Strengthening Security through Automation

FTB Governance Risk Management & Compliance Project

Cybersecurity
California Franchise Tax Board

Project Dates: July, 2020 - April, 2021 with ongoing enhancements

Nadean Shavor, Chief Information Officer
California Franchise Tax Board

Robert Mayorga, Chief Security Officer
California Franchise Tax Board

Vivian Yan, GRC Project Manager
California Franchise Tax Board

STATE OF CALIFORNIA
Franchise Tax Board

EXECUTIVE SUMMARY

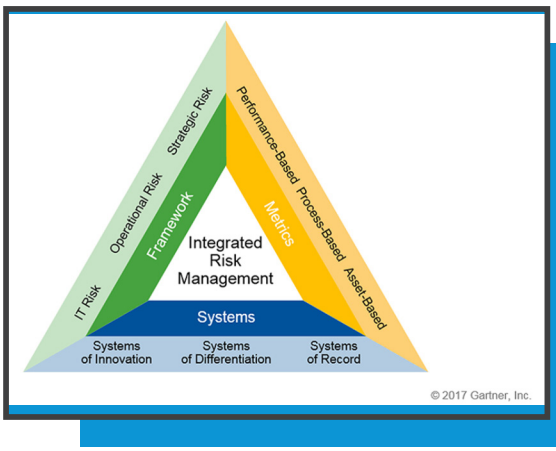
The State of California Franchise Tax Board (FTB) administers two of California's major tax programs: personal income tax and corporation tax. As part of its foundational principles, FTB is committed to protecting the privacy and security of data entrusted to the organization. FTB recently completed the Cybersecurity Governance, Risk and Compliance project. FTB prioritized and automated risk management, vulnerability and compliance management activities that harmonize laws, regulations and mandates specific to the State of California. FTB continues to improve its risk and compliance management programs with the implementation of a SaaS FedRAMP IT Risk and Compliance management solution. The IT Risk and Compliance management solution automates workflows for IT risk register dashboard, System Security Plan management workflows, Privacy Threshold Assessment and Privacy Impact Assessment management system, Plan of Action and Milestones (POA&M) management workflow systems and centralized Configuration Database management. This solution addressed priorities 1, 5 and 10 of NASCIO's State CIO Top 10 Priorities for 2022.

By leveraging service delivery partners for implementation, FTB achieved maturity in governance and compliance with security requirements and risk management through automation and increased communications workflow tracking with user-friendly workflows and templates. The solution increases department visibility in areas of non-compliance and provides audit reporting structures that assess security and privacy policy and standard compliance in several ways: NIST System Security Plan assessments, Privacy Threshold Assessments, Privacy Impact Assessments and system-generated warnings if potential gaps are identified.

The delivered solution transformed existing processes across FTB's extended enterprise into a more efficient integrated risk management program.

IDEA

Transform manual processes into an integrated risk management solution



Previously, FTB did not have a Governance Risk management tool and all security oversight, compliance processes and associated documentation were manually managed through private shared drives and a restricted SharePoint site. The objective of the Governance Risk Management and Compliance (GRC) project was to implement a robust GRC solution to enhance monitoring and minimize risks, strengthening FTB's security posture. The GRC Project implemented a department-wide security platform to effectively manage security risks and measure maturity within each unit of the organization. The platform centralized and automated security reporting, compliance, program and policy management, asset management, incident management, oversight, audits, assessment tracking and reporting for all FTB entities, and provided a departmental overview of all risks, program maturity, and trends. This overview provides actionable metrics to significantly improve the decision-making process and address risk within FTB and contributes to improved Executive Branch oversight.

IMPLEMENTATION

Once a SaaS-based platform technology was selected that met or exceeded statewide unified integrated risk management requirements in early 2020, FTB's Information Security Oversight unit began working with service delivery partners. In this partnership, FTB conducted thorough business process analysis, architected new automated flows and assessed implementation details.

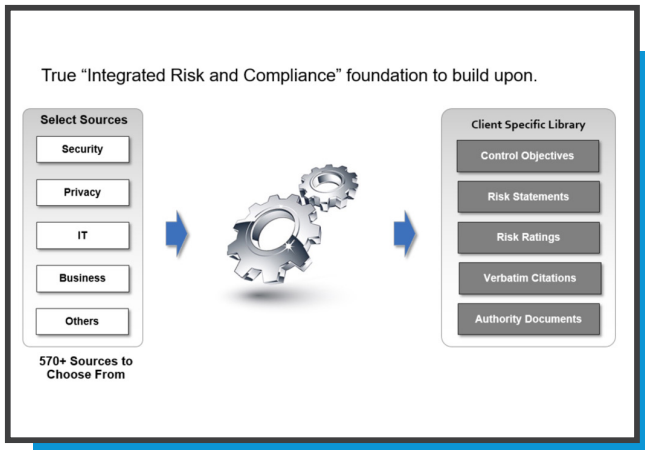
Implementation efforts focused on six specific outcomes:

1. A centralized Configuration Management Database
2. Compliance Management
3. Risk Management
4. POA&M Management
5. System Security Plan
6. Privacy Impact Analysis workflows.

The implementation process focused on success factors that included clearly defined goals and objectives, a well-defined project management process, a proven set of project management techniques and a phased approach to ensure timely delivery. The solution also included comprehensive dashboards and automated reports.

Who is involved in GRC?

- FTB's GRC solution is built on ServiceNow GovCloud FedRAMP platform
- Edgile Inc and Veteranets provided professional services support
- FTB's CIO, CSO and Privacy Officer formed Steering Committee
- FTB's Information Security Oversight Unit Managed the project and provided vision and custom requirements.
- FTB's Technology Services Division provided technical support



List of items implemented:

- Onboarded SIMM documents, NIST, and other regulatory documents into ServiceNow
- Mapped individual document citations to a common control framework
- Onboarded GRC entities and mapped to CMDB assets and business processes
- Mapped GRC entities to common control framework
- Developed a risk register tied to the common control framework
- Automated the assignment and review process for POAMs
- Developed Security Risk Assessments
- Developed Privacy Threat and Impact Assessments
- Automated the delivery and approval process for Risk and Privacy Assessments

IMPACT

Real-Time visibility of areas of non-compliance:

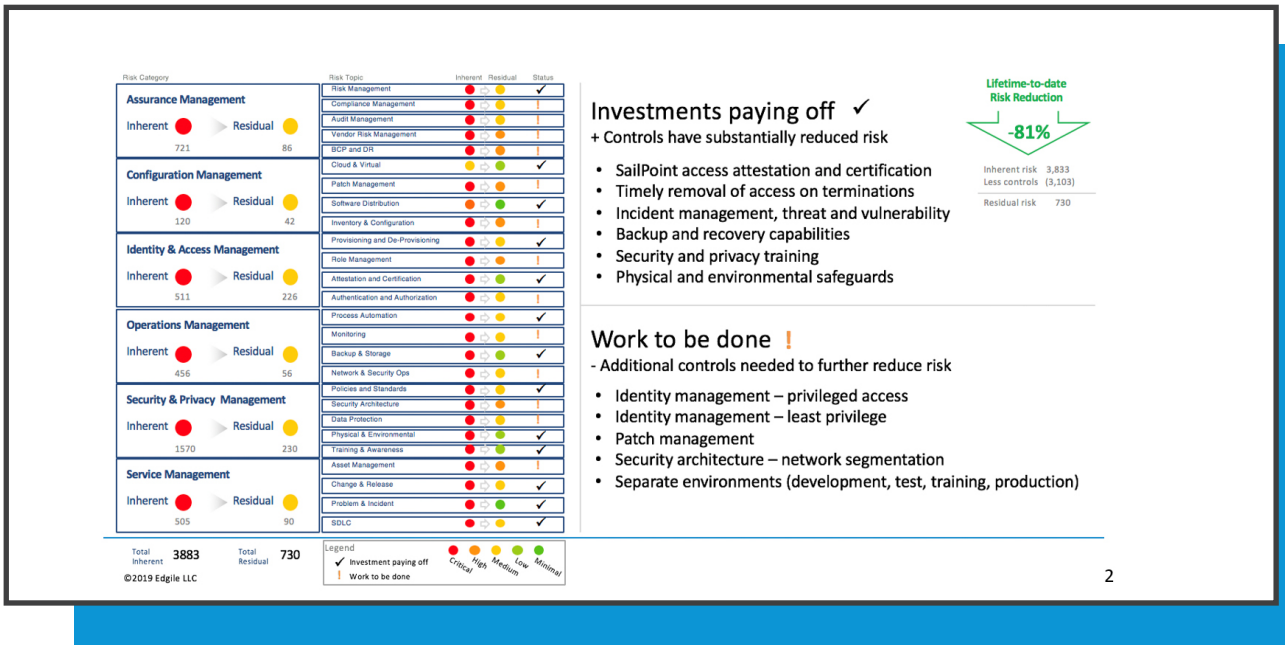
This project and the associated solution fill critical security risk compliance gaps within FTB's environment, and yield ongoing improvements in processes and management reporting that increase FTB's security posture. The supporting reports and dashboards allow FTB management teams to quickly see that the controls put in place have substantially reduced risk through timely removal of access on terminations, incident management, threat vulnerability, backup and recovery capabilities, and physical and environment safeguards.

1

[1] Sample Data

Integrated Enterprise Risk Register Dashboard

The Risk Register Dashboard highlighted the enterprise risk status and progress to communicate with stakeholders and satisfy their requirements of risk information. It also demonstrates the Return on Investments (ROI) of enterprise resources and budget allocation and identifies security control gaps. This dashboard provides a high-level view of enterprise risks and provides metrics to justify spending budget plans.



[2] Sample Data

Increased communications through workflow tracking

By moving from email and spreadsheets to a secure automated tool (ServiceNow) and providing linkages between all the Cyber Security and Privacy activities, FTB greatly improved its workflow tracking and communication. The use of an automated tool allows users to process a POA&M or Assessment much more rapidly. The dashboards used to monitor assignments are easy to use and reduce overdue responses. Reports are easily generated for multiple stakeholders using mappings of entities and a common control framework. As an added benefit, when new reporting requirements are presented, new reports can be generated quickly from existing information.

Increased workload proficiency

After the GRC implementation, the average processing time for each POA&M has been reduced from weeks to hours. Staff can produce customized reports within an hour, instead of spending days gathering data from paper documents. With automatic email reminders, overall timeframe to close a POA&M has been reduced by months.

ROADMAP

FTB is optimizing its governance compliance and improving its risk posture by continuing to add additional controls to further reduce risk, such as identity management for privileged access, security architecture for network segmentation and environment separation between development, test, training and production. In addition, this centralized solution enables FTB to prioritize automated business continuity management activities. In the future, the expansion of this automation will include configuring additional workflows, notifications, reports and dashboards related to business impact analysis, business continuity management, disaster recovery plan management and plan exercise testing.