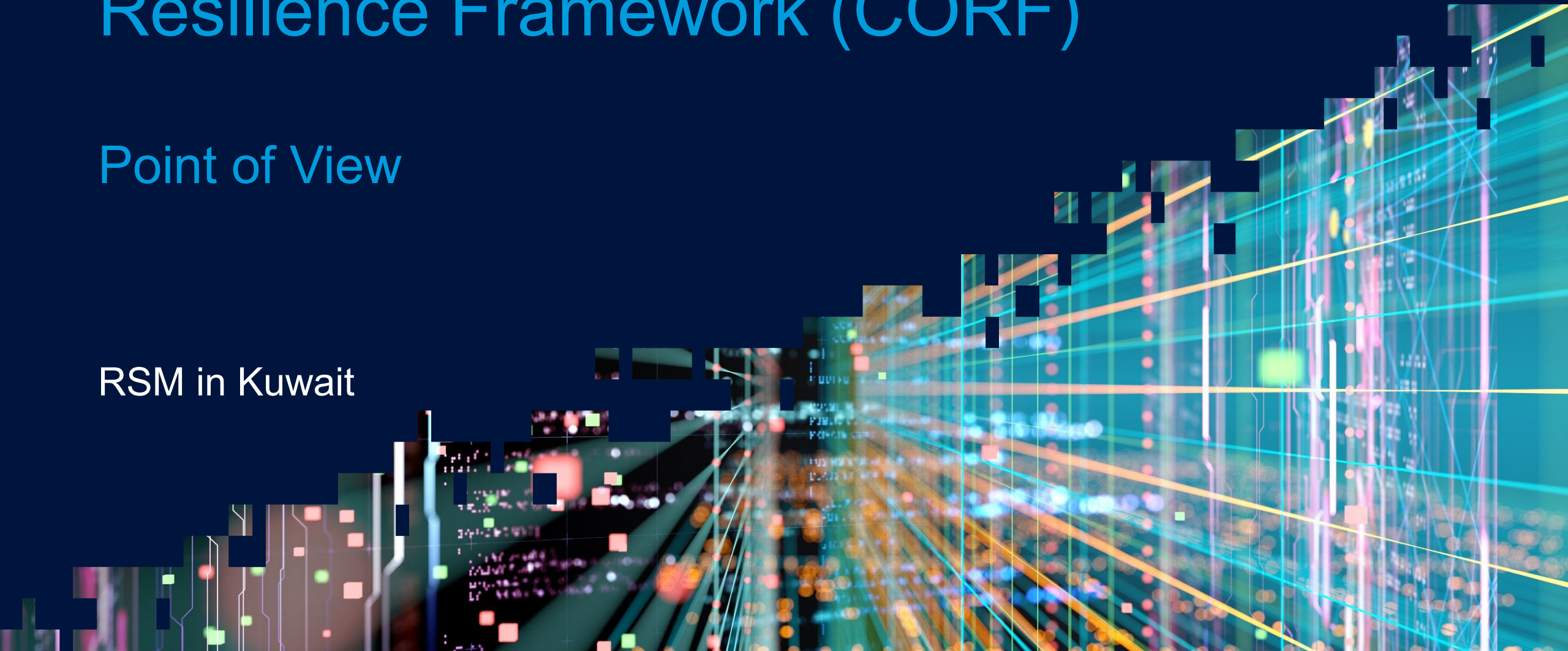
CBK - Cyber and Operational Resilience Framework (CORF)

Point of View

RSM in Kuwait



Introduction

On 3rd December 2025, the Central Bank of Kuwait (CBK) evolved the 2020 Cybersecurity Framework (CSF) into Cybersecurity and Operational Resilience Framework (CORF) to strengthen cybersecurity and operational resilience across the sector in response to evolving threats, technologies, and regulatory priorities.

The CORF aligns with internationally recognized standards and best practices like NIST, ISO27001, COBIT and encourages organizations to adopt advanced cybersecurity tools, automation platforms, and analytics to improve control effectiveness, operational efficiency, risk visibility, and enable timely risk mitigation.

The CORF applies to :

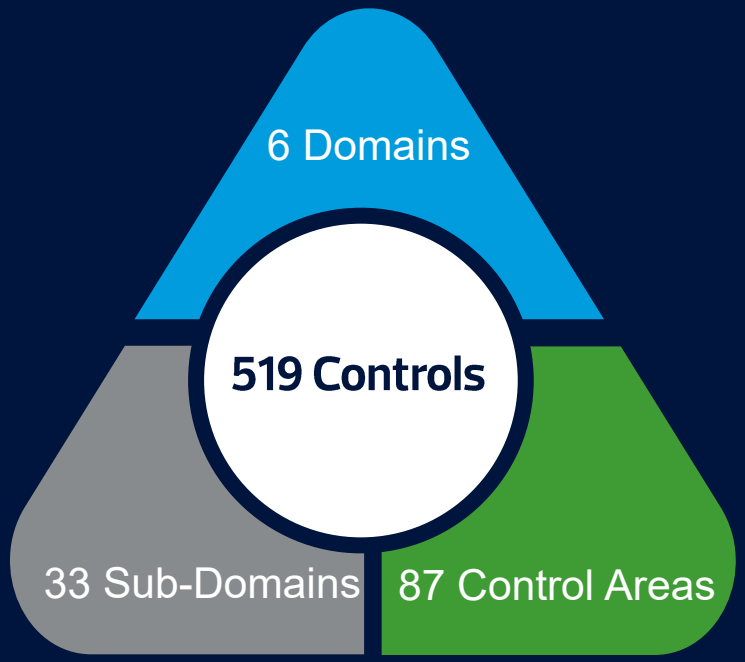
- Kuwaiti Banks;
- Foreign Banks operating in the State of Kuwait;
- Exchange Companies;
- Finance Companies;
- E-Payment of Funds Companies;
- Credit Information Companies; and
- Open Banking Service Providers.

This document provides an overview of the latest framework and key changes compared to the 2020 CBK CSF, which the regulated entities need to consider going forward.

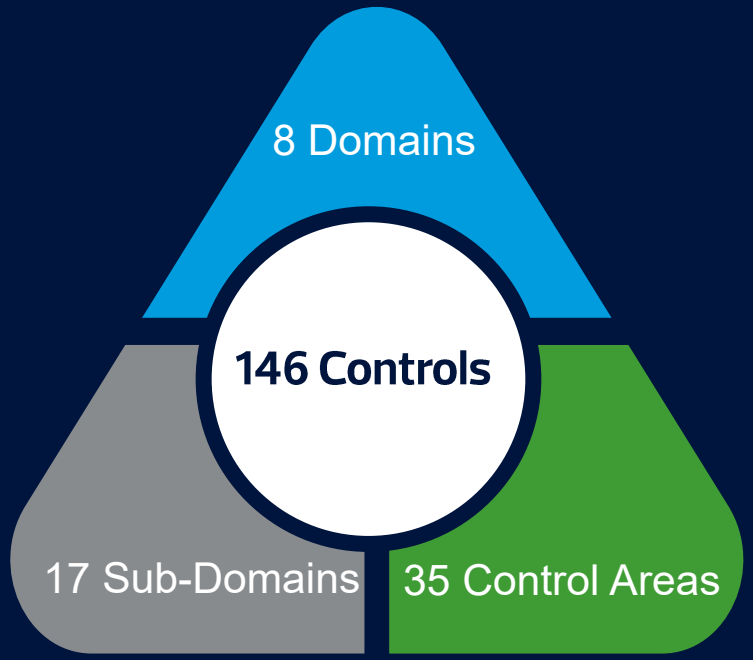
The 2020 CBK CSF comprised of 4 Domains, 36 Sub-Domains and 291 Controls.

The CORF now consists of 3 Baselines, each structured into a four-level hierarchy of Domains, Sub-Domains, Control Areas and Controls. The total number of controls has increased to **876 Controls.**

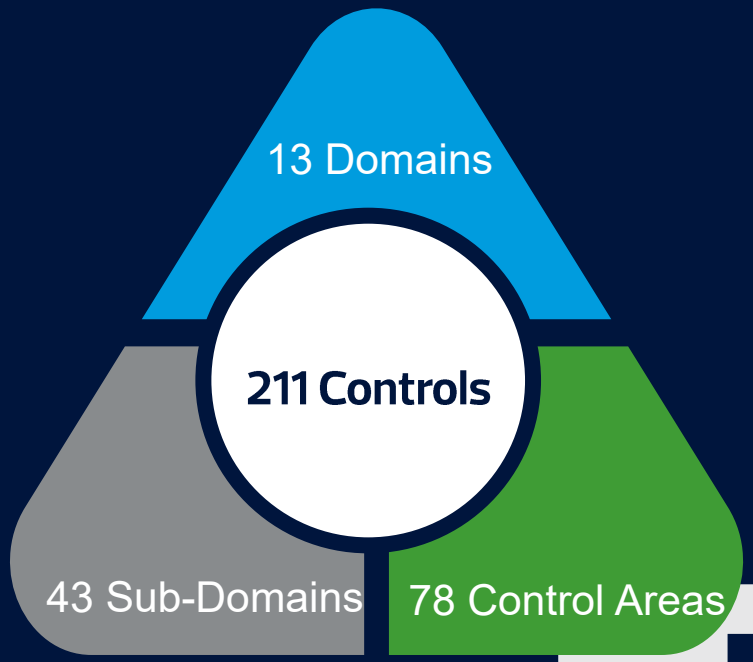
1. Cyber Resilience Baseline



2. Operational Resilience Baseline



3. Third Party Risk Management Baseline



Tier-based Assessment

CBK applies a structured and dynamic risk-based tiering model to categorize Regulated Entities based on their systemic importance, operational complexity, and overall cyber risk exposure.

Regulated Entity Risk Profile	CORF CBK Assessment Frequency
Tier – 1 : High Impact	Once every 12 months
Tier – 2 : Medium Impact	Once every 18 months
Tier – 3 : Low Impact	Once every 24 months

No tier is exempted from CBK's authority to request documentation or launch ad-hoc reviews at any time.

Each Regulated Entity shall engage an independent, CBK approved third-party assessor on **annual** basis and/or as directed by CBK to conduct an assessment against the CORF and report the results to the CBK

Assessment Structure

Compliance

Two essential tests **per control**

- Test of Design
- Test of Effectiveness

Binary Outcomes

- Compliant
- Non-compliant
- Not Applicable

- **Sub-Domain Compliance Score** – Percentage of applicable controls marked as "Compliant" within each sub-domain.
- **Domain Compliance Score** – Aggregated compliance percentage based on all sub-domains under the domain.
- **Overall Compliance Score** – Rolled-up average across all domains, offering Entity-specific (and sector-wide) compliance view.

Maturity

A standardized five-level maturity model designed to evaluate how well cybersecurity and resilience capabilities are embedded, institutionalized, automated, innovative, and continuously improved

- Level 1 - Initial
- Level 2 - Ad-hoc
- Level 3 - Baseline
- Level 4 - Advanced
- Level 5 - Innovative

Anticipatory and advanced **technology-driven** (e.g., AI-driven) practices with **real-time capabilities** that **continuously enhance** resilience, enable **adaptive response,** and promote/support sector-wide innovative practices and collaboration.

Cyber Resilience Baseline

The six domains

- Governance, Risk and Compliance
- Technology and Operations
- TPRM and SCM
- Emerging Technologies
- Payment Security
- Operational Resilience

Select maturity attributes leading to a Level 4+ maturity score

- Use of a **GRC/IRM platform** for policy, audit, TPRM, compliance, BCM and cybersecurity risk lifecycle management with real-time insights, workflows and automated dashboards.
- Automated **continuous security configurations monitoring.**
- **Security awareness and training** programs utilize AI/ML to customize content and delivery based on individual roles and needs.
- IAM processes are centralized and automated through an integrated **Identity Governance and Administration (IGA) platform.**
- **Data discovery and protection tools** (e.g., DLP, data masking, encryption) are integrated across all endpoints, servers, and cloud.
- **Fraud risk management platform** is deployed with real-time behavioral analytics and adaptive scoring per customer and device.

Operational Resilience Baseline

The eight domains

- Governance and Oversight
- Risk and Threat Management
- Business Continuity Management
- Technology Resilience
- Third-Party Resilience
- Incident and Crisis Management
- Cyber Resilience
- Testing, Training and Continuous Improvement

Select maturity attributes leading to a Level 4+ maturity score

- Use of automated tool for managing **operational resilience** policy lifecycle, BIA, DRP and BCP workflows.
- Fully fledged **crisis simulation** is conducted annually (**tactical** and strategic layer) to test decision making and resilience capability.
- Technology-enabled solution for automated monitoring of **regulatory changes** (e.g., alerts and notifications), and linked to risk registers.
- Leverage **crisis simulation platform** to design and execute end-to-end exercises.
- Key vendors and partners actively participate in **resilience exercises** to validate dependencies and coordinated response.
- **Advanced analytics** compare RTOs with dependent applications, identifying misalignments and recommending corrective adjustments before disruptions occur.

TPRM Baseline

The thirteen domains

- Governance Structure and Oversight
- Risk Management Framework
- Contractual Agreements Considerations
- Risk Assessment and Monitoring
- BCM and DR
- Incident Management
- Data Protection and Confidentiality
- Sub-Contracting
- Exit Strategy
- Storage of Data
- Cross-Border Transaction
- Usage of Cloud Services
- Inter-Affiliates

Select maturity attributes leading to a Level 4+ maturity score

- Third-party and affiliate risk scoring enhanced with **AI/ML-based predictive models**, analyzing trends in vendor failure, threat landscapes, performance, etc.
- Contract lifecycle activities are automated through a centralized platform (e.g., **Contract Lifecycle Management** (CLM) system.
- **Dependency mapping** is visualized in real-time, highlighting upstream/downstream vendor linkages, systemic vulnerabilities, and cascading failure scenarios.
- **Exit planning is predictive** and integrated with contract lifecycles, using analytics to auto-trigger pre-exit actions and initiate risk mitigation workflows.
- Real-time monitoring and advanced analytics **provide enterprise-wide visibility** into cloud risks, performance, and service health.
- Cross-border flow mapping, just-in-time access controls, and predictive retention scheduling are enabled across third parties.

The CBK CORF is a journey, not a one-time compliance check

Potential Next Steps :

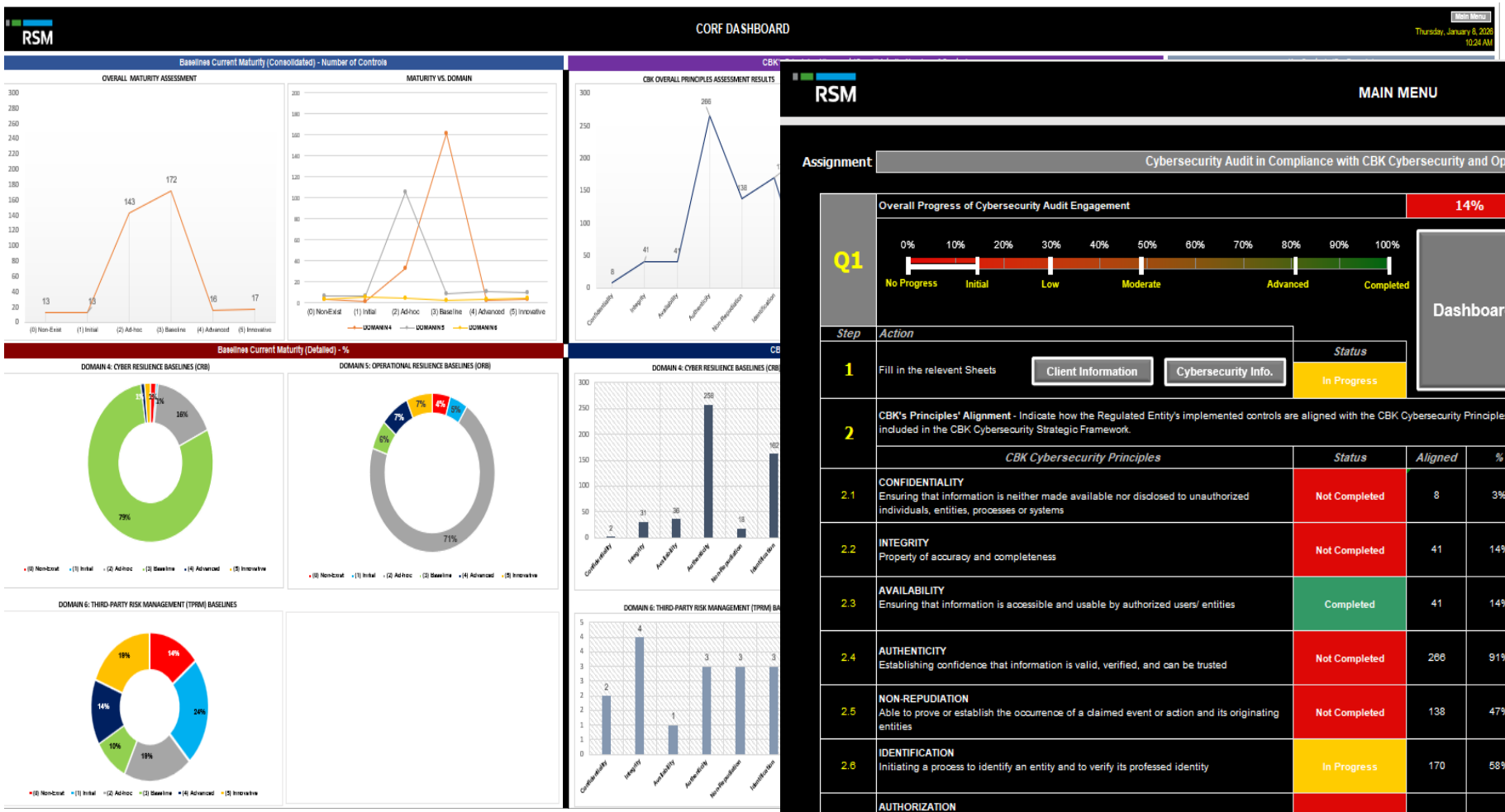
- Establish / Enhance cybersecurity and BCM framework, and automation opportunities;
- Proactively get detailed CORF gap and maturity assessment exercises conducted;
- Establish/ Enhance Third-Party Risk Management Framework and automation opportunities;
- Establish a cyber-aware culture in your organization;
- Implement / Enhance scope and functionality of an IRM/GRC platform;
- Nominate assessors and auditors for the 5-day Cybersecurity Assessors Program (CAP); and
- Estimate and assign budget to be CBK CORF compliant.

Our CORF Service Offerings

To support your CORF journey, we can assist you with the following service offerings:

Our CORF Tool

Our CBK CORF tool assists in standardizing the process of obtaining compliance and maturity scores, auto-tracks the progress of the engagement and provides reports and dashboard. Along with RSM Engage, it facilitates engagement effectiveness and efficiency



THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM in Kuwait
Arraya Tower 2 – Floors 41 & 42
Abdulaziz Hamad Alsaqar St. - Sharq
P. O. Box 2115, Safat – 13022, State of Kuwait
W: www.rsm.global/kuwait
T: +965 22961000
F: +965 22412761
E: connect@rsm.com.kw