CENTRALE BANK
CURAÇAO & SINT MAARTEN

CBCS@CENTRALBANK.CW
+599 9 434 5500

SUPERVISION NEWSLETTER

ISSUE 8| FEBRUARY 2026

EDITORIAL

Dear reader,

In 2026, CBCS will continue strengthening its supervisory framework in line with international standards. As of January 1, 2026, several changes have been implemented to our supervision structure, which we are pleased to share in this edition of the Newsletter. You will notice familiar names in new roles alongside newly appointed managers and department heads, all contributing to a more effective and future-proof Supervision Division.

To further enhance supervisory effectiveness, CBCS will adopt a stricter enforcement approach in 2026 regarding the late submission of financial statements and other mandatory reports. Institutions are therefore encouraged to ensure that their financial audit and reporting processes are well embedded to support timely compliance.

This Newsletter also includes practical tips to help smaller financial institutions strengthen their resilience against cyber-attacks.

For the Sint Maarten financial sector, a Systematic AML/CFT/CFP Risk Assessment (SARA) has been conducted last year. We highlight both good practices and areas requiring improvement. A similar assessment for Curaçao was completed earlier and discussed in a previous edition.

Climate and sustainability risks are becoming an integral part of financial supervision. These risks must increasingly be embedded in institutional policies and processes. CBCS has placed this topic on its medium-term agenda and intends to introduce related requirements over time. We encourage the sector to take a structured and forward-looking approach in addressing climate and sustainability risks.

Management Team Supervision Division

WHAT'S INSIDE THIS ISSUE:

ADVANCEMENT AND OPTIMIZATION OF SUPERVISION - 2

ANNUAL FINANCIAL STATEMENTS: EXTENSIONS END, ENFORCEMENT STEPS UP - 4

CYBER HYGIENE: SIMPLE TIPS FOR PROTECTING MICRO AND SMALL FINANCIAL INSTITUTIONS - 5

SARA COMPLIANCE ASSESSMENT FOR SINT MAARTEN - 7

CLIMATE & SUSTAINABILITY: TIME FOR THE NEXT STEP - 9

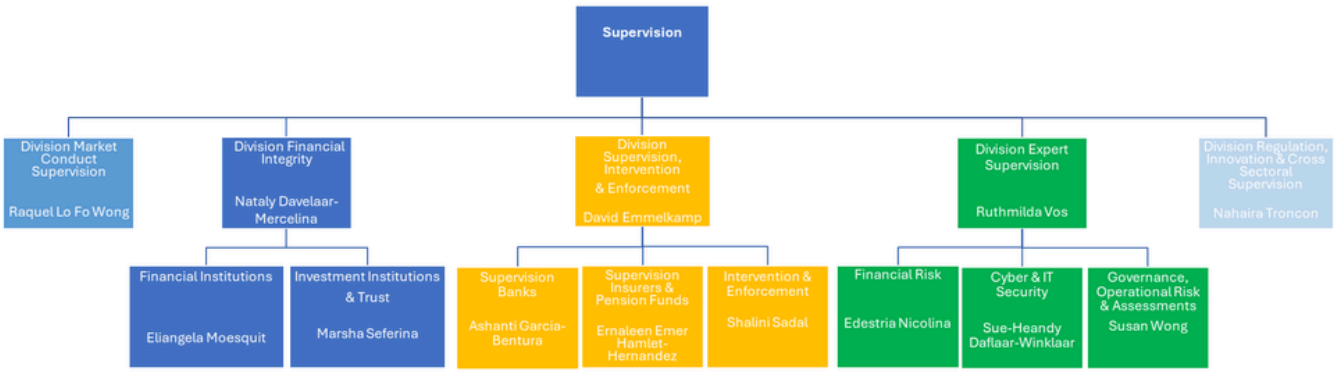
ADVANCEMENT & OPTIMIZATION OF SUPERVISION

In 2021, the CBCS launched its New Style of Supervision, a more focused and intrusive style of supervision. The new supervisory approach and methodology were implemented over the period 2021–2025, aiming to organize supervision in a risk-based, more effective, and future-proof way. This was achieved, among other things, through amendments to legislation and regulations, the use of specialized expert teams, a stronger focus on significant institutions, and the enhancement of the enforcement instruments.

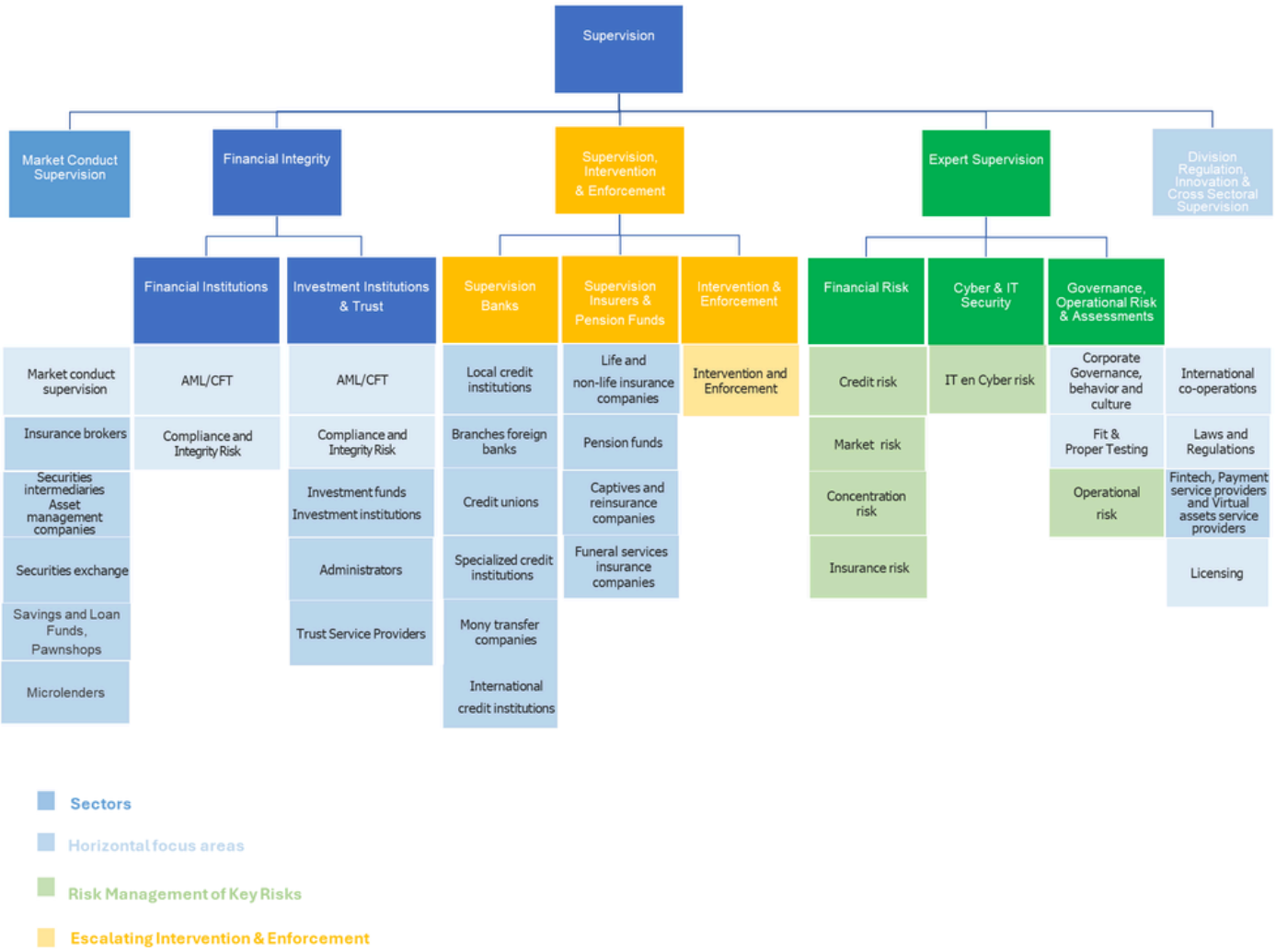
The changes were also intended to ensure compliance with international standards for effective supervision in the area of combating money laundering and terrorist financing (AML/CFT). An international evaluation of the Caribbean Financial Action Task Force (CFATF) conducted in 2025 confirmed that the CBCS has an adequate risk-based AML/CFT supervisory process and that the legislative and regulatory framework is up to date. At the same time, it was concluded that the number of conducted examinations should be intensified and that more measures should be imposed where deficiencies are identified. Furthermore, additional attention is required for risks related to terrorist financing.

To address these findings, a number of changes were introduced as of January 1, 2026, with corresponding organizational and personnel adjustments. The new organizational chart allows for the easy integration of new risk areas and institutions, including five divisions, each led by a manager. Two divisions comprise three departments each, while one division comprises two departments.

THE NEW ORGANIZATIONAL CHART of Supervision



The selected structure presented below further illustrates the key focus areas within each department followed by an overview outlining the main sectors and the respective focus areas at both the divisional and departmental levels.



More information on the New Style of Supervision is available on our website.

ANNUAL FINANCIAL STATEMENTS: EXTENSIONS END, ENFORCEMENT STEPS UP

To enhance supervisory effectiveness and promote accountability, the CBCS is reinforcing its approach toward the late submission of financial statements and other mandatory reports. This initiative forms part of the ongoing effort to ensure transparency, consistency, and equal treatment across all supervised sectors. The strengthened approach will apply to all reporting periods ending on or after 31 December 2025.

Timely receipt of annual financial statements and other legally required reports is critical to the effectiveness of our supervision. Structural delays lead to risk assessment bottlenecks and undermine equal treatment among institutions. With this change, CBCS aligns itself with international supervisory standards that require consistent and transparent enforcement of reporting obligations.



Under the strengthened approach, the CBCS will apply stricter enforcement when institutions fail to meet their legally prescribed submission deadlines. Requests for extensions will only be considered under very exceptional circumstances, such as force majeure situations (e.g. natural disasters, major IT or cyber incidents, or severe disruptions at critical service providers). This ensures uniform and transparent treatment of all institutions.

This approach applies to all supervised entities, including credit institutions, insurance companies, trust service providers, investment institutions, administrators, money transfer companies, insurance intermediaries, securities brokers and virtual asset service providers.

The CBCS may take enforcement measures if reports are not submitted within the legally required period. In principle, the CBCS's stricter enforcement procedure will be as follows:

- Upon identifying a violation, the CBCS will immediately issue a notice of intent to impose an order subject to a penalty.
- The institution will have no more than ten (10) business days from the date of the notice to submit its views in writing. If the institution submits the missing documents within that period, the CBCS will refrain from imposing the administrative sanction.
- If the 10-day period expires without the institution having submitted the missing documents and without the CBCS having received a written response to the notice, the CBCS will proceed, without exception, to impose the order subject to a penalty.
- In addition to imposing an order subject to a penalty, the CBCS may impose an administrative fine if, in its view, the violation is sufficiently serious and the institution acted culpably.

The applicable sanctions and penalty levels are defined in the relevant supervisory ordinances and may differ per sector. In general, the CBCS may impose administrative fines or penalty orders that reflect the severity and duration of the non-compliance, consistent with the legal provisions in force.

The CBCS requires every supervised institution to have internal processes and procedures in place to ensure full and timely compliance with all reporting obligations as of the 2025 year-end reporting cycle. For any questions regarding applicable deadlines or requirements, please contact your designated CBCS supervisor. For information about this policy, please send an email to info@centralbank.cw.

CYBER HYGIENE: SIMPLE TIPS FOR PROTECTING MICRO AND SMALL FINANCIAL INSTITUTIONS

In recent months, CBCS has observed an increase in cyberattacks targeting small financial institutions across the region. While these institutions may assume that their size makes them less attractive to criminals, the reality is quite the opposite. Cybercriminals often see smaller institutions as easier targets, given their limited resources and lower budgets for cybersecurity.

The consequences of a successful cyberattack (hack) for these small institutions can result in financial loss, exposure of sensitive customer information, reputational damage, disruption of services, and in some cases, a complete halt of operations.

This is why adopting strong cyber hygiene practices is no longer optional — it is essential. CBCS is therefore issuing this guide to help small financial institutions protect sensitive customer information, ensure smooth operations, and avoid costly security breaches. This guide provides the foundation for strengthening cyber hygiene and building greater resilience.

→ Back up your institutions data

Think of backups as your (digital) safety net. If your systems are ever compromised, having a backup means you can restore your important files quickly and continue providing services to your clients. Regularly back up your data in multiple secure locations (e.g., cloud and external drives), keep backups separate from main systems, and automate the process to ensure consistency and protection against cyberattacks.

→ Protect your devices from malware

Malware (like viruses or ransomware) can sneak into your systems through emails, websites, or even USB drives. Protect your devices by using up-to-date antimalware software, keeping the firewall enabled, and limiting or disabling USB use to prevent unauthorized access.

→ **Secure your mobile devices**

Institutions frequently access systems from mobile devices such as smartphones and tablets, which can be a weak link if not protected adequately. Secure mobile devices with strong passwords or biometrics, enable encryption to protect stored data, and only use trusted, regularly updated apps.

→ **Use strong passwords in combination with multi-factor authentication (MFA)**

Weak or reused passwords remain one of the biggest security risks. Make sure your passwords are strong (12+ characters, mixed symbols, not personal info), in combination with an extra layer of security using multi-factor authentication (MFA).

→ **Spot and avoid phishing attacks**

Phishing is when attackers attempt to deceive users into revealing sensitive information through fake emails, websites, social media, or currently AI-generated content. Protect against phishing by double-checking senders, training staff to recognize and report suspicious messages without clicking links or attachments and using spam filters to block harmful emails.

→ **Keep your software up to date**

Software updates often contain security patches that protect against newly discovered threats. Delaying updates can leave your institution vulnerable to imminent attacks. Therefore, keep systems secure by enabling automatic updates and regularly checking that all updates are applied.

→ **Monitor, detect, and respond to incidents**

Even with the best security practices in place, incidents can happen. Maintaining a clear incident response plan and regularly practicing it with your team so everyone knows their role is crucial for minimizing impact.

→ **Seek external support when needed**

Not every institution has the in-house expertise or resources to implement all cybersecurity measures effectively. In such cases, it is wise to seek help from qualified external professionals.



In conclusion, by making cyber hygiene a daily practice, institutions can reduce cyber risks, protect customer data, and strengthen the resilience of both their operations and the wider financial system. The CBCS strongly encourages all institutions, regardless of size, to prioritize cybersecurity as a critical component of their operations and to view cyber hygiene as an ongoing commitment, not a one-time effort.

SARA COMPLIANCE ASSESSMENT FOR SINT MAARTEN

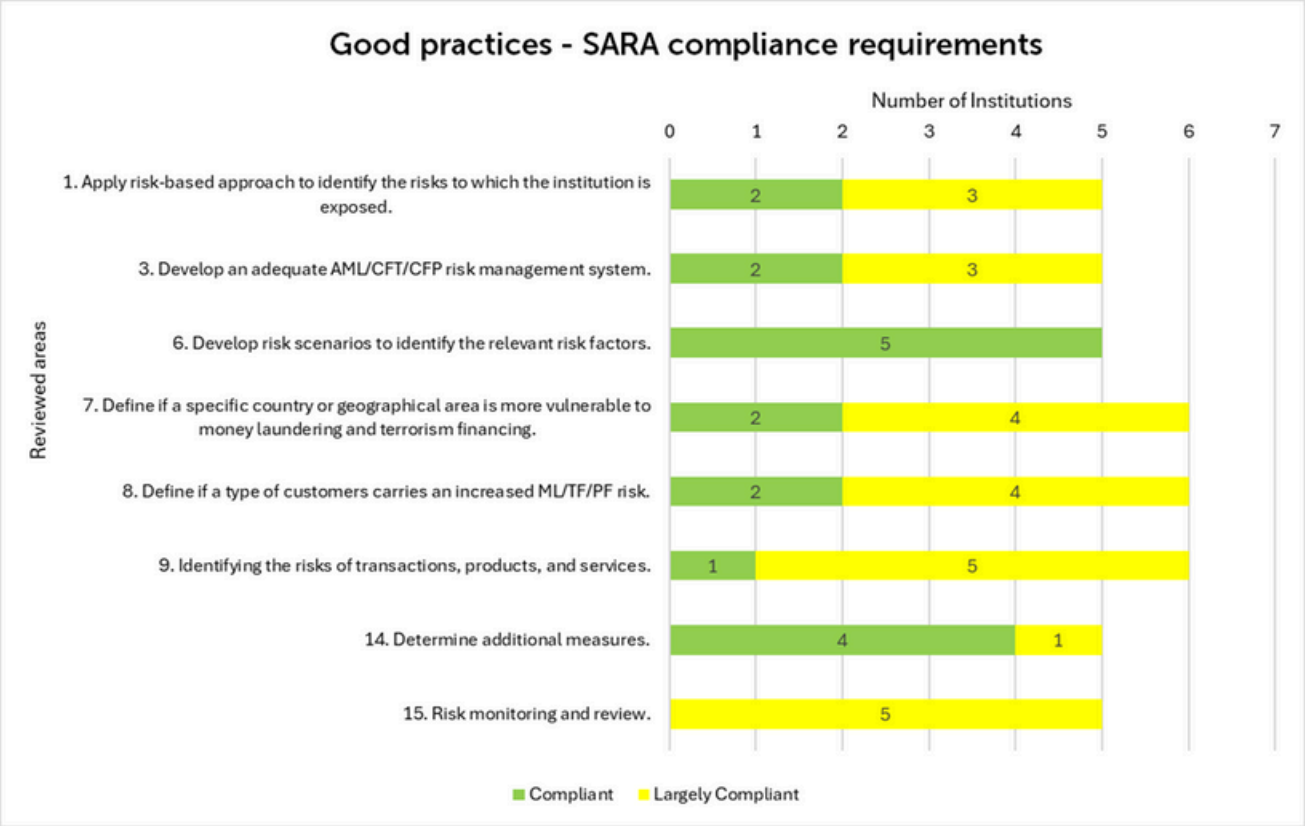
In 2025, our Governance, Compliance, and Conduct Supervision (GCCS) department conducted assessments of the Systematic AML/CFT/CFP Risk Assessments (SARA) for ten financial institutions in Sint Maarten to evaluate their compliance with applicable regulatory requirements. The institutions were selected based on National Risk Assessment results, AML/CFT/CFP risk analysis, and feedback from our Account Supervision department. The goal was to identify good practices and areas needing improvement to help institutions enhance their SARA quality.

Based on the review conducted, the CBCS determined that overall:

- Credit Institutions met most compliance criteria, showing only minor shortcomings.
- Trust Service Providers, Life Insurance Companies and Intermediaries, and Money Transfer Service Providers exhibited the most areas for improvements.

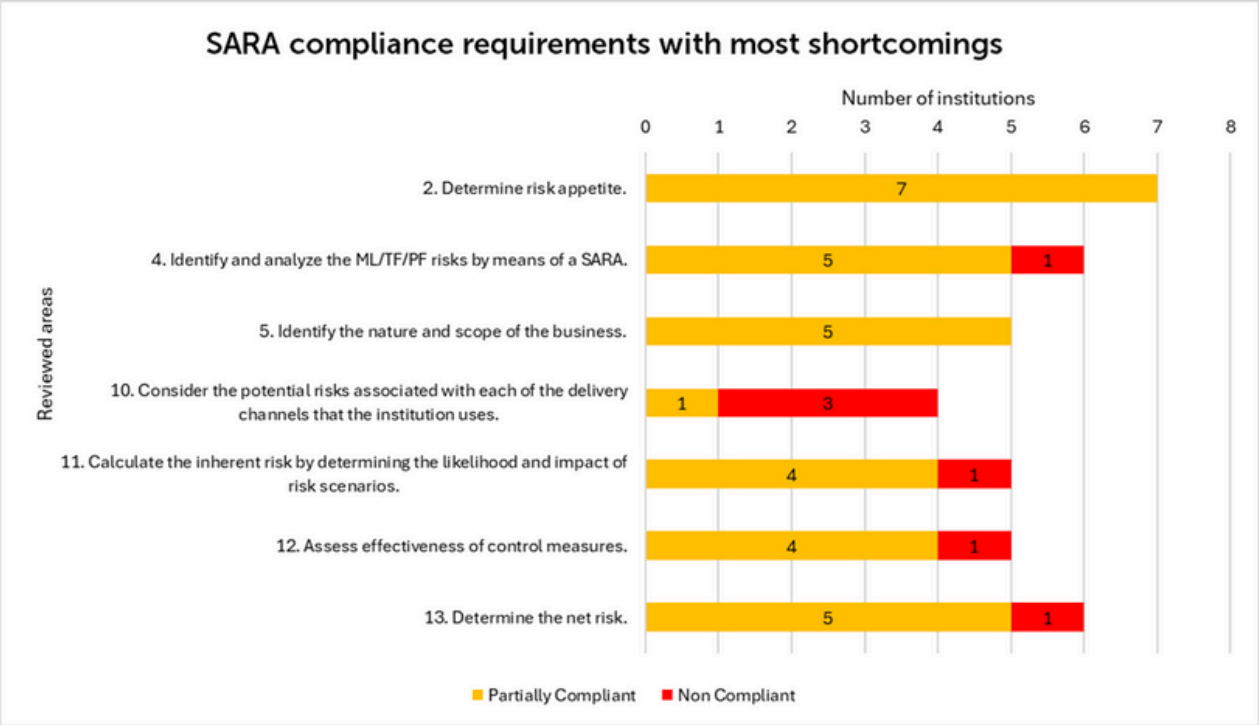
Good practices

From our review of the compliance with the CBCS' Guidance Paper on the SARA, some good practices were observed where institutions were rated compliant or largely compliant.



Areas for Improvement

These assessments also revealed some shortcomings across the board related to:



The majority of the SARAs were prepared internally by and/or with the involvement of the institution's Compliance/Risk Management functions. This suggests that the institution is aware of the importance of investing in internal Compliance and Risk Management functions to further strengthen and support the institution in its ability to effectively identify ML/TF/PF risks and to develop an adequate AML/CFT/CFP risk management framework. Additionally, engaging relevant employees in risk assessments and ensuring that senior management visibly approves the SARA is crucial to strengthening the institution's risk management framework.

By taking proactive steps to identify, assess, and manage risks, institutions not only ensure regulatory compliance but also strengthen their long-term operational integrity.

For more details on the SARA compliance requirements, please refer to the CBCS Guidance on the Systematic AML/CFT/CFP Risk Assessment for Sint Maarten on our website.

CLIMATE & SUSTAINABILITY: TIME FOR THE NEXT STEP

In recent years, we have regularly highlighted climate and sustainability risks from a supervisory perspective. Several institutions have taken initial steps, and last year's survey shows awareness is increasing. This is positive, but further action is needed.

Climate change brings risks that are becoming increasingly visible. Both physical risks (such as extreme weather) and transition risks (new regulations, the energy transition, changing customer behavior) can affect the stability of institutions. This calls for a structured and forward-looking approach.

Climate and sustainability risks are not temporary trends: they affect the core of reputation, financial stability, and business continuity. Institutions that act early and strengthen their systems will be better prepared for future external demands from markets, investors, and regulators, while also contributing to a more stable financial system.



Our expectations for the coming period

- Responsible governance: Boards and management should recognize climate and sustainability risks, establish policies, and assign responsibilities for managing them.
- Integration into risk management: Incorporate these risks into existing risk assessments and decision-making processes.
- Transparency and best practices: Follow internationally recognized sustainability reporting principles (such as those developed by the IFRS Foundation, the Task Force on Climate-related Financial Disclosures, or the Global Reporting Initiative) to ensure reporting is clear, comparable, and useful.
- Proportionality: The approach should match the size and complexity of the institution. Smaller institutions can start simply, while larger ones should adopt a detailed, structured approach.
- Broader perspective: Trust offices and service providers should integrate ESG considerations into services, due diligence, and client support for non-financial reporting or ESG policies.

The first steps have been taken. Now it is time to embed climate and sustainability risks in policies, risk management, and reporting. Doing so strengthens institutional resilience and supports the long-term stability of the financial system. While these steps are currently voluntary, the CBCS is expected to introduce formal requirements in the medium term.