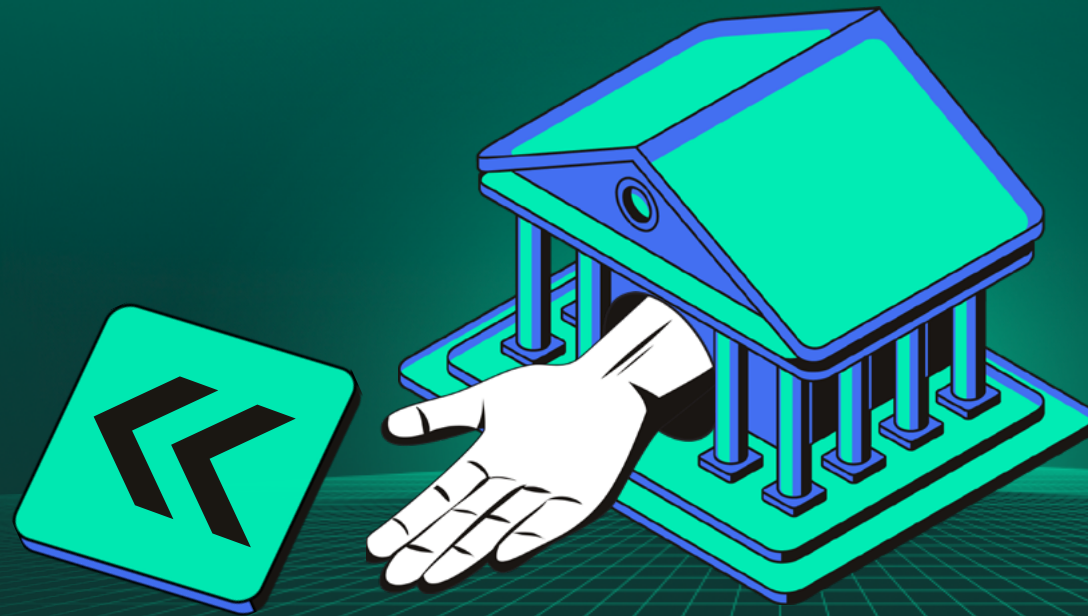# A Tailored Threat Modeling Solution for a Large US-Based Financial Institution

A large financial institution in a regulated market needed an on-premise threat modeling solution to serve two separate organizational units. Each unit had distinct needs:

- **Custom Content:** Both units required tailored content recommendations based on their specific workflows, diagrams, and responses to questionnaires. One unit also wanted exclusive access to its custom content without any default content visible.

- **Automation:** The teams needed scripts for creating projects and managing users. These scripts had to support both manual (via a user interface) and automated (via a cron job) operations, pulling information from spreadsheets.

- **Workflow Segmentation:** Separate workflows were necessary to ensure each team operated independently, with custom rules preventing overlap.

- **Environment Management:** The solution needed to be tested and validated in a development environment before being promoted to User Acceptance Testing (UAT) and, finally, production.

The institution also required inactive user accounts to be automatically deactivated after 90 days and needed the solution to integrate with their OpenShift deployment setup.

To meet the institution's needs, the IriusRisk Professional Services team worked closely with their stakeholders, starting with scoping sessions to clarify requirements. From there, the team provided tools, developed customizations, and implemented a deployment strategy

1. Configuration and Content Setup

- Delivered spreadsheets for configuration imports, simplifying data input and ensuring consistency.
- Provided templates for importing custom content, which was then structured and ingested into the platform through the API.
- Adjusted the default content to account for both teams' unique scenarios and needs.

2. Custom Automation

- Built scripts for project creation and user management. These scripts worked via:
  - A user interface for on-the-spot project creation.
  - A cron job that pulls data from spreadsheets to automate project setup through the API.
- Added functionality to automatically remove inactive user accounts after 90 days.

3. Workflow Customization

- Created two distinct workflow series tailored to the processes of each team.
- Added rules to prevent cross-access between workflows, ensuring operational independence.
- Designed permissions to align with the institution's internal processes, enforcing strict controls at each workflow stage.

4. Dynamic Questionnaires and Rules

- Created 45 dynamic questionnaires that adapted to the context of diagrams, dataflows, and scoping answers.
- Developed around 200 custom rules in the IriusRisk rules engine to apply content based on specific team needs and responses.
- Developed custom unanswered question notifications to block workflow transitions.

5. Testing and Deployment

- Configurations and customizations were first implemented and tested in the development environment.
- After thorough testing, configurations were promoted to UAT for review and approval.
- Following UAT sign-off, configurations were deployed to production using staging scripts to ensure consistency and accuracy across environments.

IriusRisk««

In just under 90 business days, the institution had a fully deployed, customized threat modeling solution that met all its requirements:

Tailored to Each Team

Both teams had separate workflows, dynamic questionnaires, and content tailored to their needs, ensuring the solution aligned with their operations.

Streamlined Processes

Automated scripts simplified project creation, user management, and account deactivation, saving time and reducing manual effort.

Scalable for Growth

The system was designed to accommodate additional teams and content in the future with minimal rework.

Secure Deployment

The multi-environment approach ensured thorough testing and compliance with the institution's security standards.

This project highlighted the importance of collaboration and flexibility in meeting customer needs. By tailoring workflows, automating key processes, and designing a scalable solution, the Professional Services team delivered a solution that fits seamlessly into the institution's environment while laying the groundwork for future growth.