NuSummit Cybersecurity

WHITEPAPER

Complying with SAMA Counter Fraud Framework

CONSUMER IDENTITY AND ACCESS MANAGEMENT

Table of Contents

Introduction

The Saudi Arabian banking and financial industry has seen a significant increase in online fraud and associated losses in recent years:

- Over 4.84 million accounts were opened remotely without verifying the customer's identification, according to the Saudi Central Bank (SAMA). This accounts for 55% of all remotely opened online accounts.
- More than half of respondents surveyed across the region reported an increase in fraud (by 6% or more) over the last 12 months, with 52% of fraud originating from digital channels.
- The impact is substantial, with organizations incurring costs between three and five times the actual value lost to fraudsters. This includes fines, fees, and effort spent on investigating fraudulent transactions.
- The most common modes of financial fraud exploited by criminals in Saudi Arabia include impersonation, fictitious recruitment, phantom investment, fake web pages or platforms, and internal fraud.
- Cybercriminals remain technologically more advanced than those tasked with combating them, with around 45% of GCC IT experts acknowledging their organizations experienced at least one known security incident in the past year.

To combat this growing threat, the Saudi Central Bank (SAMA) has established a Counter-Fraud Framework to enable financial organizations to effectively identify and address fraud risks, assess maturity levels, and evaluate the effectiveness of counter-fraud controls. This initiative is essential for safeguarding the integrity of Saudi Arabia's financial system and supporting the Kingdom's Vision 2030 goals of economic diversification and digital transformation.

This whitepaper delves into the critical aspects of SAMA's Counter Fraud Framework and how Customer Identity and Access Management (CIAM) solutions can assist organizations in achieving compliance.

The Saudi Central Bank Regulatory Framework Initiatives

The financial sector's principal regulator in Saudi Arabia is the Saudi Central Bank, previously called SAMA. To fight financial fraud, the bank has implemented a thorough Counter-Fraud Framework. This framework is part of a larger regulatory structure encompassing crucial legislation like the Anti-Money Laundering Law, the Anti-Cyber Crime Law, and the Companies Law.

Collectively, these regulations establish a solid legal basis for addressing financial fraud, explicitly outlining the duties and responsibilities of financial institutions.

Risk Management and Cybersecurity Measures

Financial entities must comprehensively evaluate fraud risks to recognize and analyze potential threats. This process creates a risk-centric strategy for fraud prevention, clearly delineating organizational roles and duties in risk management. The framework also recognizes the interconnection between cybersecurity and fraud prevention, implementing specific cybersecurity rules to bolster defenses against digitally facilitated fraud.

Fraud Detection Systems and Compliance Consequences

Financial Institutions in Saudi Arabia must:

- Use advanced fraud detection systems with the latest tech and data analysis.
- Follow mandated reporting protocols for suspected fraud.
- Maintain clear incident response and investigation procedures.

Non-Compliance risks:

Financial Penalties

Regulatory Actions

Reputational Damage

Financial Fraud Law penalties:

- Up to 7 years imprisonment
- Fines up to SAR 5 million

These penalties apply to both fraudulent misappropriation and unlawful appropriation of entrusted funds.

The Saudi Central Bank Counter-Fraud Framework

Counter Fraud Framework

3. Goverance

- 3.1 Goverance Structure
- 3.2 Counter Frarud Stratergy
- 3.3 Counter Fraud policy & proceducres
- 3.4 Roles and Responsibilities
- 3.5 Counter Fraud Department
- 3.6 Management Information
- 3.7 Supervisory Notifications
- 3.8 Counter Fraud Technolgoy
- 3.9 Counter Fraud Internal Audit

4. Prevent

- 4.1 Risk Management
- 4.2 Due Dillegence
- 4.3 Training and Awareness
- 4.4 Authentication
- 4.5 Fraud, Finacial, Crime and Cyber Alignment
- 4.6 Fraud Prevention Standards

5. Detect

- 5.1 Fraud Detection Standards
- 5.2 Fraud Detection Systems
- 5.3 Monitoring to Detection Fraud
- 5.4 Whistle Blowing

6. Respond

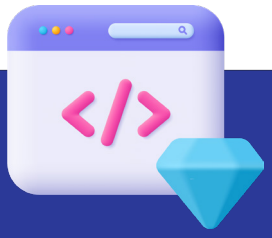
- 6.1 Fraud Response Plan
- 6.2 Alert and Case Management
- 6.3 Fraud Investigation
- 6.4 Fraud Remediation

Objectives

The Counter-Fraud Framework developed by the Saudi Central Bank is designed to:

- Create a standardized methodology for tackling fraud risks across all affiliated organizations.
- Elevate the sophistication and effectiveness of fraud control measures within these entities.
- Guarantee comprehensive and efficient fraud risk management throughout the network of member organizations.

Domains



The Counter-Fraud Framework is structured around four fundamental areas: Fraud Governance, Prevention, Detection, and Response. Within each of these areas, the framework provides detailed sub-components and directives. These elements are crafted to assist financial institutions in strengthening their approaches to preventing and mitigating fraudulent activities.

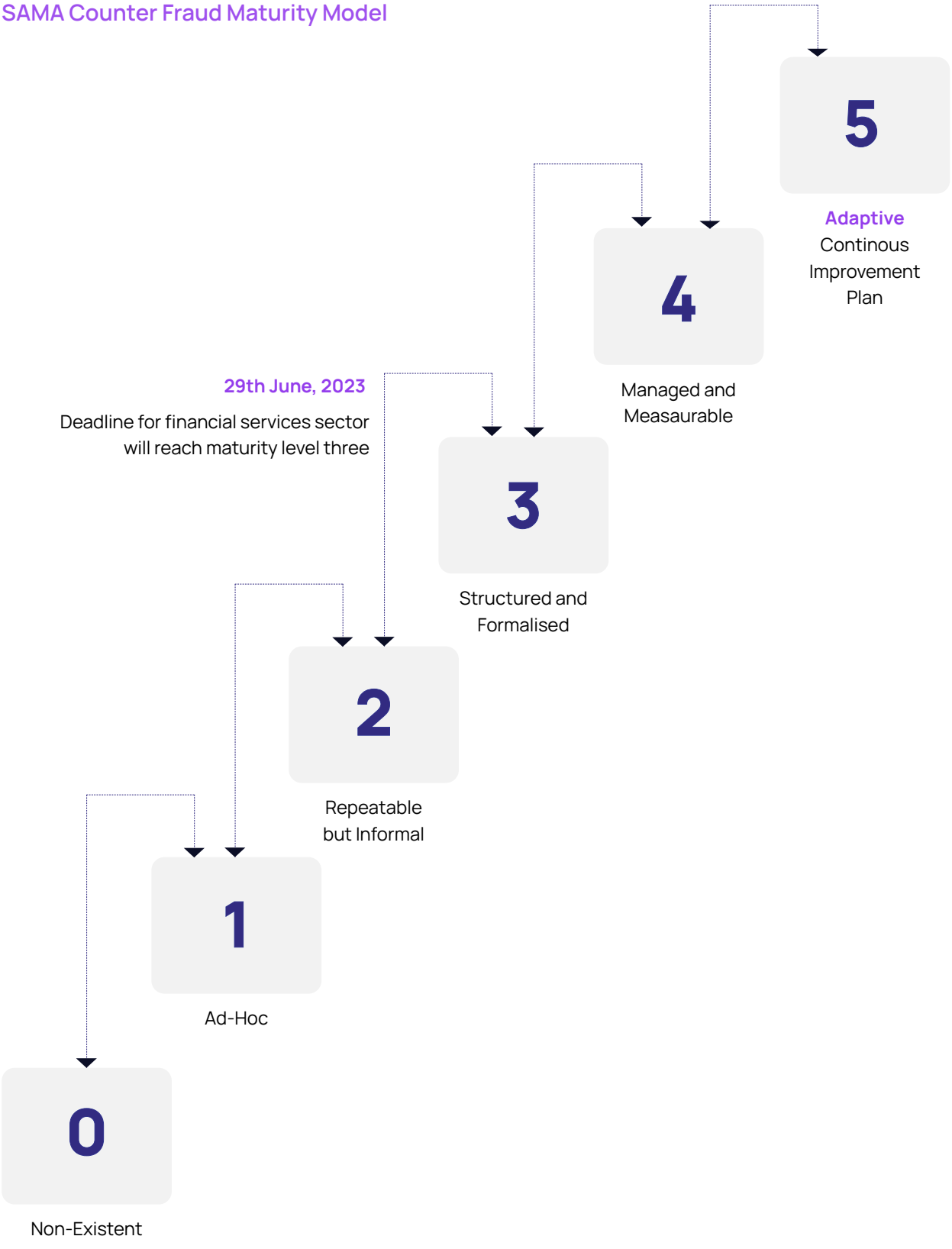
Maturity Model and Expected Maturity Levels

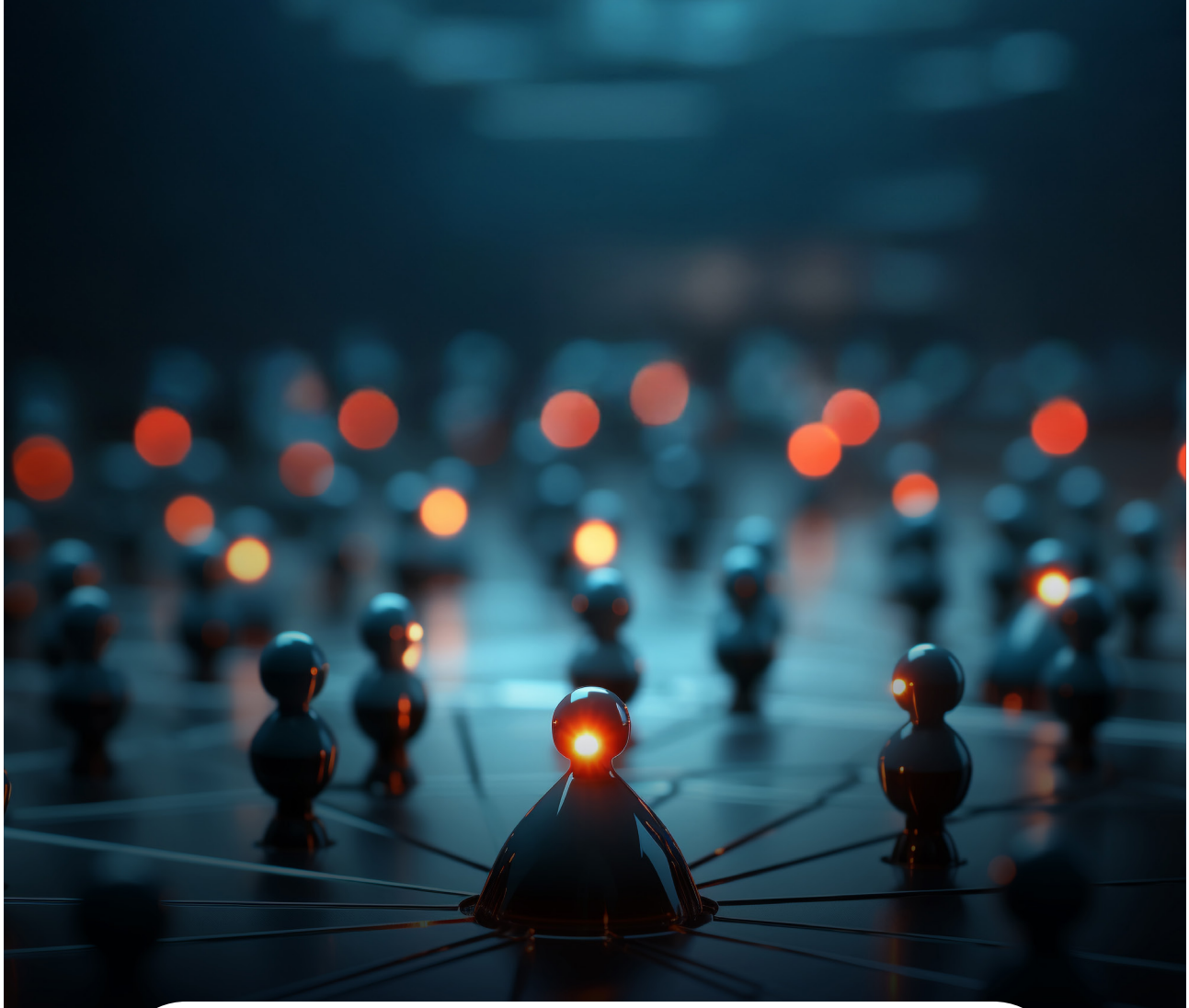
The Counter-Fraud Framework incorporates a six-tier maturity model, with levels from 0 to 5, to assess the maturity of fraud control measures in financial institutions. To achieve an appropriate counter-fraud maturity model, SAMA expects organizations to operate at maturity Level 3 or higher.

To meet level 3 criteria, institutions must have:

- Established and approved counter-fraud controls
- Functional fraud detection systems
- Continuous oversight of adherence to counter-fraud documentation protocols.

SAMA Counter Fraud Maturity Model





How Customer Identity Management Deters Fraud

Customer Identity and Access Management (CIAM) play an important role in preventing fraud originating from stolen credentials and account takeovers. It can detect and prevent fraudulent transactions, continuously evaluate the user's risk posture throughout the session, and detect compromised accounts and elevated risks. It can collect and interpret multiple signals about the user – their device, network, reputation, and known behaviors – and then make fine-grained access and authorization decisions for any high-stakes transaction.

Account Takeover Fraud

It can conduct identity authentication with robust and nuanced decision-making about when and how-to step-up authentication. It meets the requirements of strong customer authentication using the factors of:

- **Inherence** — including physical and behavioral biometrics
- **Possession** — including device intelligence and secure delivery of one-time passcodes
- **Knowledge** — including the execution of secret questions

Application Fraud

This enables customers to take a photo of themselves to match their faces to the documents they have provided. It is now possible to validate identity documents via data extraction from machine-readable chips and text andcorroborate information with third-party data sources. Further checks using holograms ensure that the documents provided have not been tampered with.

KYC and Compliance

Effective CIAM solutions are critical in conducting and maintaining Know Your Customer (KYC) processes. CIAM enables organizations to securely capture, manage, and verify customer identities in compliance with regulatory requirements. This ensures that customer data is accurate, up-to-date, and protected against unauthorized access while providing a seamless user experience. By automating KYC processes, CIAM solutions help organizations swiftly onboard customers, reduce manual errors, and continuously comply with changing regulatory requirements. By implementing robust CIAM solutions, organizations can reduce the risk of regulatory fines and damage to brand reputation, which can have severe financial consequences. Effective CIAM solutions are critical in conducting and maintaining Know Your Customer (KYC) processes. CIAM enables organizations to securely capture, manage, and verify customer identities in compliance with regulatory requirements. This ensures that customer data is accurate, up-to-date, and protected against unauthorized access while providing a seamless user experience. By automating KYC processes, CIAM solutions help organizations swiftly onboard customers, reduce manual errors, and continuously comply with changing regulatory requirements. By implementing robust CIAM solutions, organizations can reduce the risk of regulatory fines and damage to brand reputation, which can have severe financial consequences.

Account Takeover Fraud

CIAM makes sure that identity verification can be completed using AI and Machine Learning technology.

Application Fraud

CIAM confirms that only legitimate customers are using their accounts and making transactions.

KYC and Compliance

CIAM enables organizations to meet KYC requirements for regulatory compliance.

How NuSummit Cybersecurity CIAM Can Help Organizations Comply with Counter Fraud Framework

Governance (CFF 3)

Counter Fraud Framework

3. Goverance

- 3.1 Goverance Structure
- 3.2 Counter Frarud Stratergy
- 3.3 Counter Fraud policy & proceducres
- 3.4 Roles and Responsibilities
- 3.5 Counter Fraud Department
- 3.6 Management Information
- 3.7 Supervisory Notifications
- 3.8 Counter Fraud Technolgoy
- 3.9 Counter Fraud Internal Audit

4. Prevent

- 4.1 Risk Management
- 4.2 Due Dillegence
- 4.3 Training and Awareness
- 4.4 Authentication
- 4.5 Fraud, Finacial, Crime and Cyber Alignment
- 4.6 Fraud Prevention Standards

5. Detect

- 5.1 Fraud Detection Standards
- 5.2 Fraud Detection Systems
- 5.3 Monitoring to Detection Fraud
- 5.4 Whistle Blowing

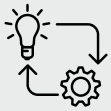
6. Respond

- 6.1 Fraud Response Plan
- 6.2 Alert and Case Management
- 6.3 Fraud Investigation
- 6.4 Fraud Remediation

Organizations often face governance-related challenges in fraud management, including:

- Insufficient detection of fraudulent activities, often due to siloed approaches and lack of cross-functional oversight.
- Unclear definition of information security-specific quantified risk appetite, misaligned with operational and enterprise fraud management governance structures.
- Difficulties in applying fraud management methodologies to accurately assess risk levels, often stemming from inadequate board-level engagement and understanding.
- Challenges in correlating vulnerabilities and risks to identify indirect risks or risk escalation, frequently due to fragmented governance frameworks.

NuSummit Cybersecurity offers comprehensive expertise in cyber counter-fraud framework programs and risk advisory services. We help organizations strategize, evaluate, and implement robust counter-fraud security initiatives. Our offerings extend to governance risk and compliance management frameworks, enhancing security standards and accelerating organizational transformation. Our governance strategies include:



Control Design and Implementation

- Design or improve internal fraud prevention controls.
- Recommend and implement fraud detection technologies.

Risk Assessment and Analysis

- Evaluate current fraud risks and vulnerabilities.
- Compare existing controls to framework requirements.

Compliance and Monitoring

- Ensure fraud prevention measures meet framework requirements.
- Set up continuous monitoring and review mechanisms.

Incident Response and Management

- Develop or enhance fraud incident response plans.
- Support fraud investigations with forensic analysis.

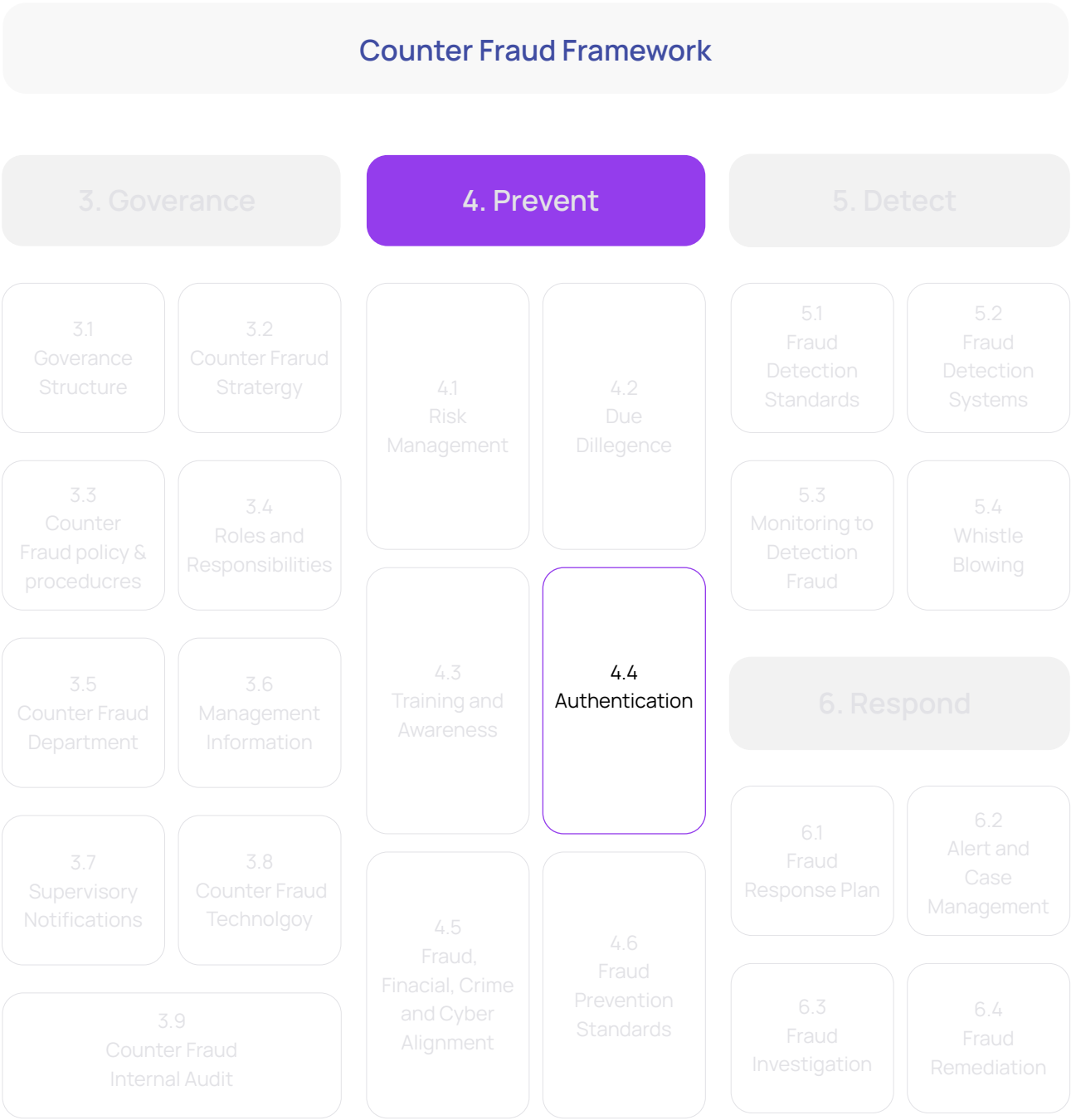
Strategic Advisory Services

- Advise on long-term fraud risk management strategies.
- Benchmark fraud prevention practices against industry standards.

From a governance perspective, our approach ensures that cyber counter-fraud programs are fully integrated into the overall corporate governance structure, with clear lines of responsibility, accountability, and reporting mechanisms extending from top management to operational levels. Our approach puts fraud risk management at the heart of your business strategy, creating a culture where protecting your organization is part of everyday decision-making. This way, fraud risk management becomes a shared concern shaping how your company operates and grows rather than being seen as another technical problem to solve.

Our methodology encompasses developing cybersecurity strategies, creating detailed roadmaps, formulating policies and procedures, and overseeing cyber risks. We incorporate industry-standard best practices tailored to specific regional, industry, and contextual requirements while ensuring alignment with corporate governance principles.

Authentication Across All Channels (CAF 4.4)



The CIAM platform combines authentication and access features with extensive contextual analysis and ongoing runtime prediction, prevention, detection, and response capabilities. It provides a versatile framework for managing end-to-end requirements, gathering, storing, and examining user context and session data to assess trust, predict risks, and implement immediate corrective measures.

Pre-Authentication

Gathers extensive contextual data, including:

- User location and IP address
- Device specifications and fingerprint
- Operating system and browser type
- Jailbreak or root status
- User profile details (if available)
- Device cookies
- Request headers
- Time of access

Uses this data to assess initial trust levels and potential risks.

During Authentication

Manages various user processes such as:

- Login
- Account creation
- Gradual profile building
- Transaction approval
- Self-service functions (password resets,account recovery)

Monitors authentication attempts

During Authentication Verifies user identity using collected contextual data.

Post Authentication

Continues to gather additional sigwnals, including:

- Number of authentication attempts
- Access time patterns
- Physical distance between user's device and multi-factor authentication method

Records all signals in the user's session.

Provides ongoing runtime prediction, prevention, detection, and response capabilities.

Informs downstream applications with collected data Implements immediate corrective measures if risks are detected.

CIAM combines authentication and access features with extensive contextual analysis throughout the process, providing a versatile framework for managing end-to-end requirements and maintaining user security.

Authentication Across All Channels (CAF 4.4)

- **Modern Web Protection**

Today's web applications demand flexible and extensible coarse-grained access control to ensure users can access what they need when needed and on their preferred devices. Access Management protects web applications, serving both consumers and your workforce. CIAM enables the creation of detailed policies for specific user groups, permissions, environments, and contextual conditions like time, location, and IP address. Access Management can easily integrate with various intelligence sources, allowing for more informed access control decisions. For seamless deployment, policies can be enforced using next-generation policy agents for Apache, nginx, and Java and Identity Gateway-based protection—additionally, native application calls via our robust REST/JSON-based API cover every resource in your environment.

- **Fine-Grained Authorization and IoT**

You can use the Access Management policy engine to safeguard custom and non-HTTP-based resources, including objects, data, and Internet of Things (IoT) components. The user-friendly design console allows you to create custom resource types effortlessly to protect what matters most. You can associate any action with any resource, such as "open" and "close" for a door or "on" and "off" for lights, and you're set. By applying environmental and contextual conditions, you can easily assign actions to the appropriate users, creating a simple yet powerful object-based protection system. The authorization policies can be enforced to enable rapid integration without requiring changes to the underlying system.

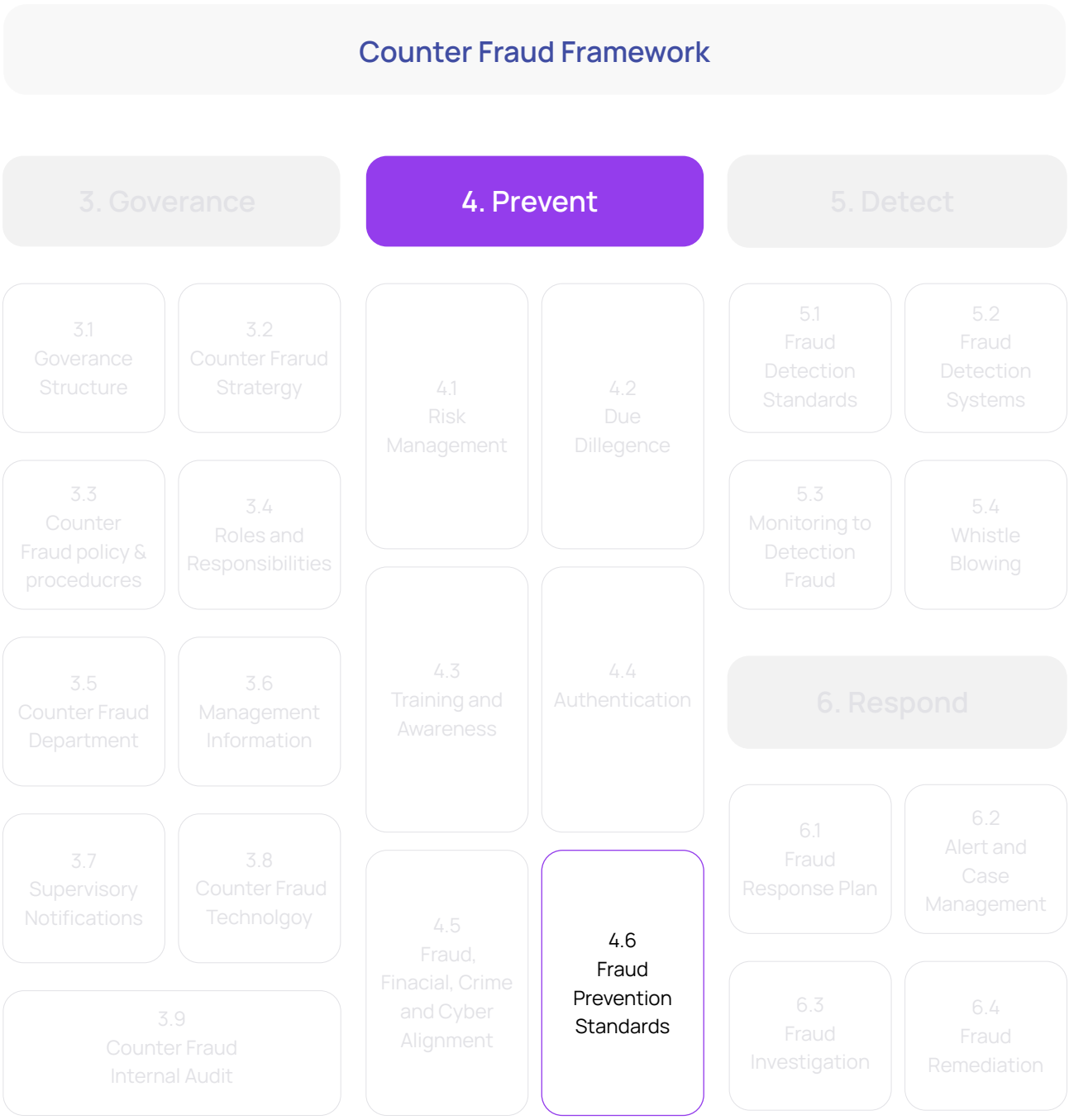
- **Standards-Based Authorization Using Oauth 2.0**

Modern applications, APIs, and microservices require standards-based approaches to authorization. The Access Management platf orm offers OAuth2 and OIDC provider and relying party (RP) capabilities. Whether issuing stateful or stateless JWT-based tokens, CIAM provides a variety of out-of-the-box and easily customizable flows and features to protect APIs and microservices at scale. Capabilities like Mutual TLS (mTLS), Client-Initiated Back Channel (CIBA), and Customizable Access Tokens deliver banking-grade security and flexibility. Advanced OpenID Connect (OIDC) identity tokens with customizable claims scripting extend functionality beyond standard token issuance. Application designers can use CIAM's out-of-thebox capabilities to transform any legacy application into an OAuth 2.0-compliant application, ensuring simple and scalable standards-based authorization.

- **Open and Extensible Authorization**

You can enhance the CIAM Authorization platform to address the most unique and demanding use cases. Despite the flexibility and power of the authorization engine, situations will always require capabilities beyond the out-of-the-box functionality. The CIAM Platform offers the necessary extension points, whether you need to integrate custom policy conditions, deliver additional entitlements and response data, or add extra fields and claims to OAuth2 Access Tokens and OpenID Connect identity tokens.

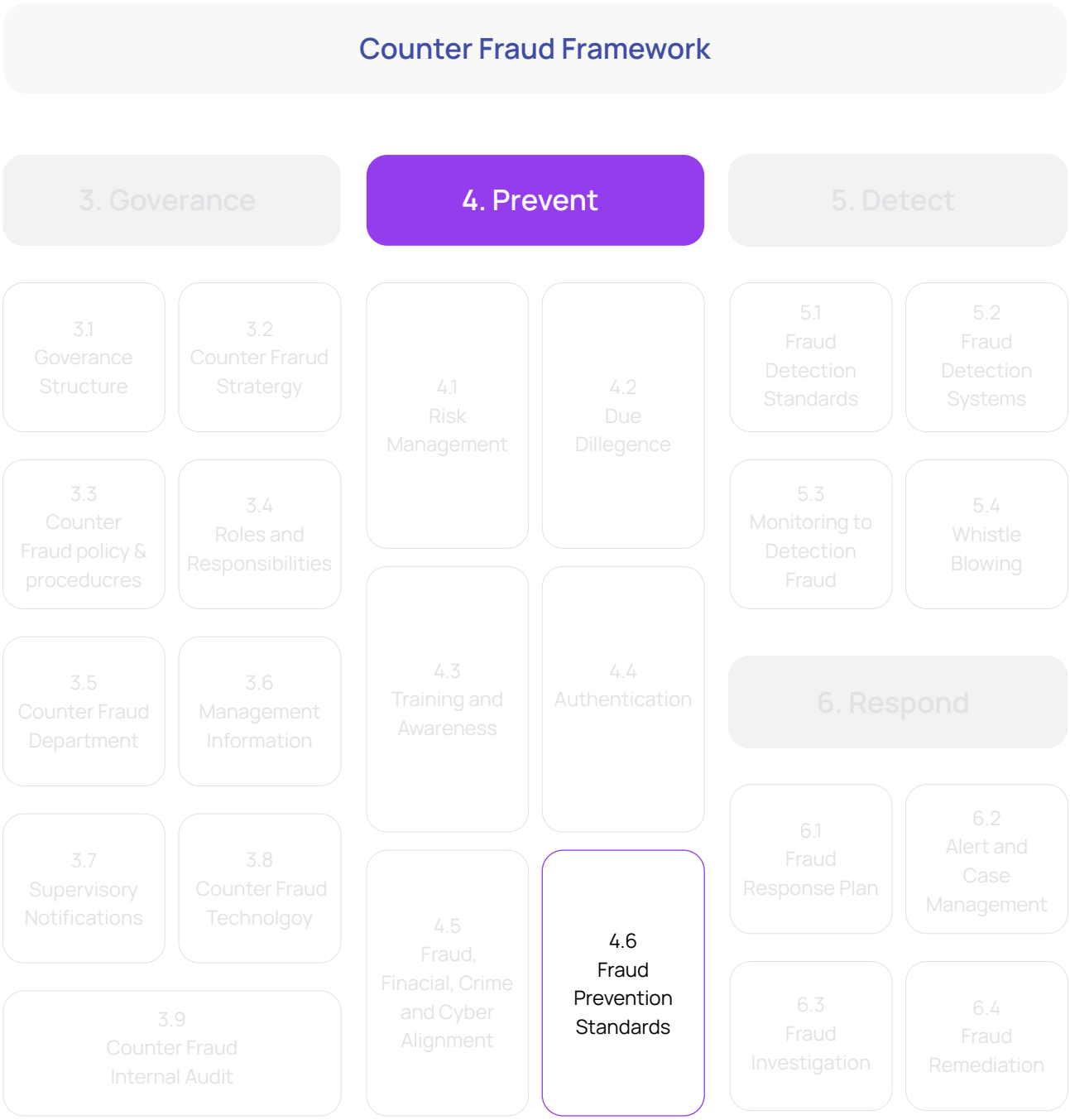
Zero-Touch Approach to Secure Resources (CAF 4.6.2)



- **Carta and Zero Trust Architecture**

The Access Management platform offers a range of capabilities essential for developing modern Zero Trust authorization architectures. Traditionally, application designers relied on network risk analysis to address security concerns, which was often inadequate in capturing the full context. The Access Management platform can combine identity and device information by capturing user and device context during login and at each transaction level, if necessary, and respond to contextual changes. By leveraging CIAM Authentication, the platform enables the storage, verification, and assessment of various contextual information to make more informed risk decisions. CIAM is the foundation for any CARTA or Zero Trust initiative, capturing and storing internal and external identity and device context. This information is either saved in the identity store or as ephemeral session properties and can be incorporated into web tokens, OAuth2 access tokens, or OIDC identity tokens. When tokens are used, the context is re-evaluated and compared to the context at login, enabling dynamic access adjustments. Any changes in context can trigger automatic throttling, data redaction, or access denial.

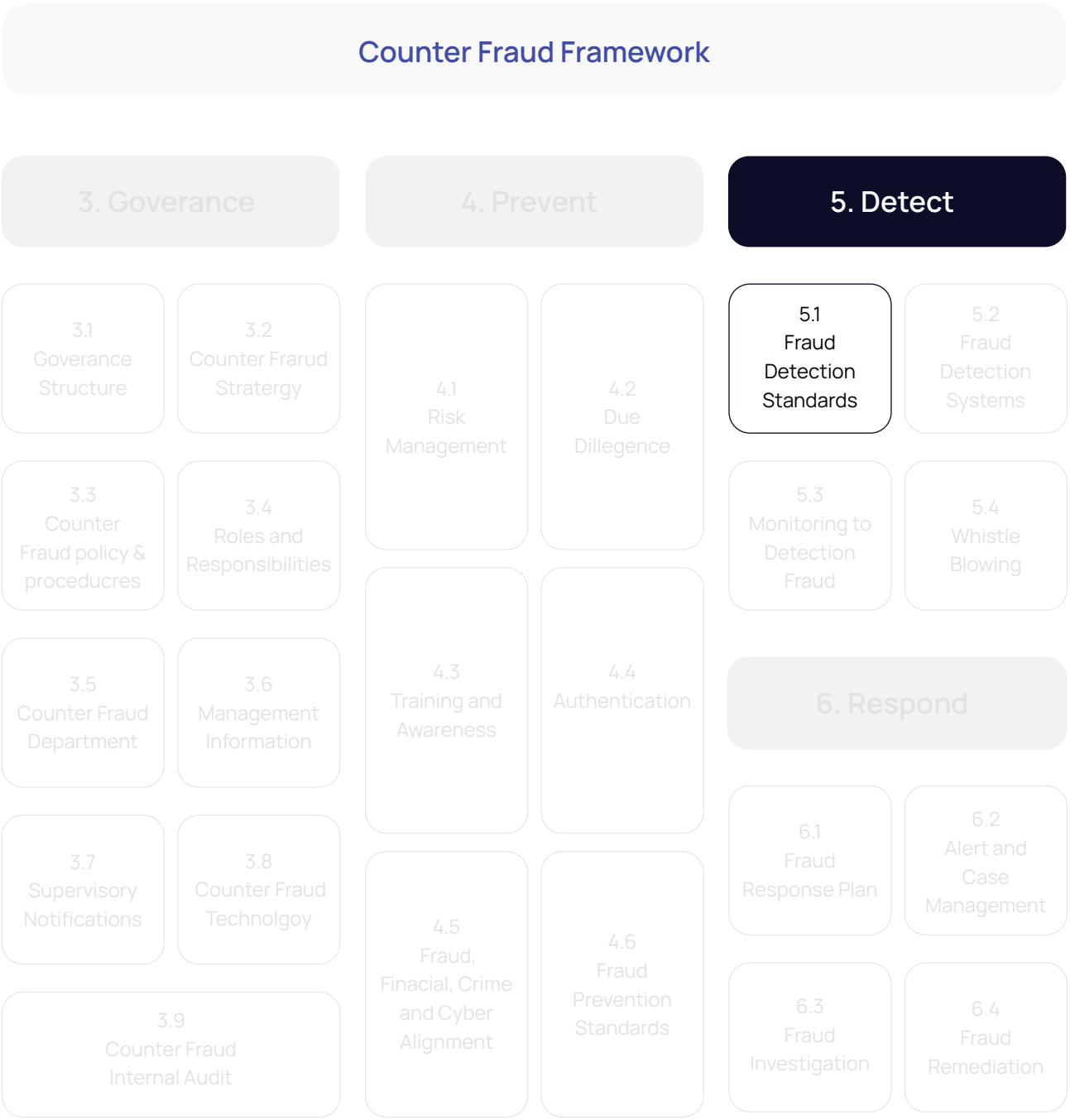
External Fraud Prevention (CAF 4.6.2)



CIAM is designed to prevent fraud and protect the customer experience by adapting to various threats. You can create CIAM user journeys tailored to specific threats, account types, and threat contexts. Here are some strategies to achieve this:

- Integrate a Google reCAPTCHA node into the registration process to require user input, thereby reducing automated and bot attacks.
- Enable step-up authentication and transactional authorization for activities outside a user's usual device, location, or behavioral context.
- Assign suspicion scores to user sessions, categorizing them as high, medium, or low risk, and redirect high risk users to a honeypot version of their intended destination.

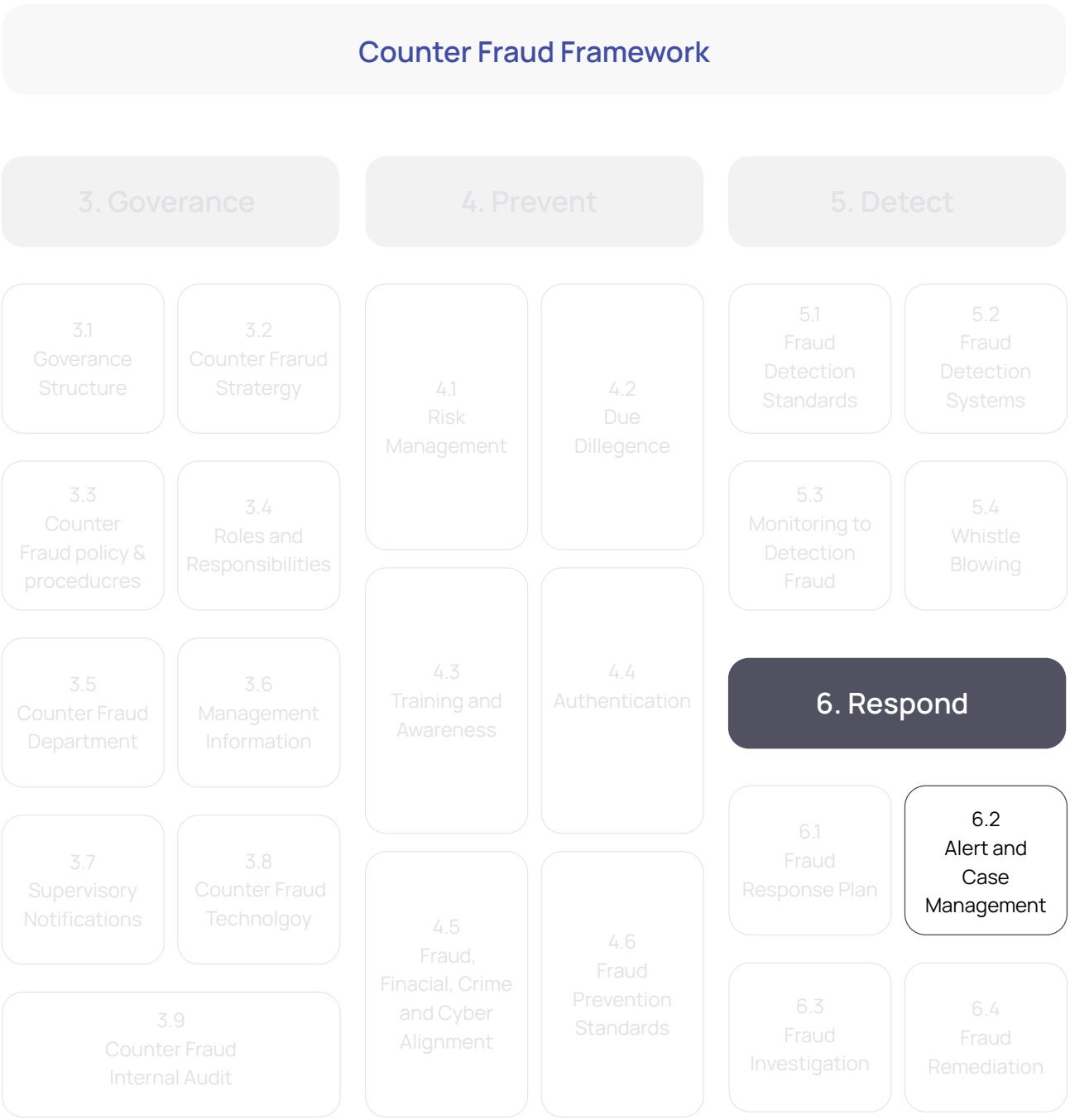
Abnormal Behavior Detection - Geo Localization and Adaptive Access (CAF 5.1)



Continuously Learning User and Device Context

CIAM can gather and store context, continuously learning more about your users. It can collect geolocation data, device information, and bot detection details. With this data, you can enhance security through identity proofing, fraud detection, and behavioral biometrics. This information is integrated into CIAM's native artificial intelligence and machine learning (AI/ML) capabilities. Additionally, you can easily create custom integrations using scripted or custom nodes.

Block Suspicious Transactions (Caf 6.2)



Remediating Fraud

If a suspicious user fails to re-authenticate correctly, your user journey can implement additional remedial actions. Here are some examples:

- Disable or delete the user's account
- Lock the account
- Force a password reset
- Send telemetry signals to other systems for further remediation

NuSummit Cybersecurity's CIAM for SAMA Counter Fraud Framework Compliance

The Saudi Central Bank's Counter-Fraud Framework emphasizes a proactive, integrated approach. By leveraging this guidance alongside CIAM solutions, NuSummit Cybersecurity can enable financial institutions to:

01 Develop a cyber anti-fraud strategy that aligns with enterprise-wide and operational risk and fraud management practices.

02 Identify and evaluate fraud by assessing threats, process vulnerabilities, and interdependencies.

03 Conduct risk and potential fraud assessments across various business functions, services, and IT assets.

04 Implement fraud scoring and ranking systems using both quantitative and qualitative methodologies.

05 Prioritize treatment based on risk level, consider compensating controls, and perform cost-benefit analysis.

06 Communicate fraudrelated information to relevant stakeholders and assign responsibility for mitigation efforts.

07 Monitor and report on treatment status and progress.

08 Automate the fraud management lifecycle using CIAM and other technological solutions.

09 Establish a Cyber Anti-Fraud (CAF) audit program, including documentation of critical performance and risk indicators for measurement and reporting.

Customer Identity and Access Management (CIAM) systems and comprehensive Access Management solutions offer a powerful framework to address modern fraud complexities. These solutions provide:

- Multi-factor authentication across all channels
- Standards-based authorization (OAuth 2.0, OIDC)
- Real-time risk assessment
- Adaptability to emerging threats

Investing in research, technology, and expertise is crucial for safeguarding Saudi Arabia's financial ecosystem and attracting international business. Implementing advanced fraud prevention strategies is imperative for stability and innovation. Embracing these solutions helps institutions stay ahead, meet regulations, and gain a competitive edge.

Glossary

- SAMA: Saudi Central Bank (formerly Saudi Arabian Monetary Authority)
- CFF: Cyber Counter-fraud
- CIAM: Customer Identity and Access Management
- KYC: Know Your Customer
- API: Application Programming Interface
- OAuth: Open Authorization
- OIDC: OpenID Connect
- JWT: JSON Web Token
- mTLS: Mutual Transport Layer Security
- CIBA: Client Initiated Backchannel Authentication
- CARTA: Continuous Adaptive Risk and Trust Assessment

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **cybersales@nusummit.com**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai
Mumbai I New Delhi I Bangalore

© NuSummit Cybersecurity Limited. All rights reserved.

All trademarks, logos and brand names are the property of their respective owners All company, product and service names used are for identification purposes only.Use of these names, trademarks and brands does not imply endorsementimply endorsement.

Follow us at: