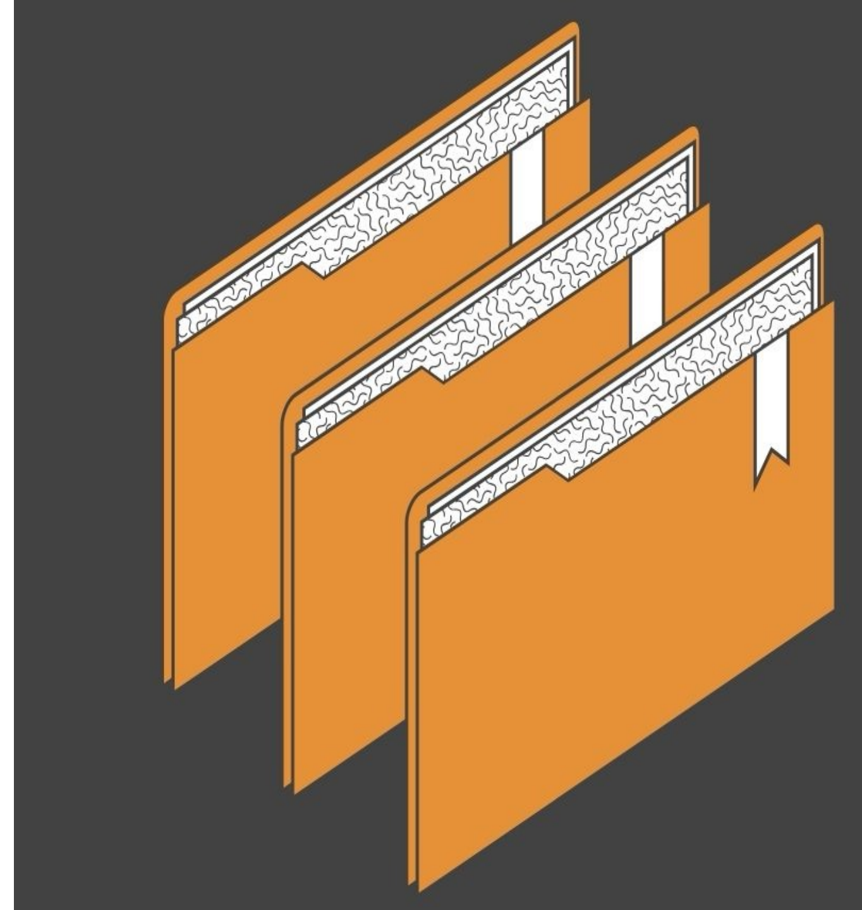


Overview

OUR CHALLENGES

- Substantial upfront costs
- Regulatory compliance risks
- Lack of a centrally managed solution

OUR GOALS

- Maintain cost effectiveness
- Enhanced regulatory compliance
- Improved risk management

Implementation Steps

- **Project Initiation:**
  - Define the project scope and objectives.
  - Assemble the project team, including key stakeholders and experts.
- **Research and Evaluation:**
  - Research various GRC solutions available in the market.
  - Evaluate potential solutions based on specific criteria.
  - Narrow down the options to a shortlist of top candidates.
- **Engage Stakeholders:**
  - Collaborate with key stakeholders, including the organization's CISO and other relevant leaders.
  - Involve different department heads and experts for diverse perspectives.
- **Comprehensive Analysis:**
  - Form a proficient team with various department representatives.
  - Conduct in-depth analysis and brainstorming sessions to assess the proposed solutions.
  - Engage in thorough debates and discussions to weigh the pros and cons.
- **Procurement:**
  - Collaborate with the Procurement department to secure licenses for selected GRC solution.
  - Navigate administrative processes and ensure legal compliance with supplier terms and conditions.
- **Deployment:**
  - Set up test and production servers.
  - Carefully configure server settings and network configurations.
  - Follow documentation and guidelines provided by the selected GRC solution for installation.
  - Integrate the servers with the organization's domain.
  - Implement security measures such as hardening and SSL certificates to ensure robust security.
- **Fine-tuning and Configuration:**
  - Configure the Eramba GRC system to optimize functionality and user experience.
  - Set up roles, permissions, and group dynamics for ease of use.
  - Integrate the PCI DSS 4.0 framework as part of the deployment.

Lessons Learned:

- **Change Management:** Implementing change management strategies to smoothen the transition process would have accelerated the adoption rate among end-users. Consider focusing on change management for similar projects in the future.
- **Communication:** Improved communication and collaboration between various stakeholders and departments is key to a successful GRC implementation. Ensure all teams are aligned and informed throughout the project.
- **Training:** Recognize the importance of ongoing training and education to ensure all users maximize the utilization of the GRC system.
- **Feedback Loop:** Establish a robust system for gathering continuous feedback from users and stakeholders to inform iterative improvements and ensure the system's full potential is realized.
- **Data Utilization:** Leverage the rich data collected for predictive analytics to enhance proactive compliance and risk management efforts.

Next Steps:

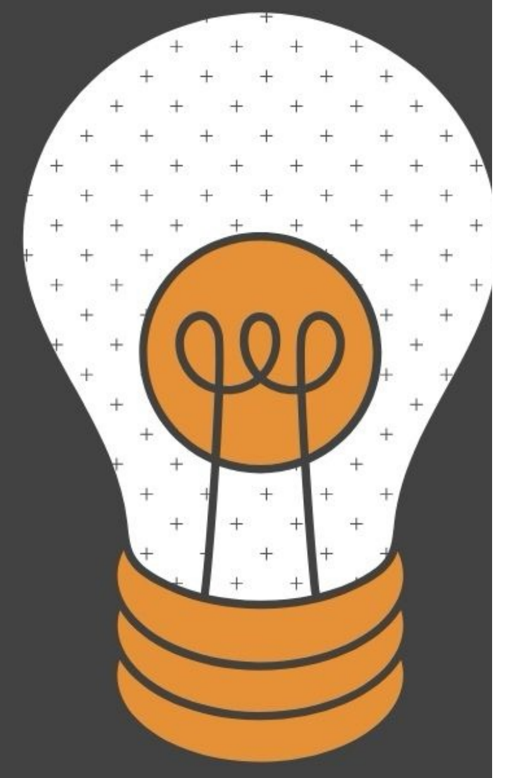
- **Expand Usage:** Encourage other business units within the organization that have not yet migrated to the Eramba GRC system to consider doing so, given the demonstrable benefits.
- **Industry-Wide Best Practices:** Share findings and experiences with organizations in the same sector to promote industry-wide best practices in GRC.
- **Continuous Improvement:** Continue refining and expanding the use of the GRC system to further enhance efficiency, risk management, and compliance in a rapidly evolving business landscape.
- **Monitoring and Compliance:** Regularly monitor the GRC system's performance and ensure compliance with changing regulations and standards.
- **Incorporate Predictive Analytics:** Explore the use of predictive analytics to improve risk management and make data-driven decisions.

Why Eramba?

- Comprehensive GRC Solution
- User-friendly interface
- Affordable implementation
- Regulatory compliance
- Centralized management
- Scalability
- Training and support
- Continuous updates

Positive Impact

- Centralized Risk Assessments
- Automated Compliance Monitoring
- Security Incident Management
- Policy Management and Documentation
- Security Awareness Training
- Auditing and Reporting



I would like to express my heartfelt gratitude to Aldwin Maloto, RIT's Chief Information Security Officer, for his invaluable guidance and unwavering support throughout the entire duration of this project. Aldwin's role as my mentor has been instrumental in the successful implementation of the Eramba GRC system and the integration of the PCI DSS 4.0 framework.

Aldwin's extensive knowledge, wealth of experience, and insightful perspective have provided me with a broader understanding of the complex GRC landscape. His mentorship was not only a source of wisdom but also a constant source of motivation, pushing me to excel and overcome challenges. His contributions went beyond mere advice; he actively engaged with our team, offering strategic insights and practical solutions. Aldwin's expertise has been a guiding light, ensuring that this project was on the right track.

Aldwin, your mentorship has been a cornerstone of our success, and I couldn't have achieved my goals without your guidance. I am truly grateful for your dedication, patience, and unwavering belief in this project. Your role in this endeavor will always be remembered as a key factor in my achievements. Thank you, Aldwin, for being a remarkable mentor and an essential part of our project's success. Your influence will continue to shape future endeavors in the world of Governance, Risk Management, and Compliance.

Aligning With ITS Values

- Champion & deliver quality solutions that advance RIT
- Increase organizational agility through continuous improvement
- Cultivate employee growth and development
- Advance information security
- Transform the customer experience

Strengthening Information Security Governance through the implementation of a GRC program for RIT's Information Security Office

By. Mike Turkowski
M.S. Professional Studies
November 26, 2023