To meet DORA compliance within TPRM, organizations must ensure that several critical requirements are addressed comprehensively. A primary focus is on detailed register containing information about the leading entity, group entities, branches, and various types of third parties. Additionally, it is imperative to identify and document all processes dependent on ICT third-party service providers. Integration for regulatory reporting is also a must, ensuring that the organization remains aligned with DORA mandates.



Visual Guide – Third-Party Risk Management

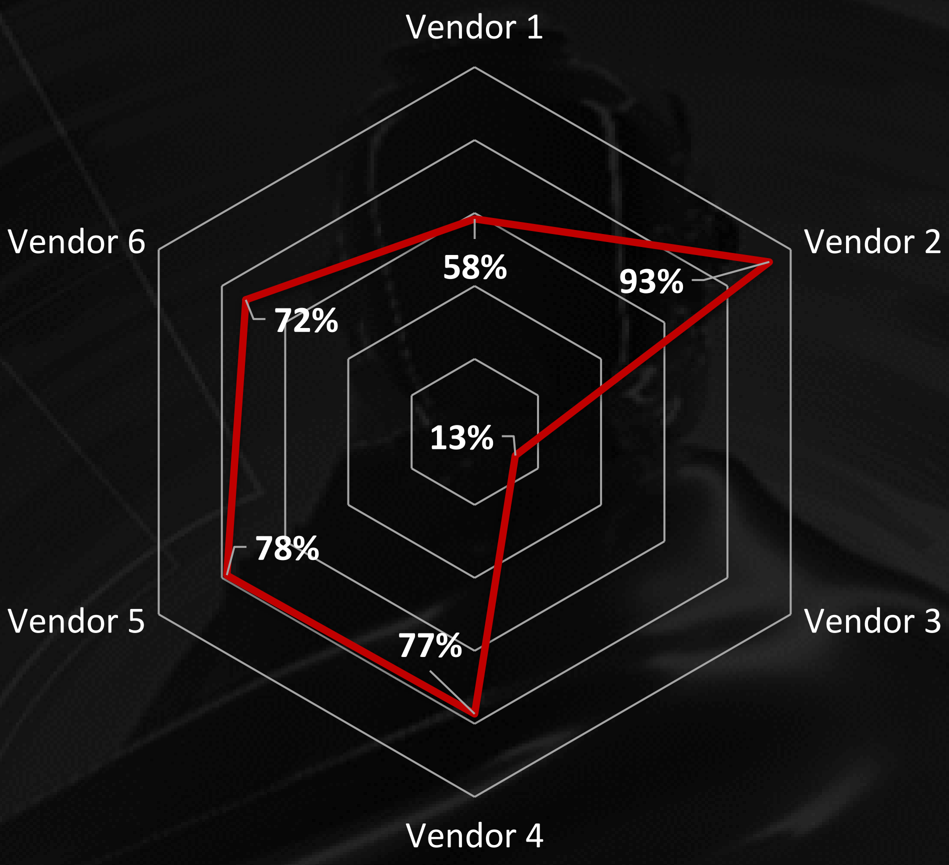
Workflows must be adjustable for third parties, particularly those supporting critical services. This flexibility is essential to accommodate the varying levels of engagement and ensure that the processes align with the organization's risk management framework.

Contracts must include comprehensive checklists covering general and specific information, as well as intra-group contractual arrangements. These checklists are crucial to ensure that all contractual obligations are thoroughly vetted and compliant with DORA requirements.

Risk management is another vital component, necessitating a framework based on ICT risk management principles. This framework helps in identifying, assessing, and mitigating risks associated with third-party engagements, thereby enhancing the organization’s overall resilience and compliance posture.

2. Business Continuity Management

The evaluation examined vendors’ capabilities in developing and implementing robust business continuity plans. This included assessing their ability to identify critical business functions, establish backup and recovery mechanisms, and ensure minimal disruption during adverse events, aligning with DORA’s resilience objectives.



Visual Guide – Business Continuity Management

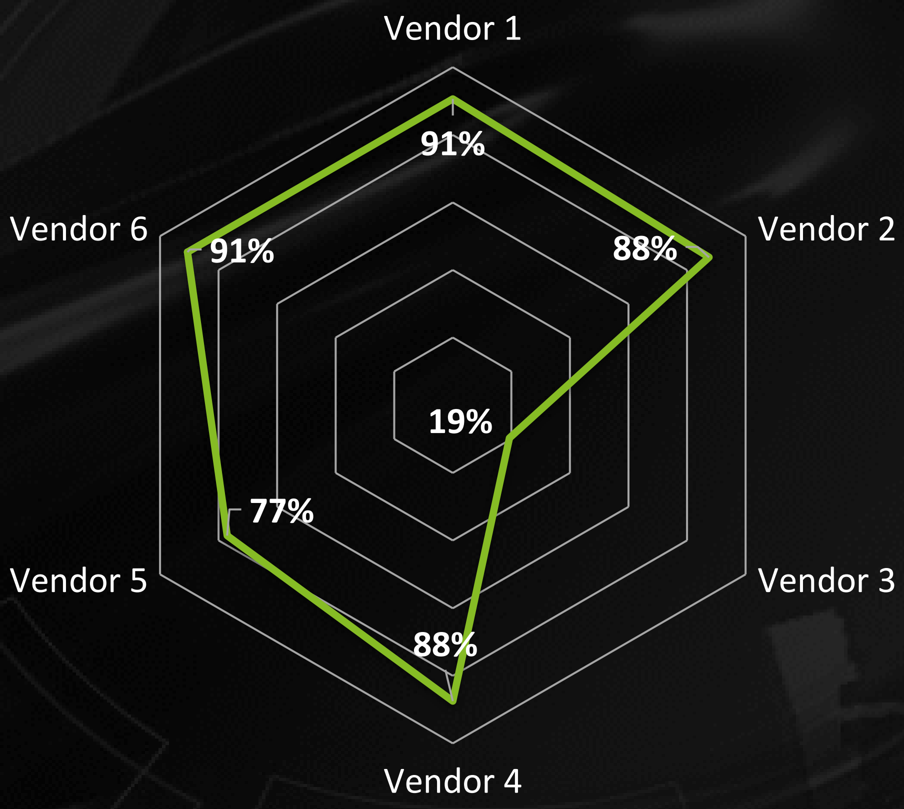
A key requirement involves the scheduling and tracking of annual testing and reviewing of response and recovery plans and Business Continuity Plans. This ensures that these plans are regularly updated and tested to maintain their effectiveness. Alongside this, testing crisis communication plans is crucial to ensure that communication during crises is efficient and effective, minimizing disruption and ensuring quick recovery.

A Business Impact Analysis (BIA) is essential for assessing the potential impacts of severe business disruptions. This helps organizations identify critical functions and determine appropriate recovery time objectives (RTO) and recovery point objectives (RPO). These calculations are vital for developing effective recovery strategies that align with business needs and DORA requirements.

While not mandatory, simulation features and functionalities for creating scenarios of cyber-attacks and switchovers, and the integration with risk assessment tools for a comprehensive analysis, enhance the robustness of an organization's preparedness. Similarly, integrating with backup systems for tracking and validating backup procedures adds an extra layer of resilience. By incorporating these essential and supportive functionalities, organizations can ensure they meet DORA compliance requirements, maintaining robust risk management and operational resilience while adhering to regulatory standards.

3. Incident Management

Vendors were evaluated on their incident management capabilities, including their ability to promptly detect, respond to, and recover from security incidents or disruptions. This involved assessing their incident reporting mechanisms and their alignment with DORA's incident management requirements.



Visual Guide – Incident Management

A comprehensive register of incidents, including all required information, is essential for effective incident management. This ensures that all incidents are documented in detail, providing a clear record for audit and review purposes.

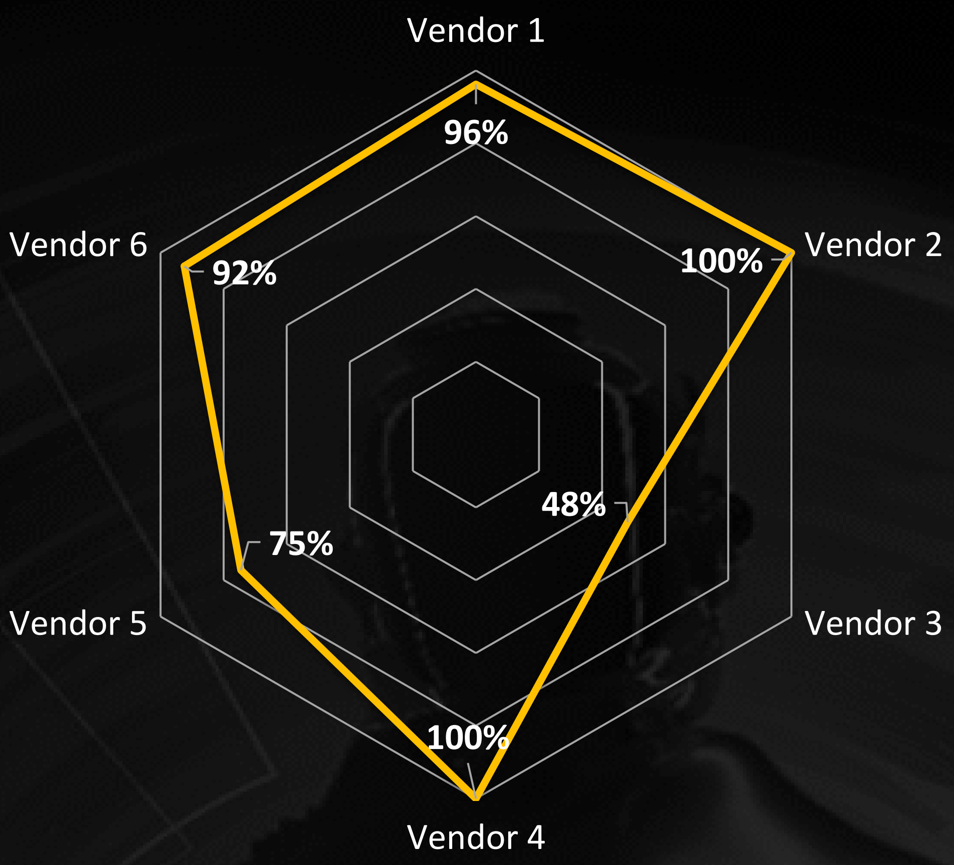
Easy navigation to related assets and services is another critical functionality. This feature allows users to quickly identify and access the resources impacted by an incident, facilitating a more efficient response and resolution process. Additionally, the impact of an incident should be suggested based on the related assets and services, although this assessment can be overwritten if necessary. This flexibility allows for more accurate incident impact analysis and response planning.

High-impact incidents require additional approval for their solutions, ensuring that these critical issues receive the appropriate level of control and oversight. This step is vital for maintaining control over significant disruptions and ensuring that they are resolved in a manner consistent with organizational priorities and regulatory requirements.

While not mandatory, several additional functionalities can enhance the robustness of the incident management system. For example, assigning workflows based on the incident impact can streamline the response process by automatically routing incidents according to their severity. Similarly, assigning solution groups based on the type of incident can ensure that the appropriate expertise is applied to resolving specific issues. Another valuable feature is allowing anyone, not just users of the tool, to report an incident. This inclusivity ensures that all potential issues are captured and addressed, even if they are identified by individuals outside of the immediate user base.

4. Policy Management

The evaluation considered vendors’ capabilities in managing policies and procedures to ensure compliance with DORA’s regulatory requirements. This included assessing their ability to establish and enforce policies, track policy adherence, and maintain an audit trail of policy changes and updates.



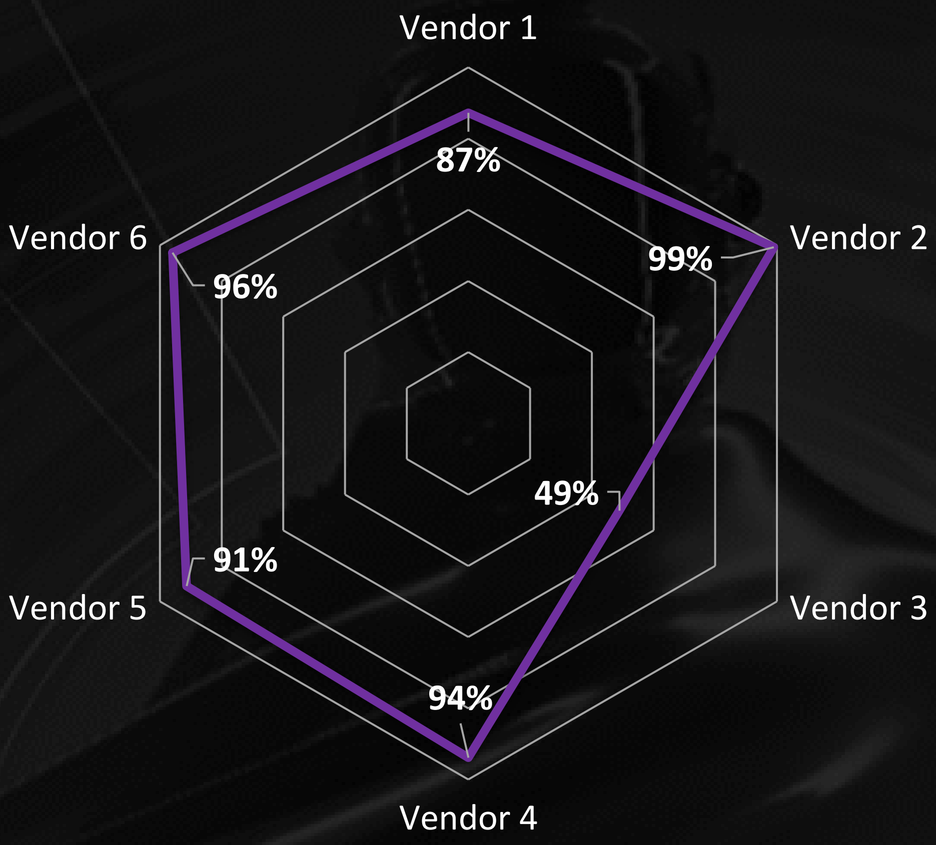
Visual Guide – Policy Management

A comprehensive register of incidents, including all required information, is essential for effective incident management. This ensures that all incidents are documented in detail, providing a clear record for audit and review purposes.

Easy navigation to related assets and services is another critical functionality. This feature allows users to quickly identify and access the resources impacted by an incident, facilitating a more efficient response and resolution process. Additionally, the impact of an incident should be suggested based on the related assets and services, although this assessment can be overwritten if necessary. This flexibility allows for more accurate incident impact analysis and response planning.

5. IT Risk Management

Vendors were evaluated on their ability to identify, assess, and manage **IT risks** in alignment with DORA’s objectives. This involved assessing their risk assessment, risk mitigation strategies, and their ability to provide comprehensive visibility into IT risks across the organization.



Visual Guide – IT Risk Management

Central to IT Risk Management compliance is the stringent documentation and mapping of all ICT-supported business functions, roles, responsibilities, and assets. A register of services and assets is essential, ensuring that all information and ICT assets, their configurations, links, and interdependencies are documented and classified. This thorough documentation aligns with DORA's mandates, ensuring critical functions and assets are meticulously mapped.

To facilitate risk management, the GRC tool must enable the identification and classification of all ICT risk sources, particularly risk exposure to and from other financial entities. It should allow risks to be associated with specific assets or services, ensuring visibility for related service owners. Additionally, the tool should support documenting accepted risks, including details on who accepted the risk, when, and why.

A comprehensive GRC tool must also provide features for monitoring legacy ICT systems to keep them up-to-date and compliant with current standards. Integration with Configuration Management Databases (CMDB) and active directories is crucial for maintaining accurate asset information. The ability to set review frequencies based on criticality and to receive notifications for upcoming reviews further enhances the system's effectiveness.

Would you like to know more? Do not hesitate to contact us.

Jakub Höll
Director
jholl@deloittece.com
+420 734 353 815

Jana Stubnova
Specialist Lead
jstubnova@deloittece.com
+420 607 988 394

Michaela Lenochova
Manager
mlenochova@deloittece.com
+420 774 636 641