Digital Government Authority
هـيـئـة الحكومة الرقمـيـة

Guideline of
Anti-Digital Fraud

December, 2025
Document Type: Guideline
Document Classification: Public
Issue No: 1.0
Document No.: DGA-1-2-5-232

Contents

01. Introduction

In its commitment to achieving its strategic objectives and supporting the objectives of Saudi Vision 2030, and in order to enhance the protection of government entities and beneficiaries from the increasing digital risks, the rapid expansion of digital technologies has highlighted the need for a clear and comprehensive guideline for Anti-Digital Fraud. This guideline aims to build trust between individuals and government entities by providing safe and efficient user experience and ensuring comprehensive protection against digital fraud.

The Digital Government Authority regulatory role in enhancing digital security by setting controls, standards, and guidelines that enable government entities to build the necessary capabilities and procedures to effectively combat digital fraud. In this context, the Digital Government Authority has developed the "Anti-Digital Fraud Guideline" to support the efforts of government entities in developing and improving practices for managing digital fraud risks. Anti-Digital Fraud requires a joint approach and cross-collaboration across entities and institutions. Therefore, government entities are encouraged to reach out to the DGA to jointly develop tailored solutions for specific issues.

Digital fraud is a dynamic issue that requires cross government and cross sector collaboration to solve. Often the cause of digital fraud and its impact take place on different digital perimeters. It is also a fast evolving and incredibly impactful materialization of risk, that leaves financial and psychological effects on its victims. To this end, this guideline document seeks to provide practical tools and recommendations to risk management practitioners and senior management on how best to structure their anti-digital fraud efforts and ensure that general societal effects are limited.

02. Guideline Objectives

This guide aims to support government entities in enhancing digital trust between government entities and their beneficiaries and reducing the impact of digital fraud, by achieving the following objectives:

01 Reduce the impact of digital fraud on digital government services to improve the level of digital government services and ensuring the provision of safer and more efficient services to beneficiaries.

02 Provide entities with the essential building blocks for developing digital fraud risk management frameworks, which contributes to improving its response to digital challenges.

03 Assist the adoption of essential anti-digital fraud principles and practices by all government entities in line with international standards and best practices, and enhancing their ability to efficiently address digital risks.

04 Enable a robust anti-digital fraud culture and enhance overall levels of risk management across services provided by government entities, to ensure the continuity of services and protect the public interest.

05 Contribute to the implementation of an effective methodology for managing digital fraud risks in government entities, which helps improve strategies for the prevention, detection, and handling of digital fraud.

06 Proactively engage in national digital fraud remediation efforts through collaboration with various sectors to activate comprehensive and unified strategies.

07 Enhance existing practices and frameworks and contribute to a more unified approach to digital fraud risk management, contributing to improving the level of protection and response to risks.

08 Raise awareness within the government sector about key digital fraud concepts and enhancing entities' understanding of the importance of Anti-Fraud and protecting the interests of beneficiaries.

03 Scope of the Guidelines

This guideline aims to guide government entities that provide digital services and products by offering the necessary guidance and recommendations to reduce digital fraud on their platforms. This guideline applies to all digital services and products provided by government entities, in addition, it considers the varying needs of different entities, allowing them to apply best practices in a way that enhances and ensures the continuous and efficient delivery of services. The guidelines includes three main pillars:

- Digital Fraud Risks: including the definition of digital fraud and the types of digital fraud risks within government entities. It also highlights the importance of digital fraud prevention efforts and clarifies its key features.
- Anti-Digital Fraud Governance: Which aims to assist entities seeking to develop or establish specialized functions for managing digital fraud risks.
- Anti-Digital Fraud Methodology: Includes a number of non-binding recommendations intended to guide government entities in using these recommendations to effectively manage digital fraud risks in a manner that suits their needs.

04. Target Audience

This guideline targets all government entities that provide digital services and products, regardless of their size and nature. The extent of the application of the guidelines depends on the government entity's portfolio of services and potential fraud risk exposure. The document is meant as a general guideline for risk management and fraud teams on how to structure and implement a potential approach to deal with digital fraud.

05 Digital Fraud Risk

5.1 Fraud definition

Fraud is a common phenomenon in business transactions. It is “an act of deception or misinterpretation committed by an individual or organization for personal gain, causing financial loss or harming others.”

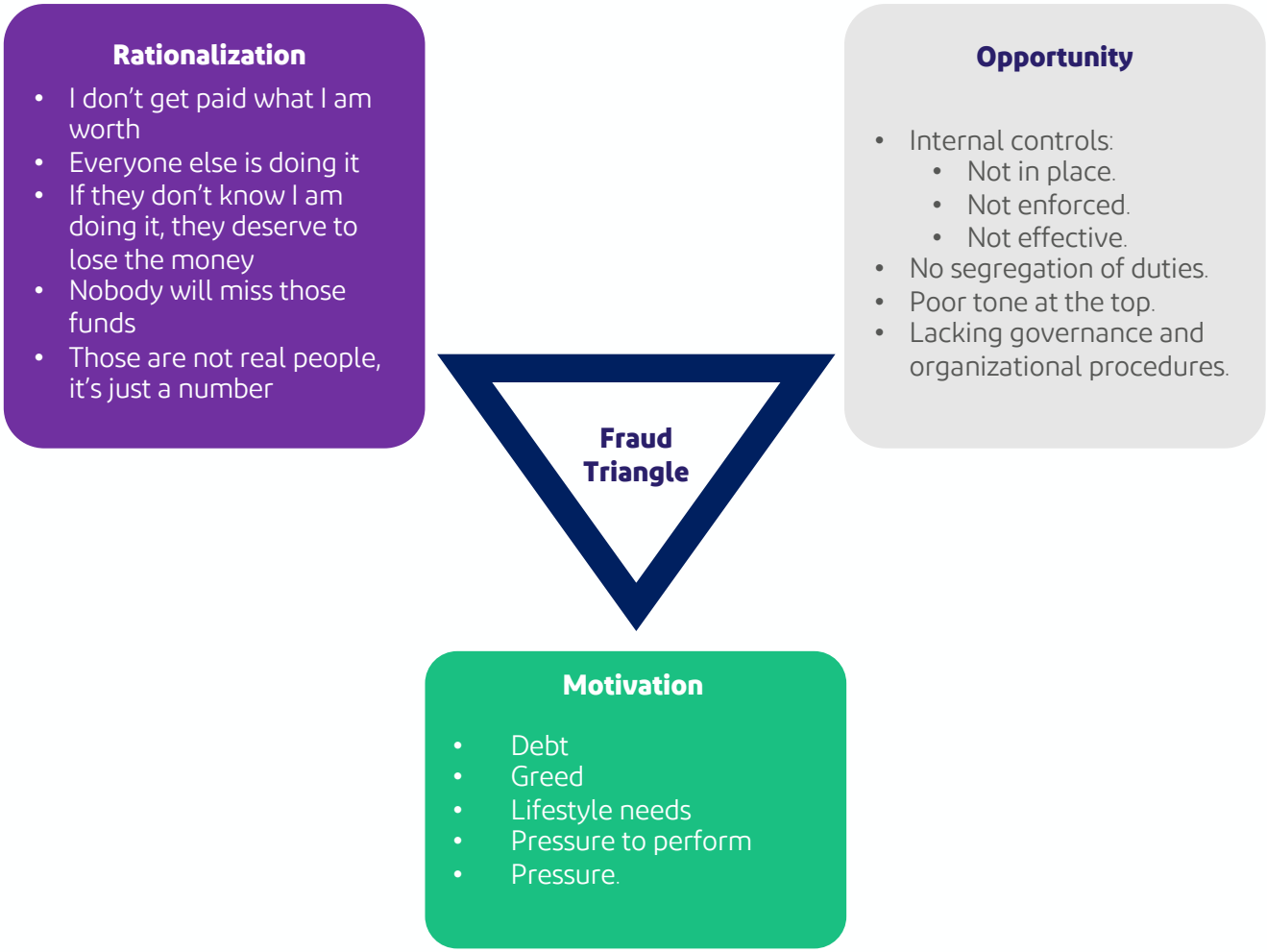


Figure 1 – Fraud triangle

Digital fraud is defined as any type of fraudulent activity carried out using technology or digital platforms. This type of fraud includes technical manipulation or deception to obtain material value or sensitive information through digital means. The above figure, “Figure 1 - Fraud Triangle," illustrates the main factors that contribute to fraud, which are rooted in three key elements related to human behavior and emotions. Fraud exists in both developed and underdeveloped societies, but it manifests in different ways[1].

ACFE Fraud Definition – Fraud Risk Management Guideline 2nd Edition.[1]

The "Fraud Triangle"[2] is an important tool when designing Anti-Digital Fraud frameworks and systems. It serves as a reminder that, despite its technical aspects, fraud remains, at its core, a threat driven by human motives. With the digital transformation that society has undergone, fraud has also evolved into a digital form. Digital fraud, sometimes referred to as electronic fraud or cybercrime, has emerged as a significant societal risk, with potential impacts that surpass those of traditional fraud. Since digital fraud relies on technological platforms to target individuals or entities, it spreads more rapidly compared to traditional fraud, which is often limited by the slower spread of its risks.

Digital Fraud Risk vs. Benefits of Digitalization

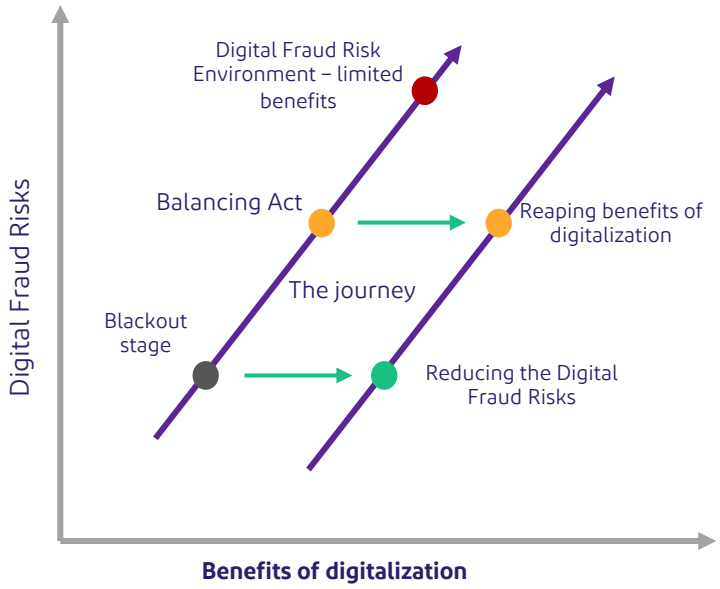


Figure 2 – Digital Fraud risks against benefits of digitalization

In contrast to traditional fraud, digital fraud anonymizes the victim and enhances all three ends of the fraud triangle because perpetrators are very rarely in vicinity of the victims. Additionally, criminal threat actors are very rarely caught, which increases significantly motivation due to the low likelihood of any adverse consequences to perpetrators. The digitalization of government services has brought increased accessibility and efficiency. However, it has also led inadvertently to an increase in digital fraud connected to these services. As services expand and become more digitalized the scope and opportunities for fraudsters expand as they are provided with a wider surface for exploitation. The figure above (figure 2– Digital Fraud risks against benefits of digitalization) highlights the various states that societies and organizations can find themselves in in relation to digital fraud risks as they increasingly digitize their own services.

Cressey – Other peoples Money: A study in the Social Psychology of Embezzlement 1953[2]
Figure is from BIS Research Paper on Digital Fraud[3]

The correlation between increased reliance on digital infrastructure and increases in digital fraud is well documented and below are several prominent examples.

1. Australia: The Australian Competition and Consumer Commission reported that Australians lost over AUD 851 million to scams in 2020, a (34%)[4] increase compared to 2019. This increase was largely attributed to the increased digital footprints and activity brought on by the COVID Pandemic. Investment scams, romance scams, and payment redirection scams were the most financially damaging.

2. **India**: Digital payment fraud in India has increased (five times)[5] due to the widespread adoption of the Unified Payments Interface in 2016. The widespread adoption of this national payment system as a part of core digital public infrastructure has changed the payment landscape and opened avenues of attack for fraudsters.

3. United Kingdom: The number of tax related scams where fraudsters impersonate HMRC has doubled in 2023 due to the introduction of digital service self-assessment returns. As many as (800,000)[6] scams were reported targeting individuals where fraudsters demanded payment based on fictitious digital self-assessments. The scams take different approaches. Some offer a rebate; others tell customers that they need to update their tax details or threaten immediate arrest for tax evasion.

The rapid pace of digitalization is only going to continue to increase and digital fraud as a social occurrence is going to continue to gain in prominence which is why it is essential that a documented, proactive and coordinated approach is in place to combat this risk.

Scammers capitalise on pandemic as Australians lose record $851 million to scams | ACCC[4]
How Fraudsters Exploit the Surge in Digital Payments and Online Banking[5]
Scams warning for 12 million Self Assessment customers | GOV.UK[6]

5.2 Digital Fraud Risk Types in Government Entities

There are several international taxonomies that relate to fraud risk and how it is meant to be measured, monitored and mitigated. All these taxonomies emphasize that by its nature fraud spans multiple dimensions and disciplines which make it a challenge to manage. The most mature fraud frameworks are currently present in the international financial sector due to fraud materializing effects in the financial services industry.

The Saudi Central Bank (SAMA) Counter-Fraud Framework defines Fraud as follows:

"Fraud is defined as any intentional act that aims to obtain an unlawful benefit or cause loss to another party. This can be caused by exploiting technical or documentary means, relationships or social means, using functional powers, or deliberately neglecting or exploiting weaknesses in systems or standards, directly or indirectly."

Although fraud is manifested primarily in the financial sector, government entities are also significantly impacted by fraud risks. In a digitalized society government entities carry out services including: payment, procurement, personnel management, and digital services administration. Therefore, the fraud risks faced by government organizations are largely like those of private sector organizations. As per the Committee of Sponsoring Organizations of the Treadway Commission [7] (COSO) [7] Fraud Risk Management Framework for the management of risk of fraud waste and abuse in government entities the below are listed as critical fraud risks:

- **Credit Fraud (loans and guarantees)**
- **Grants Fraud**
- **Logistics and supply chain fraud**
- **Purchase and travel card fraud**
- **Improper payment fraud (including vendor)**
- **Disaster relief Fraud**
- **Accounting Fraud**
- **Identity Fraud**
- **Asset misappropriation**
- **Financial Fraud**
- **Bribery and Corruption**
- **Procurement and Contracting Fraud**
- **Digital Fraud**
- **Healthcare Fraud**
- **Social Security Fraud**
- **Benefit Program Fraud**

[7] COSO ACFE Fraud Risk Management Guidelines Appendix G

Digital fraud can be considered a subset of general fraud – but when digital technology is used to perpetrate fraud this can also be considered a digital fraud as the control failure lies in the digital realm. Many of the above fraud risks could materialize via digital means and therefore they could be digital fraud.

Digital fraud is closely linked to cybersecurity incidents and regular fraud but there are some core differentiations. The Basel Committee on Banking Standards (BCBS) paper highlights these distinctions as per the figure below[8] (Figure 3 – Distinctions between Cybersecurity incidents and regular fraud). These distinctions are useful for risk management and reporting purposes. However, in an operational environment the lines between digital fraud, cybersecurity and conventional fraud will be blurred.

Differentiation	Description
 Remote/Virtual Access:	By its nature, digital fraud is committed remotely or virtually, which differs from internal fraud that requires physical access to an organization's system.
 Deception or Falsification	Digital fraud relies on deception and/or falsification to achieve its outcome. In this sense, it relies on the inability of an organization or its beneficiaries to appropriately distinguish a fraudster from a legitimate counterparty.
 Beneficiary Oriented	Digital fraud targets systems that are customer-oriented, as threat actors rely on high-volume campaigns to achieve a higher cost per attack ratio.
 Entity indirect role	Organizations can play an indirect and involuntary role in facilitating the transmission of digital fraud, being a processor of fraudulent transactions or user access requests.

Figure 3 – Distinctions between Cybersecurity incidents and regular fraud

BCBS -D558 reworded to suit government entity application[8]

5.3 Importance of anti-digital fraud efforts

Digital fraud poses a significant risk to technology users in the Kingdom of Saudi Arabia necessitating enhanced efforts to combat it. With the rapid digital development as per the Saudi Vision 2030, it has become a necessity to take effective measures to protect against it, particularly focus on vulnerable social groups.

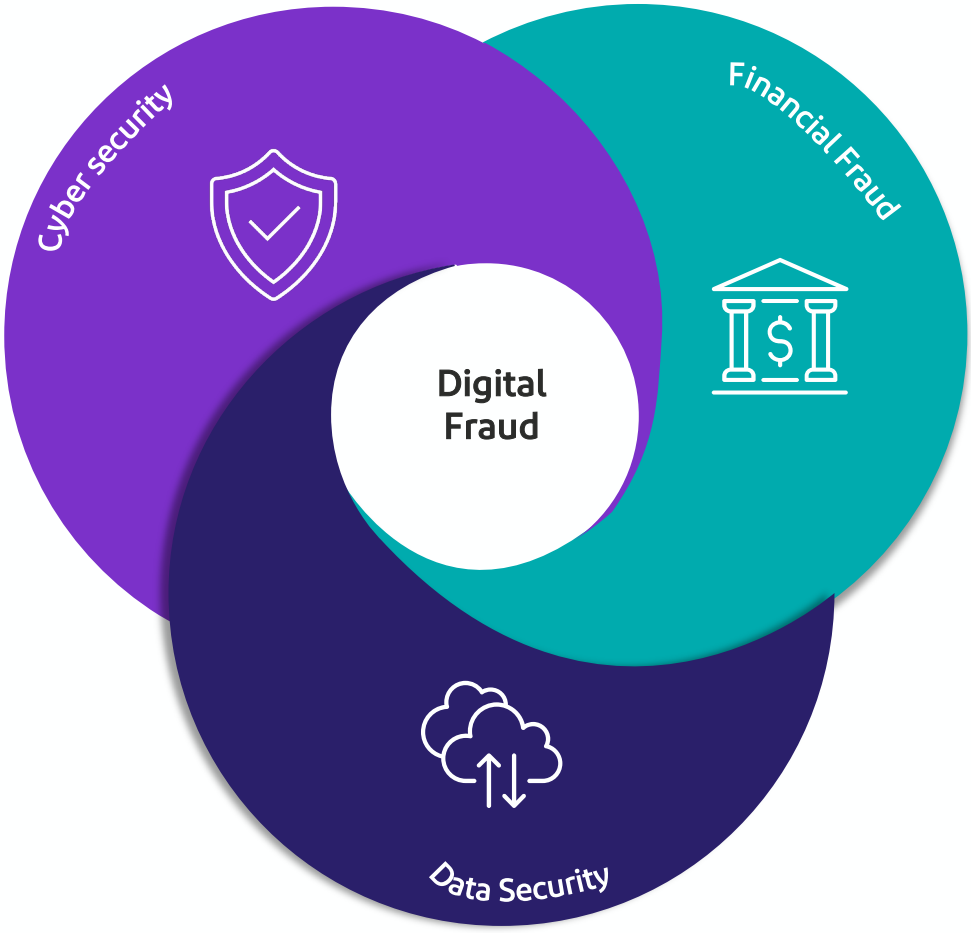


Figure 4 - Risk groups

Digital fraud is at the intersection of three recognized risk groups as per figure 4 (Risk groups), which makes mitigation a challenge Because digital fraud is at the intersection of multiple disciplines it is necessary to address it as a multidisciplinary risk. Controls for managing digital fraud often come from data privacy regulation and cyber security regulation while measuring metrics are derived from measuring the financial impact of digital fraud. This complexity makes the measurement of risk challenging, especially when complicated by the delineations between digital fraud and scams. Although they are related concepts, they have different mitigation procedures therefore they should be differentiated.

5.3.1 Digital Fraud:

Definition: Digital fraud refers to any fraudulent activity carried out using digital technologies or platforms. It involves: the use of technical compromise, or deceit to obtain something of value, often money or sensitive information, through digital means.

- Examples: Phishing attacks, identity theft, credit card fraud, account takeover, and fraudulent transactions conducted through digital channels.
- Characteristics: Typically involves unauthorized access, human errors, manipulation of electronic systems or data, and exploitation of vulnerabilities in digital infrastructure. Digital fraud often involves technical failures of internal controls.
- Mitigation: Better governance and a robust framework in conjunction with stronger technical controls, better detection software.
- Impact: Financial loss, data loss, operational downtime.

5.3.2 Scam:

Definition: Scams are deceptive schemes or fraudulent activities designed to trick individuals or organizations into providing money, sensitive information, or other valuables under false pretenses. Scams can occur through various communication channels, including digital platforms, but they may also involve traditional methods.

- Examples: fraudulent investment schemes, fake charities, scam parcels, and phishing text messages.
- Characteristics: Often rely on social engineering tactics to exploit human psychology and emotions, such as fear, greed, or compassion. Scams can target individuals, businesses, or even government entities. Scams can happen even when all internal controls have worked.
- Mitigation: Enhanced awareness raising for whole user population, national level infrastructure projects (e.g., Finnish Telco initiative).
- Impact: Financial loss for beneficiaries, reputational risk for KSA, emotional pain for beneficiaries.

Despite the rapid increase in cybersecurity incidents driven by digital technologies, digital fraud remains largely influenced by the fraud triangle, as outlined in the introduction. A proactive approach to digital fraud is essential for government entities to effectively manage, monitor, and mitigate digital risks. This requires providing necessary guidelines and continuously raising awareness, as digital fraud poses a significant threat to the security and integrity of government entities

The key threats that digital fraud presents to government entities include:

First, digital fraud reduces public trust in government entities, as it exposes weaknesses in protecting sensitive data and effectively managing resources.

The loss of trust can lead to reduced citizen engagement and compliance, hindering government operations and the implementation of public policies.

Second, as government entities manage vast amounts of citizens' personal data, they become prime targets for criminal organizations. The data held by government entities plays a crucial role in enabling digital fraud and deceptive activities. Digital fraud incidents affecting government platforms can result in identity theft and privacy breaches, causing severe harm to individuals and institutions.

Government entities are also key players in the digital fraud ecosystem, as impersonation of their identities, misuse of personal data, and exploitation of public digital infrastructure are often at the core of fraudulent activities. Therefore, they must take an active role in mitigating digital fraud risks.

As the regulatory authority and part of the second line of defense within the three lines of defense model, the Digital Government Authority has developed the Anti-Digital Fraud Guideline. This guideline aims to enable government entities to effectively manage digital fraud risks across their platforms. It provides practical recommendations Anti-Digital Fraud while encouraging entities to implement them in a manner tailored to their specific needs and circumstances.

5.4 Anti-Digital fraud characteristics

The core principles of Anti-Digital Fraud are closely linked to the characteristics of digital fraud. When developing a framework or an approach for Anti-Digital Fraud, the following principles should be considered:

Adopting a Multidisciplinary Approach:

To effectively combat digital fraud, government entities can adopt a comprehensive approach that integrates multiple disciplines to address the issue from various perspectives. Since digital fraud involves technical causes, financial impacts, and other negative consequences, experts from different disciplines should contribute to developing the Anti-Digital Fraud framework. This includes cybersecurity teams, Anti- Fraud specialists, operations teams, legal experts, human resources, and digital product design teams. The involvement of these specialists ensures a holistic approach to minimizing digital fraud risks.

The Role of Data Management in Anti-Digital Fraud:

Data plays a crucial role in mitigating digital fraud risks. Government entities should be encouraged to collect and analyze extensive data to identify trends related to digital fraud risks. To enhance fraud detection and prevention, it is essential to apply machine learning models and advanced modeling techniques. These technologies rely on accurate and comprehensive data, requiring government entities to explore innovative data-linking methods, such as correlating digital product usage rates with potential fraud scenarios.

Focusing on Beneficiaries and Employees:

Government entities should regularly train employees and educate beneficiaries about digital fraud risks, as fraud schemes are becoming increasingly complex. Awareness and training initiatives are fundamental principles that should be integrated into any Anti-Digital Fraud framework.

Flexibility and Adaptability:

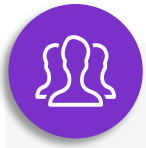
An Anti-Digital Fraud framework must be adaptive to evolving fraud risks. Given the rapid changes in this field, policies and controls should be regularly reviewed and updated. This approach ensures that government entities remain proactive and responsive to emerging fraud threats.

5.4.1 Key Characteristics of Digital Fraud

The following figure (Figure 5 – Core characteristics of Digital Fraud) illustrates the key characteristics of digital fraud:

Impact Across All Platforms

Since digital fraud represents a practical manifestation of risks, it intersects with multiple risk categories, making its prevention highly complex. Digital fraud risks often impact various domains, requiring a comprehensive approach to effectively mitigate them.



Rooted in Society

The practical execution of digital fraud inevitably adapts to societal traditions and customs. In most cases, criminal threat actors need to establish trust with their victims to carry out their schemes. This behavior may include imitating specific customs or exploiting known communication patterns in some societies to increase the effectiveness of the attack.

Targets Vulnerable Groups

Criminal threat actors target the most vulnerable individuals in society, as this type of exploitation is often more successful. This includes people who may lack technical knowledge or who are in difficult social or economic circumstances.

Rapid Spread

Digital fraud risks materialize instantly and escalate rapidly, as perpetrators typically exploit situations and vulnerabilities within processes or systems to quickly achieve their goals, making detection and combat increasingly complex.

Figure 5 – Key characteristics of Digital Fraud

5.4.2 Key Challenges in Anti-Digital Fraud

Anti-Digital Fraud is a major challenge, so government entities Should take these challenges into consideration when implementing anti-fraud frameworks to ensure that the system remains effective and able to adapt to future changes.

The most prominent challenges in Anti-Digital Fraud include the following:

The Volume of Fraud Incidents

The vast number of detected digital fraud incidents can overwhelm the analytical capabilities of fraud prevention teams, as criminals rely on high-frequency attempts to monetize their efforts.

Monitoring Societal Trends

Digital fraud prevention teams can monitor subtle societal trends that may enable or amplify the impact of digital fraud, which often becomes evident only after it is too late.

Advanced Fraud Risks

Digital threat actors employ advanced techniques such as service impersonation fraud, deepfake manipulation, and AI-driven social engineering tactics to continuously target entities and beneficiaries.

Balancing Fraud Prevention Efforts and User Experience

Digital fraud prevention teams struggle to find the right balance between effective fraud protection controls and user satisfaction, as excessive restrictions can sometimes cause more harm than the fraud itself.

5.4.3 Anti Digital Fraud Success Enablers

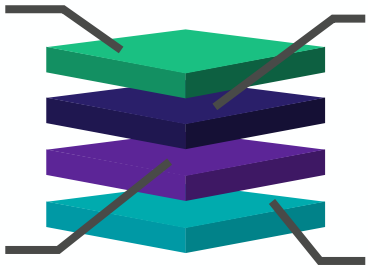
Developing an effective framework for Anti-Digital Fraud is a challenge, but it is not difficult or impossible. There are key steps that can be taken early on to enhance the effectiveness of the program and framework over the long term, and ensure success in combating these threats. The following figure (Figure 6 – Anti Digital Fraud Success Enablers) illustrates the ingredients for Anti-Digital Fraud:

Step 1: Risk Monitoring

Digital fraud and scam threats evolve rapidly as malicious actors adapt to new tactics. Therefore, it is essential for those responsible for managing digital fraud risks to rely on continuous monitoring rather than periodic checks to ensure effective tracking of emerging threats.

Step 2: Active Control Framework

Since digital fraud and scams pose evolving risks, control processes must be strengthened, adjusted, or replaced quickly to adapt to new threats. Dynamic control frameworks ensure effective management of emerging threats.



Step 3: Agility in Response

Rapid product development methods in government entities contribute to driving the necessary innovations to reduce digital fraud risks. The digital fraud management function should be involved in product development to ensure vulnerabilities are addressed and controls are strengthened within the process.

Step 4: Intelligence

A proactive data-driven approach focused on digital fraud can provide a strategic advantage for government entities in addressing these threats.

Figure 6 – Anti Digital Fraud Success Enablers

06 Anti Digital Fraud Governance

6.1 Framework Establishment

This section of the Guideline will outline the core elements that a government entity can use to build out its digital fraud risk management framework. Elements of the framework can be taken as standalone pieces, or they can be consequently implemented in a roadmap sequence. When developing its anti-digital fraud frameworks government entities are encouraged to consult national level frameworks for a better understanding of their potential risk and role in the digital fraud chain.

6.1.1 Policy

To ensure effective management of digital fraud risks, government entities can establish a clear anti-digital fraud policy, which is a key governance document in this area. Depending on the organizational context of the entity, this policy can be standalone, part of the overall anti-fraud policy, or an annex to the risk management policy. The scope of implementation of the policy is also determined internally at the entity level and its employees, or with parties external to the entity. The policy can provide a general framework and classification that helps stakeholders manage digital fraud efficiently without affecting workflow.

When developing an Anti-Digital Fraud policy[9], senior management should ensure that the policy:

1. Aligns with the entity's purpose: The government entity should assess its products and review actual digital fraud-related incidents to define the policy's scope. Accordingly, the document's objective should be clearly established and effectively achieved.

2. Identifies key stakeholders in the government entity: The entity should determine where digital fraud risks reside within the organization and designate responsible decision-makers.

3. Commitment to compliance with applicable recommendations: Timelines, cycles, and checkpoints should be established to ensure adherence to relevant control measures.

4. Provides a framework for setting Anti-Fraud objectives: Based on the policy's purpose, first-line controls within the (three) lines of defense can be established, ensuring the development of effective plans.

5. Defines principles for collecting digital fraud incident data: A clear definition of digital fraud incidents should be established, along with procedures for gathering information, including assessing the impact of incidents. [10]

6. Commits to continuous improvement: The policy should incorporate mechanisms to leverage lessons learned from incident reports and control failures, integrating findings into the development of new procedures.

ISO37003 Reference for basic policy principles that have been enhanced and adapted[9]
Potentially utilize impact matrix of Risk Management Guidelines[10]

7. Consequences for non-compliance with policy requirements: The policy may be assertively pro-digital messaging, with clear sanctions for non-compliance.

8. Exists as a documented and officially recorded policy: The policy should be formally documented and classified within the entity's risk management framework.

9. Is communicated across the entity: Inputs from cybersecurity, risk management, audit, and Anti-Fraud teams should be integrated to ensure comprehensive coverage of technical and procedural aspects.

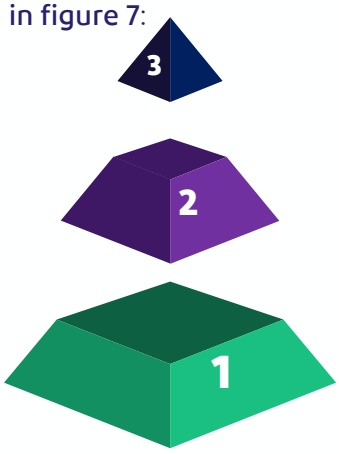
10. Is accessible to relevant stakeholders as needed: The policy should be made available to employees as necessary, emphasizing the importance of digital fraud risk management.

11. Is drafted in an appropriate tone and language for the government entity: The policy's style and wording should align with other officially adopted policies within the entity.

Government entities can choose to implement one or more of these guidelines when addressing digital fraud risks. The primary principle remains that the digital fraud risk management policy should comprehensively reflect the entity's needs.

6.1.2 Roles and Responsibilities:

Managing digital fraud risks[11] requires providing adequate resources, building capabilities and procedures to develop and improve Anti-Digital Fraud practices in line with the entity's organizational structure, taking into account the risks faced by the entity and its beneficiaries. Government entities can also adopt an approach that is consistent with digital threats, by distributing responsibilities in the three-line model, so that government entities adopt a model consisting of three lines of defense to facilitate the management and supervision of risks associated with digital fraud. This structure can be consistent with the requirements of the government entity, and the charter of roles and responsibilities can be based on the three-line model as shown below in figure 7:



- The audit function in the third line must oversee the entire process, conduct investigations after major incidents, and have full authority to investigate any matter at any time.

- Risk management teams in the second line are responsible for reviewing, challenging, and testing first-line control plans to ensure alignment with regulatory policies.
- Second-line risk management teams prepare management reports related to digital fraud.
- Second-line risk management teams provide support to the first line when needed.

- The responsibility for the first line of defense lies with product owners and business unit managers, who are accountable for managing digital fraud risks or scams.
- Product owners and business unit managers must implement first-line control frameworks and designated security measures to combat digital fraud or scams.
- Product owners and business unit managers must implement first-line control frameworks and designated security measures to combat digital fraud or scams.

Figure 7 – The three lines model

[11]The name of the digital fraud risk management unit may vary depending on the entity and its business requirements.

Digital fraud risk management falls under the second line of the three-line model of the organization, along with several departments such as (enterprise risk management, business continuity management, and cybersecurity management). While the three-line model is effective, the reality is that digital fraud risks can cross other lines. Therefore, roles and responsibilities can be flexible enough to adapt to the changing threat landscape. It is essential that the digital fraud function maintains close working relationships with other risk management functions due to the interconnectedness of digital fraud incidents, through careful examination, digital incident collection and mechanism, as well as an effective committee structure. The following figure (Anti-Digital Fraud in the three lines model) illustrates the position of digital fraud risk management within the three lines:

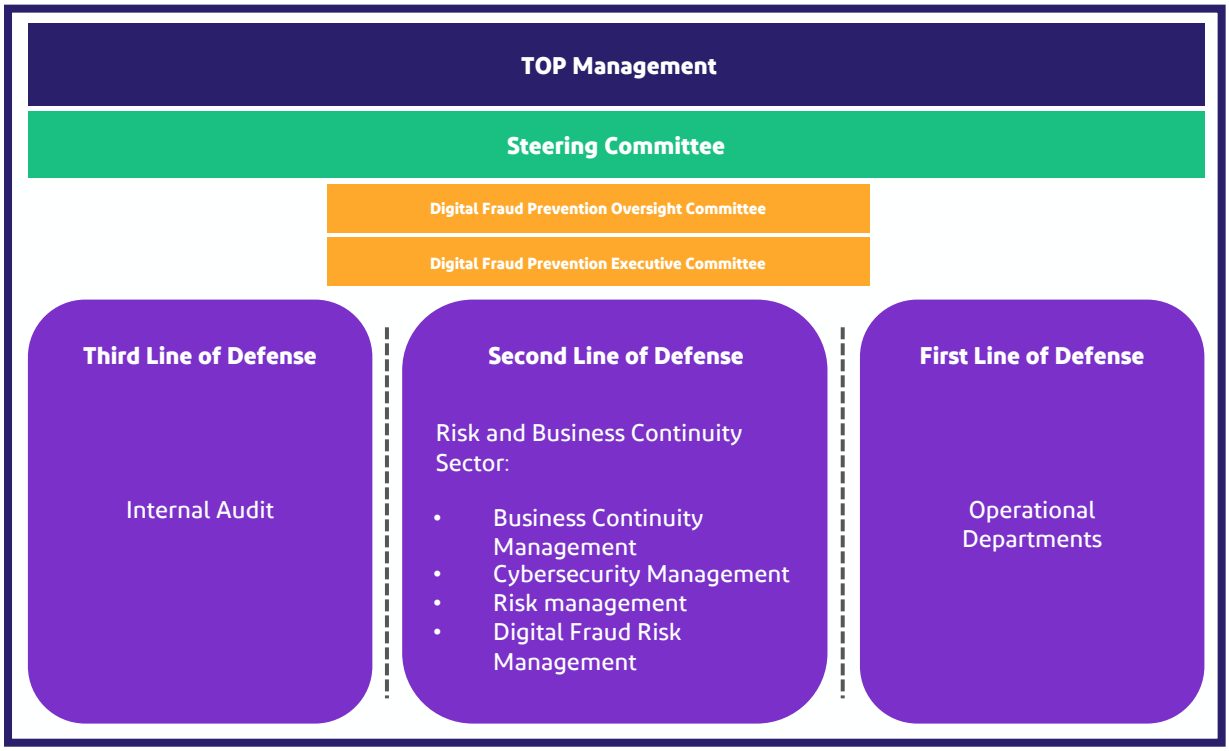


Figure 8 – Anti-Digital Fraud in the three lines model

As shown in table 1 below, the potential tasks and responsibilities for the first, second, and third lines of defense are outlined based on the methodology, phases, and lifecycle of digital fraud. These tasks and responsibilities serve as guidelines, and each government entity can develop a functional framework that aligns with its governance structure and risk exposure.

Stages of Digital Fraud					
Functional Role	1- Prevention	2- Detection	3- Response	4- Reporting	5- Continuous Improvement
First Line of Defense	1. Establish product-level controls to ensure that the risk of digital fraud on beneficiaries is minimized.	1. Responsible for detecting fraud on beneficiaries, products and related business units.	1. Responsible for coordinating efforts to respond to digital fraud incidents on the perimeter of the service/government entity.	1. Prepare regular reports on digital fraud incidents, trends, and risk exposure for review by risk management committees and senior management.	1. Develop and implement new and improved controls based on lessons learned from previous fraud incidents.
	2. Implement enterprise-wide controls to prevent digital fraud incidents.	2. Recording digital fraud operations in accordance with the procedures for collecting incidents and recording them within the incident collection system.	2. Charged with moving from investigation to incident.	2. Ensure that all digital fraud incidents and related activities are reported.	2. Ensure all employees understand their roles in preventing digital fraud.
	3. Provide beneficiaries with appropriate training and education to raise awareness of digital fraud.	3. Run its own technology toolkit and calibrate it to detect fraud on beneficiaries and internal systems.	3. Charged with modernizing, maintaining and complying with incident response procedures.		3. Regularly update and improve these controls to address evolving threats and vulnerabilities.
	4. Conduct risk assessments to manage and monitor digital fraud risks.		4. Organizational responsibility for each incident – and the one who takes responsibility for the incident in principle can always be in the first line.		
			5. Assigned to post-incident analysis and perform all data entry activities.		

Table (1) - Stages of Digital Fraud (First Line)

Stages of Digital Fraud					
Functional Role	1- Prevention	2- Detection	3- Response	4- Reporting	5- Continuous Improvement
Second Line	1. Increase monitoring to detect any residual risks or threats arising after the incident.	1. Determine incidents classification criteria.	1. Conduct a comprehensive assessment of the fraud incident to understand its scope and impact.	1. Ensure that reporting requirements are clearly aligned with business requirements.	1. Increase monitoring to detect any residual risks or threats arising after the incident.
	2. Foster a culture of continuous improvement by incorporating lessons learned from the digital fraud incident.	2. Determine verification levels when monitoring potential critical incidents.	2. Conduct root cause analysis to deeming how the fraud incident occurred.	2. Reporting as appropriate to senior management regarding the status of digital fraud risks.	2. Foster a culture of continuous improvement by incorporating lessons learned from the digital fraud incident.
		3. Enrich the initial intelligence flow with more insights.	3. Provide additional support to the first line entities during high level/high impact digital fraud incidents.		3. Oversee the intelligence loop and ensure that lessons learned are followed promptly.
		4. Immediate reporting of hazardous incidents.	4. Coordinating communications with senior management and relevant stakeholder.		
			5. Providing Passive supervision over the incident management procedures.		

Table (2) - Stages of Digital Fraud (Second Line)

Stages of Digital Fraud					
Functional Role	1- Prevention	2- Monitoring	3- Response	4- Reporting	5- Continuous Improvement
Third Line of Defense	Oversee all aspects of the process using a risk-based approach.				

Table (3) - Stages of Digital Fraud (Third Line)

6.1.3 Committee

The supervisory committee that is responsible for Anti-Digital Fraud:

To implement an effective framework for Anti-Digital Fraud, government entities can create or leverage existing supervisory committees and assign them key tasks to ensure adequate anti-digital fraud controls are in place. In principle, this committee could be a senior management committee comprising chief information officers, chief information security or cybersecurity officers, internal audit officers, and risk officers (or equivalent level officers) to discuss and make decisions on digital fraud risks. This committee could meet approximately twice a year.[12]

Key tasks of the supervisory committee:

Adopt Policies

Adopt policies and procedures relevant to Anti-Digital Fraud.

Develop Guideline

Adopting controls and guidelines to manage an effective Anti-Digital Fraud framework and evaluating the outcomes of implementing the policy (6.1.1).

Provide Supervision

Ensure oversight and supervision of the Anti-Digital Fraud framework within the entity.

Verify Resources

Ensuring that execution teams have sufficient funding and assets to achieve the framework's objectives.

Provide Advisory

Provide opinions on risk decisions, including accepting, mitigating, or rejecting risks.

The Supervisory Committee may assume full responsibility for implementing and ensuring compliance with all aspects of the Anti-Digital Fraud Framework.

Anti-Digital Fraud Executive Committee:

Each government entity can establish a subcommittee under the Supervisory Committee to manage Anti-Digital Fraud operations. This committee will hold regular meetings, typically once a month, and will oversee the operational and technical aspects of Anti-Digital Fraud. The committee can include specialists in cybersecurity, risk management, Anti-Fraud, data analysis, legal affairs, and compliance to ensure a comprehensive and adaptable approach to mitigating digital fraud risks. It may also have delegated authority from the Supervisory Committee to monitor and manage the operational aspects of digital fraud risks.

ISO 37003 Roles Responsibilities and authorities[12]

Responsibilities of Anti-Digital Fraud Executive Committee:

Oversee Execution

Monitor and direct the implementation of Anti-Digital Fraud plans.

Principle Implementation

Ensuring the integration of Anti-Digital Fraud principles into the design and workflows of products.

Assessment Management

Conduct periodic risk assessments for digital fraud.

Report Reviewing

Reviewing digital fraud risk reports, key risk indicators (KRIs), and primary risk management performance metrics in order to guide risk management.

Training and Awareness

Leading training and awareness efforts for beneficiaries and employees.

Incident Management

Handle high-impact digital fraud incidents.

Submitting Policy Recommendations

Submitting recommendations to the Supervisory Committee regarding digital fraud risk management policies.

Activity Coordination

Align and organize operational systems for Anti-Digital Fraud across most departments.

These responsibilities are indicative and not exhaustive of all possible activities. Each government entity (when needed) can design the structure of its anti- digital fraud executive committee to fit its governance procedures and risk management practices. In some cases, especially in entities with low exposure to fraud risks, such committees may be unnecessary or may constitute an operational burden.

6.1.4 Operations and Procedure

From a regulatory perspective, an Anti-Digital Fraud policy may include a set of integrated operations and procedures that support the overall framework. These operations and procedures can be incorporated within the current frameworks or developed as independent procedures and policy-specific documents. The appropriate implementation approach depends on the regulatory structure of government entities.

The table below outlines possible methods for updating frameworks, in addition to the references that government entities can establish or update to manage digital fraud risks.

Procedure (non-comprehensive)	Description	Independent Document	Integration into the Current Framework
Risk Assessment Procedures	A digital fraud risk assessment identifies vulnerabilities, and potential threats related to fraud in digital environments. Help government entities understand their exposure to risks, set initial mitigation priorities, and develop effective strategies for fraud risk reduction.	If the risk assessment process is documented as an independent reference, it should include at least the following sections: 1. Impact Assessment 2. Probability Assessment 3. Risk Matrix 4. Controls Mapping 5. Gap Analysis and Recommendations 6. in Action Plan	Digital fraud can be incorporated into the current risk assessments by adding a dedicated section or a set of fraud-specific risks questions. Additionally, government entities conducting broad risk assessments can integrate fraud risks as an additional category.
Investigation	The digital fraud investigation policy defines the necessary procedures to detect, investigate, and mitigate fraudulent activities in digital contexts.	If the digital fraud investigation process is documented as an independent reference, it should include at least the following sections: 1. Composition of the Investigation Team 2. Investigation Data Sources 3. Classification of the Investigation 4. Transition from Investigation to Incident 5. Post-Investigation Follow-up	From a procedural perspective, digital fraud investigations may require a specialized officer. If pre-established internal investigation procedures exist, they can be followed.

Table 4 - Possible Methods for Framework Updating

Procedure (non-comprehensive)	Description	Independent Document	Integration into the Current Framework
Incident Collection	Incident collection procedures include protocols for gathering digital fraud incidents. They help define how incidents should be collected, categorized, and classified, as well as determining the level of criticality—whether the incident is a crisis or not.	If the digital fraud incident collection process is documented as an independent reference, it should include at least the following sections: 1. Data sources for digital fraud incident collection 2. Linking incidents to operational procedures 3. Sub-Classification of digital fraud incidents 4. Incident cause 5. Incident impact 6. Data analysis	If digital fraud monitoring and detection systems are well-defined and a classification already exists, digital fraud (including relevant subcategories) can be addressed through existing incident collection procedures, provided these procedures are highly automated and mature.
Incident Management	Digital fraud Incident management procedures include steps to handle potential digital fraud incidents, containing the threat, eliminating its source, restoring affected systems, and conducting post-incident reviews to modify preventative measures.	If incident management is documented as an independent document, it must include at least the following sections: 1. Incident Management Team Formation 2. Incident Classification Matrix 3. Standard Incident Management Flow 4. Crisis Incident Management Flow 5. Remediation 6. Lessons Learned 7. Root Cause Analysis	Digital fraud, if well-defined (including relevant sub-categories), can follow previously defined incident management procedures provided that they are highly mature. (For example, Archer and ServiceNow incident management systems are in place).
Reporting	The reporting process can define key risk indicators and determine the data on which they are based. It is linked to the incident management policy and can establish reporting thresholds for risks while outlining regulatory changes in cases of threshold breaches.	If digital fraud risk reporting is documented as an independent reference, it should include at least the following sections: 1. Reporting requirements 2. Key risk indicators 3. Measurement methodology 4. Reporting periods 5. Linking reporting to risk tolerance levels 6. Protocols for follow-up reports	Reporting digital fraud incidents can be conducted as an independent process or integrated as a subcategory within existing risk management procedures.

Table 4 - Possible Methods for Framework Updating

6.1.5 Controls

The Anti-Digital Fraud Controls can be categorized from a digital fraud risk perspective according to the three-lines model:

First-Line Controls:

Technical Controls: Include technical rules designed by product owners and cover areas such as access controls, activity monitoring, and task separation.

Examples:

When registering a user for a new government digital service, government entities must ensure biometric indicators are collected.

Conducting daily social media scans through Automated Brand Protection Services to detect fake government platforms targeting beneficiaries.

Second-Line and Third Line Controls:

Supervisory Controls: Ensure the proper implementation of digital fraud practices within the entity.

Examples:

A government entity may have a defined classification for digital fraud risks that aligns with national strategic guidelines.

A government entity may have an approved incident response plan for digital fraud incidents.

When implementing the regulatory framework, it is essential to ensure that the framework is well-documented, systematically updated, and clearly understood by all relevant employees. Digital monitoring can be integrated within the broader regulatory oversight framework. When designing any type of monitoring framework, the principles outlined in ISO 37003 [13] regarding Anti-Fraud regulations can be considered.

These principles require the establishment of the following:

01

Risk-Based Controls

After identifying and assessing risks, corresponding controls should be established to mitigate them.

02

Continuous Improvement Process

Ensuring regular review and systematic updates of controls.

03

Controls Dissemination

Making controls accessible to all employees in alignment with their responsibilities and roles.

04

Ease of Access to controls

Ensuring employees can obtain the latest version through an efficient internal monitoring system.

05

Conducting Internal Audits

Including compliance with internal controls.

06

Leadership Commitment

The board and executive management should lead by example in adhering to regulatory oversight.

07

Enhancing Awareness

Educating employees on the importance of compliance to regulations, including linking compliance to controls with a regular performance review program.

Monitoring processes are fundamental to preventing digital fraud risks. They can be developed and utilized according to business requirements based on identified risks. There is no single framework that suits all entities; therefore, risk management leaders in government entities can determine the most effective methods for managing digital fraud risks in a way that aligns with their entities' needs.

[13] ISO 37003 Fraud Management Control Systems – Page 20

6.1.6 Identifying Potential Risks of Digital Fraud

Digital fraud risk falls within the intersection of legal risks, compliance risks, operational risks, and cybersecurity risks, making it difficult to define. Typically, the causes of digital fraud are classified under cybersecurity risks, although their impact often extends to operational, legal, and compliance risk categories. To accurately identify and assess digital fraud risks, it is recommended that government entities follow the risk identification methodology outlined in the Risk Management Guideline.[14]

Figure 9 –Methods for Identifying Risks

Risk identification efforts can be periodic and aligned with the main risk classification adopted by government entities or the classification of fraud risks mandated by the government. Risk identification efforts can also take into account the operational objectives of sectors and departments within government entities, as illustrated in the diagram above. One of the stages of identifying key risks is determining predefined major risks. Therefore, all digital fraud risk management efforts may originate from past incidents and investigations.

[14] Guidelines For Risk Management issued by the DGA

07. Anti-Digital Fraud Methodology

The methodology outlined in this section is designed for government entities to integrate Cyber Fraud aspects with the digital fraud risk management, providing a comprehensive framework focused on Anti-Digital Fraud. This methodology relies heavily on elements from various disciplines and should not be considered in isolation; rather, it serves as a complementary document within a broader national risk management framework. The following diagram presents a proposed methodology for anti-digital fraud.[15]

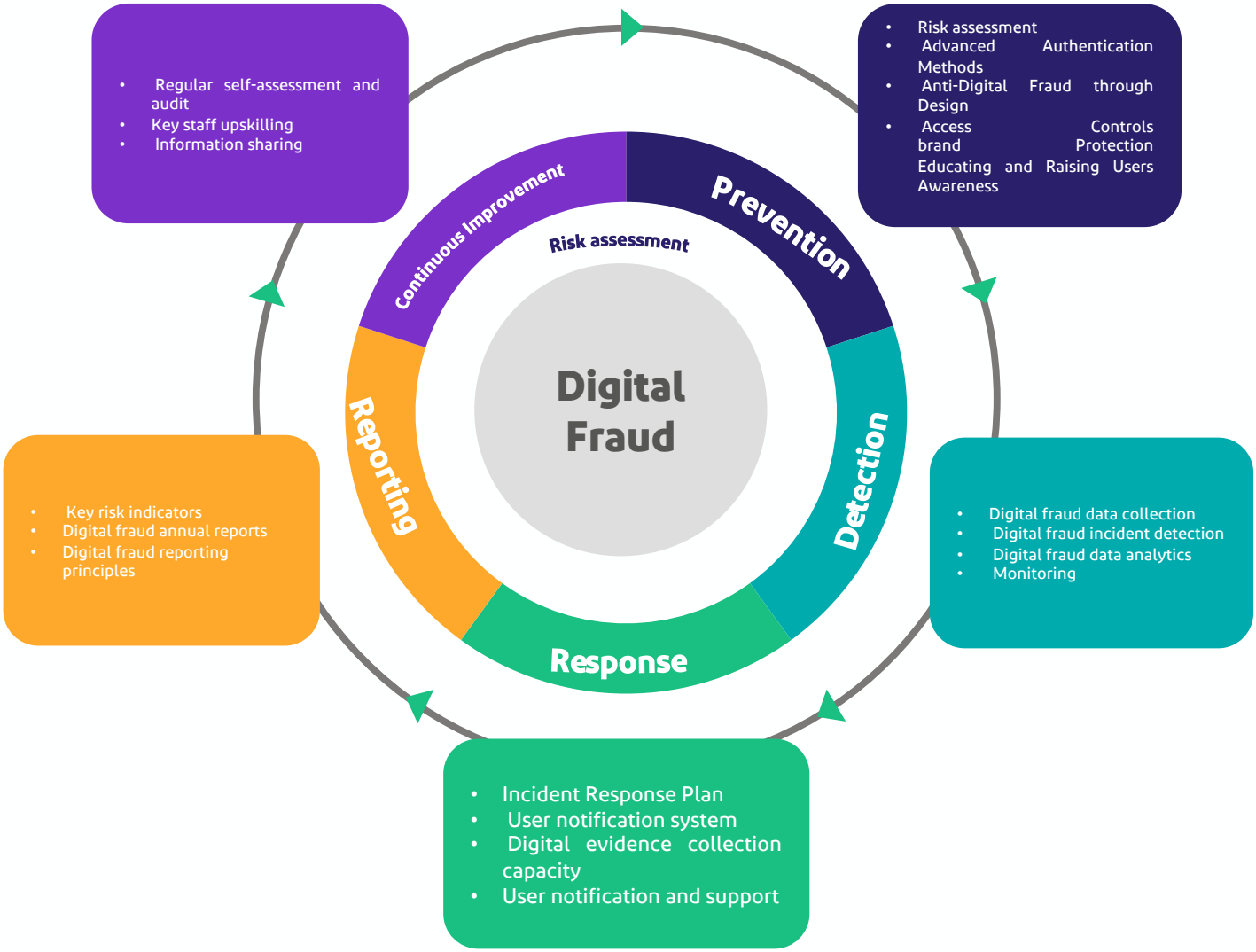


Figure 10 – Anti-Digital Fraud Methodology

The stages and recommendations mentioned in this methodology are merely suggestions and should not be considered mandatory. Each government entity can adopt recommendations based on its exposure to digital fraud risks and comprehensive service requirements.

Government entities are encouraged to utilize these recommendations for managing digital fraud risks effectively in a way that aligns with their specific needs and exposure to digital fraud risks and comprehensive service requirements.

ISO 37003 Fraud Management Control Systems[15]

7.1 Digital Fraud Initial Self-Assessment

Government entities can benefit from the initial self-assessment model provided in Appendix (A) to gain a better understanding of their current and future maturity in the field of digital fraud. This model aims to provide an indicator of potential risk exposure by assessing the elements of Anti-Digital Fraud framework, serving as a rich starting point for information regarding the likelihood of potential risks. Based on the extracted results, government entities can conduct a comprehensive assessment of digital fraud risks using the methodology outlined in the Risk Management Guideline issued by DGA. Additionally, the Digital Government Service and Business Disruption Risk Matrix can also be used to classify the provided digital services, helping to determine the level of service importance alongside the initial self-assessment results of the entity.

7.1.1 Defining Scope and Objectives

Government entities can define their scope based on their existing risk management practices and conduct an initial identification of the requirements for the Digital Fraud Initial Self-Assessment. When defining the scope, entities may consider the following factors:

You can find the Digital Fraud Initial Self-Assessment Model in Appendix A

Nature of Services Provided

Does the entity have identity services or services that use a large amount of personal or payment data?

Size

Does the entity service many beneficiaries?

Risk Materialization

Has the entity detected digital fraud incidents, or has a failure of its own systems contributed to digital fraud materializing in a different entity?

Likelihood and Impact

What is the chance of a digital fraud event(s) materializing, and what is the material impact that these events have had or will have?

Figure 11 – Scope defining considerations

The Digital Fraud Initial Self-Assessment aims to enable government entity leaders to quickly understand potential digital fraud risks and assess their entity's readiness to address these risks.

You can find the Digital Fraud Initial Self-Assessment Model in Appendix A

7.2 Prevention

Preventing digital fraud is not just a technical challenge; it is a strategic necessity that requires efforts to secure the entity's work environment. This includes implementing strong security controls, fostering a culture of vigilance and awareness, and staying ahead of emerging threats through continuous monitoring and analysis.

To implement effective fraud prevention strategies, government entities need to ensure that its approach includes the following:

- Risk assessment
- Advanced Authentication Methods
- Anti-Digital Fraud through Design
- Access Controls
- Brand Protection
- Educating and Raising Users Awareness

All these elements are integrated into the broader framework of Anti-Digital Fraud across various specialized domains, reflecting the complex nature of digital fraud and the need for concerted efforts of the entire entity. This guide aims to define specific areas within Anti-Digital Fraud efforts. It will refer to relevant frameworks that can assist in measuring and monitoring digital fraud risks. Government entities are advised to seek guidance from relevant domain frameworks and implement technical prevention controls according to their requirements.

It is recommended that risk management teams within government entities conduct risk assessments in collaboration with relevant stakeholders, such as risk representatives, operations teams responsible for risks, and others. Risk assessments serve as fundamental tools for preventing digital fraud risks, as they help identify areas where residual risks are concentrated at the institutional level, which may not always align with risk tolerance data.

7.2.1 Risk Assessment

Government entities' risk management teams are encouraged to conduct risk assessments in cooperation with relevant parties such as risk representatives, operations teams responsible for risks and others. Risk assessments are the foundational tools of Digital Fraud risk prevention as they indicate where residual risk is organizationally concentrated and potentially not aligned with risk tolerance levels.

Recommendations on Risk Assessment	
1 **Risk assessment**	A government entity may conduct annual digital fraud risk assessments to maintain a high level of risk awareness. It is recommended that the methodology stated in Section 6.2 of the DGA's "Risk Management Guidelines" be used to assess fraud risks.

As stated in Chapter 6.1.2 on roles and responsibilities with appropriate supervision from risk management specialists on the second line. Risk assessments can serve as the first line among the three lines. Additionally, results can be fully documented and provide an integrated framework for managing digital fraud, identifying the risks and controls needed to intensify efforts to prevent digital fraud risks. [16]

[16] NCA Essential Cybersecurity Controls Document

7.2.2 Advanced Authentication Measures

Advanced authentication methods play a crucial role in Anti-Digital Fraud by enhancing security and verifying the identity of users, transactions, or entities. This makes authentication a fundamental requirement for accessing system resources. The technical aspect of authentication is essential for all users interacting with products that effectively prevent digital fraud. Government entities can adopt one or more of the technologies listed below based on the significance of the digital government services they provide.

Government entities can adopt advanced authentication measures by referring to the regulations issued by the relevant government entities to ensure compliance with Anti-Digital Fraud design principles. This includes the regulations issued by NCA such as:
- Basic cybersecurity controls.
- Implementation guideline for basic cybersecurity controls.

Additionally, government entities can refer to the regulations issued by the Digital Government Authority to determine the importance of digital government services and define appropriate authentication levels accordingly.

Advanced Authentication	Description
Multi-Factor Authentication	Requires multiple verification levels, providing layered security against digital fraud. If one factor is compromised, additional security measures prevent escalation of criminal threats.
Behavioral Analytics	Determines access based on user behavior, such as browsing habits, download patterns, typing dynamics, and other metadata that contribute to detecting fraudulent activity.
Biometric Authentication	Biometric authentication is a verification technology that uses unique physical characteristics—such as facial recognition, fingerprint recognition, and iris recognition—to ensure accurate identity verification.
Token-Based Authentication	Physical hardware or digital software tokens can generate short-span time-sensitive prompt codes that can be used in conjunction with other login credentials to ensure user authenticity.
Risk-Based Authentication	Contextual risk analysis and evaluation ensure that a risk level is present during every login. Based on key risk data, additional controls in the form of accountability acceptance statements can be activated in product flows.

Figure 12 – Advanced Authentication Methods

Advanced authentication methods have become increasingly important with the development of search engines and artificial intelligence platforms. As impersonation attacks targeting high-profile individuals and senior executives become a tangible reality, modern technologies now require additional protocols, such as question-and-answer protocols, especially with the rise in incidents targeting key stakeholders through identity fraud techniques.[17]

Advanced Authentication Measures Recommendations		
2	**One or more advanced authentication measures**	Government entities should assess the criticality of their digital services, and based on the assessment apply one or more authentication measures as outlined in the DGA controls to categorize sensitive digital services and authentication levels.

With the increasing use of deep-fake technologies and sophisticated identity-based fraud techniques, the need to adopt advanced authentication principles has become more critical to ensure the security and reliability of digital transactions.

The key principles of advanced authentication include:

Principle	Description
Design Phase	Anti-Digital Fraud/Scam teams should be included in the design stage of products and systems builds. They should coordinate with design teams and cybersecurity teams in product design committees to ensure that systems and applications are built with sufficient protections.
Risk Scenario Usage	The Government entity needs to ensure that it has a set of digital fraud risk scenarios that it uses to test and benchmark their systems and applications through a project lifecycle. These services should be tested against all of these scenarios to ensure effective performance.
Fast Cycle Testing	Government entities should ensure that they continuously test existing systems, services, applications to ensure that anti-digital fraud measures work against digital fraud/scam risk threat vectors. Employ a rapid feedback loop to ensure continuous adaptation of protection measures.
Active Control Framework	Government entities should design products, systems and services so that the control environment can be enhanced based on incident reporting or risk intelligence. These enhancements should be instant in their application and can be added or removed based on risk exposure.

Figure 13 – Anti-Digital Fraud Design Principles

Appendix B Incident 1 – Ferrari NV Incident

7.2.3 Anti-Digital Fraud by Design

Adopting anti-digital fraud design principles is crucial for establishing strong, fraud-resistant internal systems within government entities while delivering secure products for beneficiaries. While these principles and methodologies cannot eliminate all forms of digital fraud, they contribute to enhancing product flexibility and security, resulting in a safer and more seamless user experience.

At times, Anti-Digital Fraud principles may conflict with certain aspects of the digital experience of beneficiaries, as they might require additional verification steps for the legitimacy of use. Therefore, government entities should determine the level of criticality of their beneficiary's engagement systems before determining the level of Anti-Fraud controls required for each product or system.

These principles should be tailored to fit the use case of the service or product and are best applied based on a risk-based approach. While these principles are neither comprehensive nor definitive, they are effective tools for designing and operating resilient services capable of countering digital fraud, their application should be assessed using the evaluation model provided in Appendix (C) to measure the effectiveness of anti-digital fraud measures within the entity. Additionally, a systematic roadmap should be developed for the structured adoption of these principles.

Anti Digital Fraud by Design Recommendations	
3 **Early Adoption**	Government entities should consider digital fraud scenarios in the stage of designing and developing new product whether these products are internal or beneficiaries-oriented
4 **Control Flexibility**	Government Entities should design their products and service with sufficient flexibility so that additional control layers can be added, if necessary, from a digital fraud/scam risk perspective.
5 **Interaction By Design**	Government entities should design their products and services with direct channels to beneficiaries so they can be notified of possible scam or fraud and so they can also report digital fraud when necessary.

7.2.4 Access Controls

Access controls are a critical element in enhancing the ability of government entities to combat digital fraud. Managing access for beneficiaries and internal staff to systems and applications is a fundamental measure in preventing digital fraud.

Criminals often rely on accessing and exploiting confidential data to gain financial or other advantages, which is one of the primary causes behind many digital fraud incidents. Therefore, government entities can ensure the implementation of adequate levels of access controls to prevent such occurrences.

Recommendations for Access Control		
6	**Implementing Access Control Methodologies**	Government entities can refer to the regulations to Identity and Access Management control tools from the National Cybersecurity Authority and develop effective access control systems.
7	**Privileged Access Management**	Government entities can ensure that the privileges of users with elevated rights are revalidated regularly, especially with regard to databases containing beneficiary data that may be exploited to commit digital fraud.
8	**Segregation of Duties**	Government entities can ensure the segregation of roles and responsibilities among relevant functions to prevent interference that could lead to the unauthorized exploitation of data.

When determining the appropriate access controls that can be implemented, government entities can refer to the basic cybersecurity controls issued by the National Cybersecurity Authority relating to Identity and Access Management in addition to the controls for classifying sensitive digital government services and verification levels issued by DGA. In establishing the level of implementation of these controls, government entities must collaborate with information and asset owners to identify the relevant information security and business requirements associated with access controls. [18]

[18] Article 5.15 Access Control from ISO27002_2022

Given that the presence of access controls is a preventive measure, it is essential for preventing digital fraud. It establishes protocols for verifying user access legitimacy and authorizing it, thereby reducing unauthorized activities and mitigating fraud risks. By implementing access control measures, government institutions ensure that access to sensitive data and critical systems is restricted exclusively to authorized personnel, thereby enhancing protection against breaches that could lead to digital fraud incidents.

From the perspective of preventing digital fraud, particular emphasis can be placed on restrictions for privileged access and the segregation of duties. Shortcomings in these areas may allow system exploitation by internal staff or compromised accounts. It is advisable for government entities to adopt the comprehensive access rights management principles outlined below to ensure effective prevention of digital fraud. [19]

The three most commonly used principles when designing access controls for product systems and applications are:

Need-to-Know: Beneficiaries, organizations, or individuals are granted access to information only if it is necessary for them to perform their duties.

Need-to-Use: Access rights to IT infrastructure are provided solely when there is a clear and justified need.

Principle of Least Privilege: Everything is considered forbidden unless explicitly permitted.

Furthermore, the implementation of access controls contributes to enhancing capabilities for digital evidence collection and activity monitoring, which serves as an important source for developing early warning indicators and tracking user behavior patterns. Studies have shown that institutions that implement effective access control strategies are less susceptible to digital fraud risks. Thus, access controls are a fundamental pillar of cybersecurity in reducing the damage caused by digital fraud and enhancing trust and the integrity of digital product operations.

[19] Article 5.15 Access Control from ISO27002_2022

7.2.5 Brand Protection

Brand protection is one of the fundamental practices for safeguarding employees and beneficiaries from deceptive fraudulent operations. According to the definitions provided in Section 5, fraudulent deceptive operations rely on deceiving the victim and their cooperation, with this fraud being closely linked to Brand impersonation. Criminal threat actors often attempt to impersonate well-known government entities to build a bridge of trust between the victim and the fraudster. [20]

Brand protection involves enhancing resources and strengthening safeguards to make exploiting a particular identity costly and unattractive to fraudsters. Since criminal actors seek profit, increasing the cost of their efforts may deter them from impersonating certain institutional or governmental identities.

Recommendations for Brand Protection		
9	**Brand Protection Guide**	Brand Protection Guide Government entities can adopt elements of the Brand Protection Guide according to their risk exposure and business requirements.
10	**External Monitoring**	Government entities can leverage external monitoring capabilities related to their brand.
11	**Brand Risk Assessment**	Government entities can conduct a brand risk assessment at least once a year to identify potential risks and protect their reputation from harm.

Brand Protection is a monitoring system that primarily focuses on external aspects and relies heavily on third-party technologies and monitoring mechanisms to detect fraudulent content used in deceptive schemes against beneficiaries. The challenge of protecting brand stems from the fact that such activities often occur outside the direct purview of the government entity, necessitating an active and comprehensive scanning process to mitigate the risks of misuse.

From the perspective of fraudulent deception, the misuse of brand by government entities includes the following:

- Copyright Infringement: Copying government images and logos without permission.
- Imitation Websites: Using an alternative domain to mimic the official government brand.
- Social Media Impersonation: Creating accounts that mirror the governmental or individual identity.

[20] See Appendix B incident 2 -Government Impersonation (USA) Case

- Ad Theft: Copying the brand's name or advertisement content in marketing campaigns.
- Bidding on Your brand: Presenting offers using keywords associated with a government identity.
- Domain Name Mimicry: Creating malicious online profiles that imitate the domains of government platforms with slight character alterations.

To implement an effective framework for brand protection, reduce digital fraud, and enhance digital trust, it is recommended that government entities adopt the elements listed below.

Domain Management

- Maintain continuous control over domain names associated with the government. To prevent unauthorized registration or use.
- Prevent domain name mimicry and hijacking through ongoing monitoring of domain registrations.
- Employ secure data transfer protocols, such as HTTPS, to protect users visiting government websites.

Content Management

- Implement a content approval process to ensure consistency and accuracy in digital representation.
- Review and approve digital content— including websites, blogs, and press releases— prior to publication.
- Address any unauthorized content that might harm the government entities or the reputation of the Kingdom of Saudi Arabia as a whole.

Brand Monitoring

- Develop clear policies and guidelines outlining how government entity identities should be represented online.
- Establish rules for using logos, typography, color schemes, and visual elements to ensure consistency.
- Ensure uniform brand across all websites, social media platforms, and other digital channels.

Collaboration Across Entities

- Collaborate with other government entities to exchange best practices and address challenges related to brand.
- Combat products or services that misuse the government entity's name.

Standardizing brand on Social Media

- Establish clear guidelines for social media profiles, cover photos, and profile pictures to ensure consistency.
- Regularly monitor official government accounts and promptly address any instances of impersonation or misuse.
- Educate employees on social media branding techniques to enhance protection.

Cybersecurity

- Protect against phishing attacks that exploit the government's brand by implementing effective preventive measures.
- Raise employee awareness of security risks related to emails and links that may impact brand.
- Collaborate with the National Cybersecurity Authority to secure government websites and prevent breaches.

7.2.6 Domain Management

Domain management is a critical aspect of preventing digital fraud as impersonation of defined government domains is a key technique utilized by cyber threat actors to establish trust bridges with beneficiaries to defraud them.

Organized criminal threat actors exploit all kinds of domain related vulnerabilities to deceive individuals and organizations with the goal of achieving unauthorized access to sensitive information and personal data. Top Level Domains (TLD's) are at the top of the list for cyber criminals who are looking to exploit legitimate websites of government entities to defraud users; to obtain their personal data, and to carry out credibility-based fraud attacks.

Some of the most common threads related to content management lifecycles are:

Domain Spoofing: Deceptive domains that closely resemble official government websites tricking users into submitting confidential information.

Typo Squatting: Registering domains misspelled words or using foreign languages (such as the Cyrillic alphabet).

Subdomain Takeovers: Badly managed or ignored subdomains can be exploited to host fake or fraudulent content or to distribute malicious content or info stealer malware.

Expired Domain Exploitation: Domains are not renewed and can be acquired by malicious actors and used for impersonation of fraudulent activities.

Open Redirect: Occurs when a web application unintentionally allows a (fraudster) user-controlled input to direct (victim) traffic to an external site. Allows attackers to redirect unsuspecting victims from legitimate (sa) sites to fraudulent pages.

Domain management is a fundamental aspect of national Anti-Digital Fraud efforts. By securing official domains, proactively monitoring fraudulent activity, and educating the public on identifying suspicious websites, government entities can significantly reduce the risk of domain-related fraud.

Implementing robust domain security measures and educating beneficiaries also will enhance trust in digital interactions and protect beneficiaries from digital fraud.

Domain Management Recommendations	
12 **Secure domain registration and renewal**	Government entities should adopt elements of the brand production framework as per their exposure and business requirements.
13 **Internal domain management and mapping**	Government entities should link all their internal and external domains and control and review them on regular basis to ensure the proper direction of traffic.
14 **Educating Beneficiaries**	Government entities should conduct frequent awareness campaigns to educate citizens employees and business about the risk of frequent domains.

Of special note is the cybersecurity aspect of domain management as entities should benchmark themselves according to the national related regulations and frameworks.

In addition, government entities are encouraged to avoid using links in text or email messages directed to beneficiaries. Instead, entities are encouraged to rely only on notifications from official applications and platforms affiliated with the entity. This aims to enhance the protection of beneficiaries of digital government services from the risks of fraud through suspicious or fake links.

7.2.7 User Education and Awareness

Efforts to educate and raise awareness among users are vital in Anti-Digital Fraud and deceptive misinformation on government platforms. These initiatives provide government employees and beneficiaries with the knowledge and skills necessary to identify, report, and effectively respond to potential threats. Given that digital fraud is inherently linked to human nature, enhancing individuals' ability to recognize digital fraud is essential. The diagram below illustrates a proposed methodology for Anti-Digital Fraud Training:

Figure (14) – Anti-Digital Fraud training

Comprehensive training programs educate employees on the latest phishing tactics, social engineering attacks, and other fraudulent activities. By understanding the methods employed by digital fraudsters, employees can recognize suspicious activities and take appropriate measures to effectively prevent digital fraud. Regular training ensures that all employees remain well-informed about new and emerging threats, promoting a proactive rather than reactive approach to Anti-Digital Fraud. Moreover, continuous training is essential for maintaining a robust defense against increasingly sophisticated fraudulent schemes day by day.

Internal Awareness Recommendations		
12	**Annual Training:**	Government entities can organize at least one online course per year on combating digital fraud, during which the main trends in this field are presented.
13	**Role-Based Training:**	Government entities can develop role-based training content tailored to the level of responsibility and role within the organization, ensuring that individuals receive the appropriate training to combat digital fraud.
14	**Risk-Based Training:**	It is essential for government entities to alert employees about the likelihood of increased digital fraud cases during peak times.

Public awareness campaigns are vital tools for preventing digital fraud, as they enhance the security of government platforms by educating beneficiaries on how to protect themselves against deceptive digital fraud schemes. These campaigns can include informational resources, workshops, and multimedia content to teach individuals how to identify fraudulent websites, recognize phishing emails, and maintain secure internet connections.

General Awareness Recommendations		
15	**Targeting Methodology**	Government entities should implement a targeting strategy to ensure that beneficiaries receive training and awareness initiatives tailored to appropriate demographic segments.
16	**Quarterly General Awareness Campaigns**	It is recommended to launch at least four general awareness campaigns annually, focusing on various fraud prevention topics.
17	**Integration with brand Protection**	Efforts to protect brand should be linked with general awareness campaigns. In cases of increased incidents of brand misuse, initiatives should be promptly launched to inform beneficiaries of significant developments.

By raising awareness, government entities can reduce the susceptibility of their platforms and beneficiaries to digital fraud and deceptive misinformation. An informed citizen is less likely to fall victim to fraud.

7.3 Detection

Government entities, regardless of their size or significance, can adopt proactive mechanisms to detect digital fraud. These mechanisms may be based on initial self-assessments of risk and general practices for verifying digital fraud.

Basic monitoring efforts include:

Digital fraud data collection

Digital fraud incident detection

Digital fraud analytics

Monitoring

Monitoring digital fraud is a key element in developing predictive risk models. It is an essential tool for fraud risk management and facilitates the design of more effective controls. Digital fraud monitoring heavily relies on data, and its effectiveness is tied to the maturity of fraud data processing activities.

Beyond being a data-driven practice, digital fraud monitoring aims to improve decision-making by providing concise information about fraud. Adopting an approach that focuses on timely and actionable data collection can empower decision-makers to effectively apply monitoring principles and strengthen prevention frameworks.

In the early stages of the monitoring process, government entities work on developing their capabilities to detect incidents after they occur. As analytics progress, the ability to identify incidents before they occur also evolves.

Monitoring activities include detection processes and procedures specifically designed to identify attempts at digital fraud—or actual fraudulent activities—in a timely manner, thereby mitigating the impact of any digital fraud that bypasses preventive controls.

7.3.1 Digital fraud data collection

From the perspective of digital fraud detection, data is the foundation of government entities' ability to detect digital fraud activities. This process involves collecting incident data and metadata that may indicate impending incidents, thereby enhancing the application of advanced measurement techniques and real-time processing, which leads to more efficient detection of digital fraud incidents. Data collection includes both internal and external sources, such as automated internal and external platforms, as well as reports from beneficiaries or employees.

Data is the cornerstone of digital fraud risk management, and a digital fraud risk management framework cannot be effective without the continuous collection of data from multiple sources. Depending on the activities and scale of the government entity, there may be various datasets that contribute to an improved overall understanding of digital fraud.

Potential Data Sources include:

1. The government entity and its internal systems
2. Users and beneficiaries
3. Third-party specialized Anti-Digital Fraud service providers
4. The general public
5. Other Entities
6. Regulatory bodies

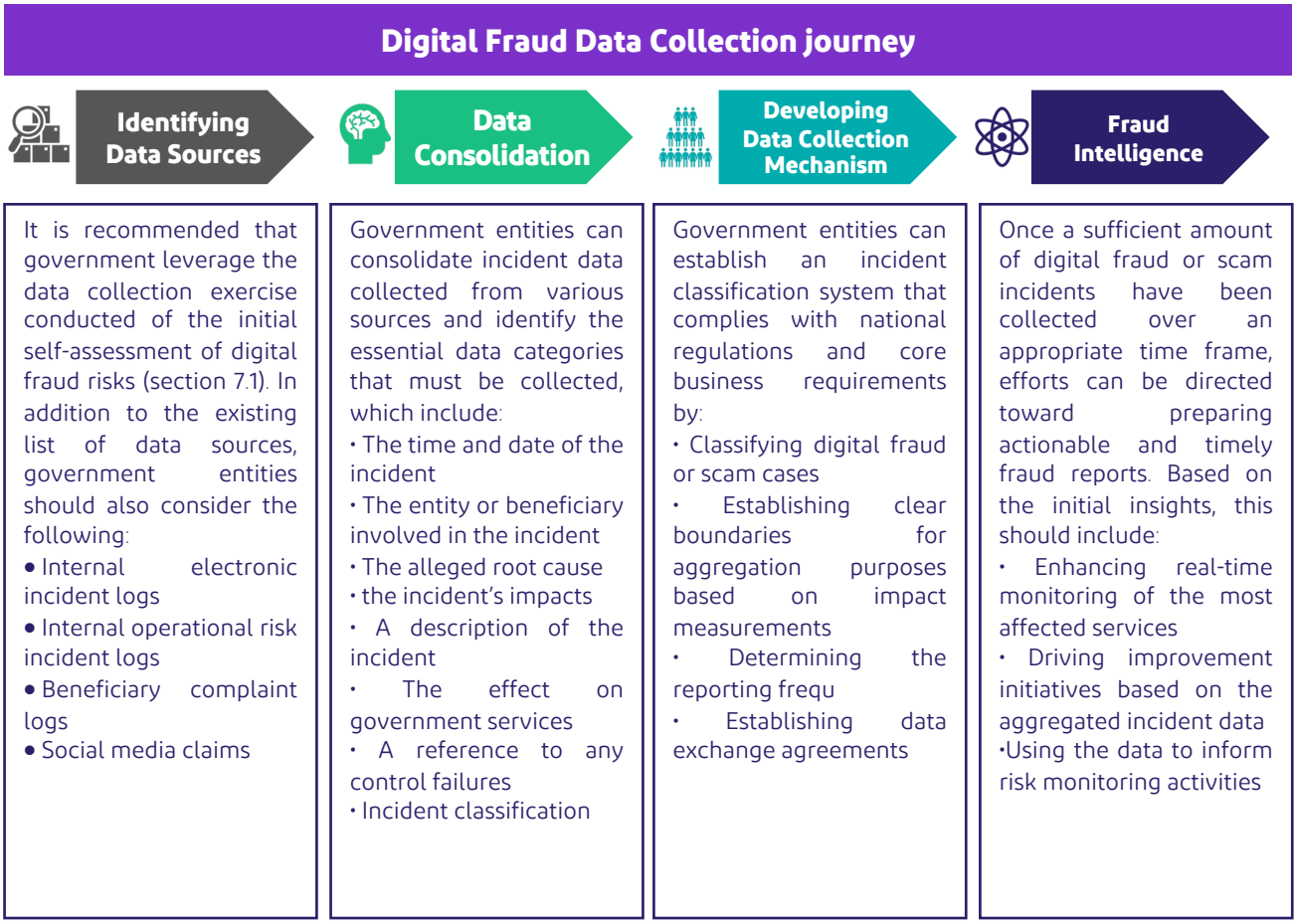
Types of Data That Can Be Collected Includes:

- User data
- System and network data
- Incident data
- Human resources data
- Brand protection information
- Complaints center data
- Geospatial data
- Law enforcement data
- Fraud monitoring alerts
- External information report
- Transaction data

(e.g., payment transactions or government services)

The extent of the data collected and how it is used depends on the digital fraud use cases faced by the institution. Below in figure (15) is the journey of collecting digital fraud data: [21]

ISO 37003 Roles Responsibilities and authorities.[21]



Figure(15) – Digital Fraud Data Collection journey

Through collecting data and conducting purposeful analysis, government entities can enhance their efficiency at all stages of digital fraud risk management and streamline digital fraud reporting processes. Based on data and its analytical capabilities, fraud intelligence can be developed to support proactive control activities when needed.

This approach will provide senior decision-makers with a clear view of how the organization responds, how its resources are optimized, and how to prioritize the most relevant risk management solutions. Government entities can establish an incident collection framework as the foundation for fraud monitoring efforts.

Creating a robust database of digital fraud incidents contributes significantly to facilitating control and monitoring activities. It is essential to regularly update and maintain this database to ensure it remains aligned with emerging events. The goal is to build a strong foundation that can be relied upon to create an effective database for incidents and investigations through the collection of relevant data. Once the datasets are consolidated, real-time fraud intelligence and monitoring tools can be applied to render the monitoring process predictive in nature.

Recommendations for Collecting Digital Fraud Data	
18 **Risk-based Data Collection**	Government entities should, based on a digital risk assessment, determine the minimum data required to be collected for managing their digital fraud risks.
19 **Process Standardization**	Government entities should strive to standardize the collected data into a format that can be utilized at the national level.

7.3.2 Digital fraud incident detection

Detecting digital fraud incidents is vital, as many such incidents go unreported or undetected. According to the Internet Crime Complaint Center (IC3) of the U.S. Federal Bureau of Investigation (FBI), 791,790 internet crime complaints were filed in 2020, resulting in losses exceeding $4.2 billion. However, digital incidents are often underreported due to factors such as victim embarrassment, lack of awareness, or the belief that reporting is futile. Some estimates suggest that only 10–12% of digital fraud victims report their experiences, meaning the majority of incidents remain undiscovered or unreported.

To address this issue, government entities can ensure that all employees and beneficiaries have the ability to report digital fraud incidents through official channels. Additionally, efforts should be made to raise awareness and encourage effective reporting of digital fraud cases.

General Awareness Recommendations		
20	**Internal Mailbox**	Government entities should establish an internal mailbox to enable employees to report cases of digital fraud.
21	**Direct Reporting**	Government entities should enable beneficiaries to directly report incidents of digital fraud or scams to the relevant authorities.
22	**Mandatory Reporting**	Employees must be required to report any suspicious digital fraud or scam incidents — even if discovered in the public domain.
23	**Incentives**	Incentives should be offered to encourage the reporting of digital fraud incidents.

Since victims may be hesitant to report, it is essential for government entities employees and beneficiaries to have a comprehensive understanding of clear reporting methods. This facilitates proper incident reporting and contributes to a more accurate measurement of digital fraud risks.

While employees and beneficiaries serve as primary sources for detecting digital fraud, many incidents are also uncovered through the cybersecurity monitoring tools of government entities or through specialized Anti-Digital Fraud platforms.

Once an incident is reported, it can be investigated in accordance with established procedures and standards, with clear indicators to determine whether the investigation has confirmed a digital fraud incident.

Recommendations for Digital Fraud Analytics		
24	**Investigation Process**	Government entities may adopt a defined investigation process for cases of digital fraud or deception, in line with risk management requirements and incident handling protocols.
25	**Incident Logging**	Government entities can record all digital fraud or deception incidents in a centralized repository, classifying them as digital fraud or deception incidents.

In addition to the required reporting by employees and beneficiaries, government entities can establish and utilize mechanisms to detect digital fraud, whether internally or through a third party. These mechanisms can be directed to encompass all data collected as part of data-gathering efforts, with particular emphasis on critical products to enhance the effectiveness of digital fraud monitoring.

7.3.3 Digital Fraud Analytics

Anti-Digital Fraud analytics leverages data science, machine learning, and artificial intelligence to identify patterns, anomalies, and trends that may indicate potential malicious activity. By analyzing large volumes of data and user behavior in real-time or near real-time, these tools can detect fraud attempts before they cause significant harm. Data analytics tools, including design data analysis testing, can be used to capture relevant indicators of digital fraud exposure. [22]

[22] ISO37003 – 8.3.5 Data Analytics

When baseline data and data collection procedures are available, government entities can apply data analytics to detect fraud, providing early warning indicators that contribute to an enhanced information cycle. Based on these indicators, government entities can develop accurate detection systems tailored to their operational needs and objectives, ensuring effective digital fraud monitoring, taking into account artificial intelligence applications and systems.

Digital Fraud Analytics Recommendations		
26	**Analytic Data Assembly**	Government entities should ensure that their data collection efforts are in line with national level capacities.
27	**Technology POC's**	Government entities with higher digital fraud risk exposure should conduct POC's to determine which technologies and third-party providers can assist in digital fraud mitigation.

Advanced fraud data analytics can include three alternative methodologies: [23]

1. Real-Time Analysis: Involves live data analysis within systems. This approach is used in banking transactions and payment systems, where the risk logging system immediately blocks suspicious transactions and accounts. Similar techniques are employed in anti-money laundering efforts.

2. Near Real-Time Analysis: This approach involves deploying solutions that monitor fraudulent activity almost instantaneously, enabling rapid verification of potential security threats.

3. Retrospective Analysis: This method analyzes previously collected data to identify fraud trends, enhance risk assessment, and adjust control environments accordingly.

The results of data analysis can be based on fraud intelligence principles to provide timely, actionable, and relevant insights for monitoring efforts and predictive intervention.

Government entities should leverage existing tools and technologies, integrating data analytics requirements with available national resources. Depending on the chosen strategy, collaboration with third-party service providers may be necessary to achieve the desired level of data analysis. Therefore, it is crucial to effectively define analysis requirements in line with the desired business outcomes

ISO 37001 Benchmark[23]

7.3.4 Monitoring

When establishing a successful monitoring framework for digital fraud detection efforts, government entities can adopt an oversight process based on controls and incidents. From a monitoring framework perspective, leveraging controls outlined in the National Institute of Standards and Technology (NIST)[24] framework is an effective method for continuous monitoring of digital fraud incidents. Since digital fraud and deception are often driven by cyber domain activities, these controls serve as robust building blocks for creating a consistent monitoring framework. It is recommended to integrate these controls into the digital fraud monitoring frameworks of governmental entities.

Security controls can undergo continuous review, with their performance compared against collected digital fraud incidents. This process enables government entities to assess the effectiveness of controls and determine if any adjustments are needed in the overall monitoring framework.

Strong building blocks are essential for establishing a consistent monitoring framework. It is recommended to integrate these controls into the digital fraud monitoring frameworks of governmental entities.

Continuous Monitoring:

- Continuous Monitoring 1: Monitor networks and network services to detect potential malicious events.
- Continuous Monitoring 2: Monitor the physical environment to detect potential malicious events.
- Continuous Monitoring 3: Monitor employee activities and technology usage to detect potential malicious events.
- Continuous Monitoring 6: Monitor the activities and services of external service providers to detect potential malicious events.
- Continuous Monitoring 9: Monitor the operating environments of hardware, software, and their data to detect potential malicious events.

Digital Fraud Monitoring Recommendations

28	**Compliance with National Monitoring Frameworks**	Monitoring efforts by government entities can align with national frameworks or relevant international standards.

Conducting periodic assessments of controls based on incident data can be a crucial indicator of their effectiveness. These assessments also help identify digital fraud risk gaps more accurately and efficiently. [25]

NIST – Continuous Monitoring Framework Controls[24]

ISO 37001 Framework On Monitoring and Measurement Activities[25]

7.4 Response

When responding to a digital fraud incident or campaign, immediate action is required by following established procedures supported by clear communication lines, with well-defined roles and responsibilities. During the response phase, the priority is to provide an organized approach to handle the incident, minimizing the overall impact on government entities and beneficiaries.

From a digital fraud perspective, the key elements that a government entity should have to ensure an effective response include:

• Incident Response Plan: Ensures clear steps for handling the incident.

• User Notification System: To inform affected beneficiaries and users about the incident.

• Digital Evidence Collection Capability: Ensures proper documentation of the incident.

Digital fraud response and recovery processes can follow the foundational guidelines of pre-existing risk incident response plans. Government entities should pay special attention to the unique aspects of digital fraud due to its significant impact and rapid spread. Additionally, it is essential to document as much data as possible, especially in high-impact digital fraud incidents.

7.4.1 Incident Response Plan

When preparing a digital fraud incident response plan, it is essential to clearly define the purpose and scope, specifying the tasks covered by the plan to isolate activities related to handling specific incidents rather than broader risk management.

Incident Response Recommendations	
29 **Incident Response Plan**	Government entities can integrate digital fraud into general incident response plans or create standalone plans based on business requirements.

Digital fraud incident response plans can follow a phased approach that includes the following steps:

01 **Preparation:** Emphasize the importance of proactive preparation, including regular employee training, incident simulations, and periodic updates to the response plan.

02 **Identification** Establish clear procedures for detecting and confirming a digital fraud incident, with steps for gathering initial information and accurately assessing the situation.

03 **Containment:** Provide clear guidelines for containing the incident to prevent further damage. This can include short-term and long-term containment strategies.

04 **Eradication:** Define the necessary steps to eliminate the root cause of the incident, such as revoking access for suspected users, shutting down affected services, or halting the use of compromised data and services.

05 **Recovery:** Detail how to restore affected services, implementing additional controls to prevent future fraud incidents.

When developing an incident response plan, it is crucial for government entities to heavily leverage the principles outlined in the guidelines for clearly defining communication lines for roles and responsibilities, as described in Section 6.1.2 of this guideline. Clearly defined roles in incident response are essential to ensure effective management of the response framework, especially given the time-sensitive nature of the response and the potentially significant impact of digital fraud incidents on government entities or beneficiaries.

In addition to having a clear response plan, government entities should ensure that their personnel are involved in digital fraud incidents receive appropriate training. This training should be aligned with the roles and responsibilities assigned to the staff, ensuring comprehensive coverage of all relevant aspects and the necessary level of detail.

7.4.2 Digital Evidence Collection Capability

Forensic analysis is a crucial step in understanding the origin, methods, and scope of digital fraud incidents. By examining digital evidence, such as logs, emails, and transaction records, digital fraud experts can reconstruct the sequence of events leading to the incident and more accurately identify potential residual risks. Digital evidence collection can be part of investigative procedures, ensuring that these procedures align with the government's comprehensive incident management framework.

Digital Evidence Collection Recommendation	
30 **Enabling Digital Evidence Collection**	Government entities can have the capability to record and collect digital evidence related to fraud or digital scam incidents.

This analysis contributes to understanding attackers' tactics and methods, enabling government entities to address security vulnerabilities and reduce the likelihood of future incidents. Forensic analysis also plays a crucial role in assessing the extent of damage caused by fraud, including identifying affected systems and data. It is an essential component of comprehensive incident response and the development of an effective recovery strategy.

7.4.3 User Notification and Support

User notification and support are critical success factors in the digital fraud response framework. Timely notification enables beneficiaries to take necessary actions, such as securing their accounts, monitoring suspicious activities, and seeking support from relevant authorities, thereby reducing the potential impact of digital fraud. [26] Therefore, quick and secure access to beneficiaries is crucial when dealing with or mitigating the effects of digital fraud incidents. [27]

User Notification and support Recommendations	
31 **Integrated Reporting**	Government entities can integrate user response mechanisms into a comprehensive digital fraud prevention strategy to, focusing on both proactive and reactive measures.
32 **Accurate Information**	Government entities can provide detailed notifications about potential fraud incidents, including the nature of the compromised data, potential risks, and recommended actions for beneficiaries.
33 **Two-Way Communication**	Establish channels for citizens to report suspected fraud, coupled with a two-way communication system to enhance the resilience of the national digital infrastructure.
34 **Embedded Functionality**	Notification and response processes can be embedded within the digital journey of government product offerings.
35 **Victim Support**	Government entities can provide necessary support to beneficiaries and employees affected by fraud.
36 **Information sharing**	To maintain data security, government entities should avoid sending sensitive data or digital platform references through SMS or unencrypted communication channel.

By integrating user notification and response processes within a comprehensive Anti-Digital Fraud framework, government entities can reduce the direct impacts of fraud and enhance public trust in digital services.

[26] See Appendix A – Initial Self-Assessment of Digital Fraud Risks
GDPR mandates that citizens need to be notified of an incident regarding their data without undue delay[27]

7.5 Reporting

To ensure effective reporting, government entities should establish well-known reporting channels, and frontline teams should be able to send incident reports to a centralized repository, such as a (Digital Reporting Service). A robust data architecture will enable the creation of management reports that support strategic decision-making regarding resource allocation for Anti-Digital Fraud.

When designing the report structure, the following key principles can be followed:

1. Properly record all digital fraud incidents across all organizational units.

2. Investigate all suspected fraud incidents and use the investigation results as a basis for action.

3. Identify vulnerabilities in internal controls.

4. Take corrective actions to address weaknesses in internal controls.

Collecting this data enables senior management to manage digital fraud risks more effectively. These principles also help build a set of Key Risk Indicators (KRIs) that can be used as predictive tools to avoid risk exposure. These indicators can be regularly monitored to ensure that senior management takes appropriate preventive measures and effectively mitigates damages.

7.5.1 Key Risk Indicators (KRIs)

Key Risk Indicators (KRIs) are essential tools that act as early warning systems, alerting users to potential negative consequences of risks. They play a crucial role in risk management by helping assess the effectiveness of existing controls and estimating the likelihood of risks. KRIs are characterized by their ability to measure, predict, and compare, and any changes in them should be regularly reported, analyzed, and monitored to ensure an effective and appropriate response.

Examples of Key Risk Indicators for Potential Digital Fraud:

KRI	Description
Monitoring critical periods for digital fraud incidents.	It is essential to understand and monitor numbers of digital fraud incidents in high interaction periods to be able to deploy active controls.
Erroneous access requests for digital government services.	Increased numbers of erroneous access requests can serve as an indicator of platform product or service compromise that can lead to digital fraud.
Global Trend Monitoring	Monitoring digital fraud international trends as it is mostly external criminal threat actors targeting government entities and beneficiaries.
Number Of Digital Fraud Incidents	According to incident collection data the overall number of digital fraud incidents is a critical risk materialization indicator.
Number of Scam Incidents	Number of scam incidents recorded in a quarter or similar measurable period to assess their prevalence.
Ratio of brand protection incidents Successful/Unsuccessful	Ratio will showcase the effectiveness of brand protection efforts for a government entity.
Number of beneficiaries defrauded	Determine the number of individuals impacted.
Amount of funds defrauded	Estimated amount of funds defrauded from beneficiaries.
Number of significant cyber security incidents	Significant cyber security incidents like data breaches can lead to digital fraud and they should be monitored.

Table 5 – Key Risk Indicators

7.6 Continuous Improvement

Continuous improvement in digital fraud risk management is essential as it enables government entities to anticipate evolving threats and adapt their strategies accordingly. Digital fraud trends and patterns change rapidly, posing a significant challenge for all entities. Given the potentially significant impact of digital fraud risks, maintaining a static risk management approach is insufficient. Therefore, continuous improvement can serve as a key focus area to drive effective risk management efforts.

7.6.1 Periodic Self-Assessments and Audits:

Government entities should ensure regular self-assessments and audits of digital fraud risks to maintain effective monitoring and adapt fraud mitigation measures across all aspects of the organization. Internal audits play a critical role within the comprehensive risk management framework, and integrating digital fraud risks into their evaluations is a strategic necessity for government entities exposed to high levels of these risks.

Self-Assessment Recommendations and Audit Processes	
37 **Regular Assessment Log**	Government entities can set a schedule and frequency for self-assessment and audit cycles within their digital fraud risk assessment.
38 **Integration with Audits**	Government entities can leverage existing audit frameworks and expand their scope to include assessment of digital fraud impacts.
39 **Integration with Planning**	Government entities can integrate digital fraud assessment results into their strategic planning for risk management activities and develop appropriate action plans to address these risks.
40 **Culture of Evaluation And Accountability**	Government entities can promote a culture of transparency and accountability by ensuring the clarity of audit results for all stakeholders and effectively following up on the implementation of recommendations.
41 **Integrated Feedback Loop**	Government entities can implement feedback loops from audits processes, incident responses, and employee training program to continuously improve the digital fraud risk management framework.

In many government entities, internal audit processes are among the most advanced from a risk management perspective. Incorporating digital fraud risks into this context is an effective practice for resource allocation. Additionally, it may be necessary to increase the frequency of assessments from a self-assessment perspective due to the dynamic nature of digital fraud risks. If a government entity lacks a mature self-assessment function for digital fraud risks, the proposed assessment in Annex A can be used as a preliminary self-assessment model.

7.6.2 Upskilling Personnel specialized in combating financial fraud

Government entities should ensure that their employees receive continuous education to enhance their skills, as continuous professional development is crucial in Anti-Digital Fraud. It strengthens employees' ability to handle evolving challenges and increases their awareness of digital fraud issues, forming a key foundation for effective prevention.

Upskilling Senior Staff Recommendation		
42	**Continuous Learning Program**	Training efforts can be customized to enhance skills based on the roles and responsibilities of senior staff.
43	**Role-Based Training**	Training efforts can be customized to enhance skills based on the roles and responsibilities of senior staff.
44	**Certifications and Accreditations**	Senior staff can be encouraged to obtain relevant specialized certifications and accreditations.
45	**Enhancing Cross-Departmental Collaboration**	Facilitating knowledge exchanged collaborative learning between different departments.
46	**Measuring Training Effectiveness**	The effectiveness of training can be regularly evaluated through assessments and feedback to ensure continuous skill improvement.

In addition to improving technical capabilities, Upskilling Personnel specialized in Anti-Digital Fraud helps build a specialized workforce that meets the needs of government institutions in alignment with Vision 2030 objectives. It also fosters a culture of awareness and proactive risk management within the organization.

When employees receive regular training on the latest digital fraud trends and best practices, they become more vigilant and gain in-depth knowledge. This training enhances their ability to detect threats and enables them to disseminate this knowledge within their immediate social circles. Consequently, awareness is widely distributed, effectively extending the influence of digital security culture throughout the organization or entity.

7.6.3 Information Sharing:

Since digital fraud incidents often originate in one domain and impact others, information sharing among government entities becomes crucial for gaining a comprehensive understanding of the digital fraud landscape. Information sharing is a fundamental component of Anti-Digital Fraud within government entities, enabling the effective and timely exchange of threat intelligence and best practices across different entities. At a minimum, government entities should aim to establish:

Information Sharing Recommendations		
47	**Information Sharing Protocol**	Government entities can establish clear and specific protocols for sharing digital fraud data, both within and between government entities.
48	**Public-Private Partnerships**	Government entities can collaborate with private sector partners to exchange threat information and leverage their expertise and resources, thereby enhancing the overall security posture.
49	**Information Sharing Communities**	Government entities can collaborate with private sector partners to exchange threat information and leverage their expertise and resources, thereby enhancing the overall security posture.
50	**Secure Information Exchange**	Government entities can adopt strong encryption technologies and secure communication channels to ensure the protection and confidentiality of shared information.

Adopting these requirements enables government entities to collaborate with a broader range of partners to jointly combat digital fraud. It also raises awareness of the issue and improves monitoring and response procedures. Information sharing also helps allocate resources more effectively. When government entities share insights on security breaches and digital fraud risks, they expand the knowledge base that benefits all stakeholders involved.

This active participation enhances prevention, monitoring, and response within the broader digital fraud risk management framework. Additionally, fostering a culture of information sharing within and between organizations promotes transparency and generates valuable fraud intelligence. By openly sharing information about digital fraud and the measures taken to combat it, organizations demonstrate their commitment to protecting public resources and their willingness to be accountable.

8. Conclusion

Anti-Digital Fraud is a sophisticated and critical undertaking that can significantly impact the delivery of digital government services and the overall user experience. Inadequate security measures can result in profound financial, operational, and psychological impacts requiring effective digital fraud risk management to monitor and mitigate their damage. To effectively mitigate these risks, governments must establish robust frameworks for anti-digital fraud—or enhance existing ones—to stay ahead of the ever-evolving threat landscape.

When determining the most effective approach, government entities should consider the following:

• Adopt a risk-based and risk-appetite approach: It's crucial to implement risk management practices that align with broader organizational goals. Emphasis should be placed on understanding the risks associated with digital fraud, balancing risk tolerance, and ensuring that anti-fraud efforts support the entity's strategic aims.

• Increase the Frequency of Risk Assessments: Government entities must conduct frequent, comprehensive assessments of digital fraud risks, drawing on national and local intelligence. This allows them to remain agile and responsive to rapidly evolving fraud tactics.

• Foster a Culture of Transparency and Continuous Learning: Government entities should encourage a culture transparency of about digital fraud, discuss risks openly, and provide ongoing training to ensure that employees are equipped to identify and address the latest fraud trends.

• Support Active Controls: Services and applications should be developed with digital fraud scenarios in mind. In addition to ensuring the ability to introduce new controls or discontinue services when needed.

• Collaborate with external entities. Government entities should work closely with other organizations and leverage national frameworks and capabilities to enhance the effectiveness of Anti-Digital fraud efforts and gain a broader understanding of fraud's overall impact.

In conclusion, there is no one-size-fits-all solution for managing digital fraud risks. The recommendations and methodologies outlined in this guideline enable government entities to effectively manage digital fraud risks. Government entities can leverage these principles to develop appropriate frameworks that align with their business requirements and the digital fraud risks they are exposed to.

09 Table of Definitions

Term	Definition
The Authority	The Digital Government Authority.
Digital Government	Promotes administrative, organizational and operational processes within and across government sectors to achieve digital transformation, develop, improve, and allow easy and effective access to government digital information and services.
Government Entities	Ministries, authorities, public institutions, councils, national centers and the like.
Controls	A policy, procedure, practice, process, technology, or other measure designed to mitigate the likelihood and/or impact of risks.
Digital Transformation	Strategically transforming and developing business models to be digital, based on data, technologies, and business solutions.
Risks	Potential events that could affect the objectives of an entity.
Risk assessment	A quantitative or qualitative approach to identifying, analyzing, and estimating the likelihood of occurrence and impacts of potentially risks, taking into account exposure factors, vulnerabilities, and susceptibility.
Continuous Improvement	Ongoing activity aimed at enhancing the performance of digital fraud risk management processes.
TOP Management	All those responsible for making key decisions within the entity
Training	Building skills and competencies to enhance the performance of those involved in specific roles or responsibilities.
Stakeholders	Parties and entities that affect and are affected by decisions, directions, procedures, objectives, policies and initiatives of the digital government and share some of their interests and outputs and are affected by any change that occurs in them.
Self-Assessment	A detailed plan guiding and clarifying progress in achieving initiatives and goals.
Awareness	Development of understanding of primary risks and threats that could negatively affect the achievement of objectives.
Procedures	Specific, regulated, and detailed steps followed to carry out tasks, operations, or activities related to risk and business continuity, based on relevant policies and standards.
Operations	Interconnected, integrated activities aimed at achieving defined outcomes in risk management and business continuity, based on established policies and procedures.
Workshop	A discussion-based exercise designed to guide participants or provide an overview of plans, policies, legislation, resources, capabilities, and strengths.

Term	Definition
Exercises	An operational exercise used to test or practice a specific procedure, role, or mechanism of action within a specific work team.
Business Continuity	The resources, capabilities, procedures, and activities of an entity required to continue providing essential services and important products at predefined levels and within an acceptable timeframe in the event of a disruption or interruption.
Biometrics	Unique physical characteristics of individuals, such as fingerprints.
Sponsoring Organizations Committee	An organization that provides frameworks and guidance on risk management, corporate governance, and fraud deterrence.
Digital Fraud	Any type of fraudulent activity carried out using technology or digital platforms. This type of fraud includes technical manipulation or deception to obtain material value or sensitive information through digital means
Fraud	Deliberately deceiving a person to obtain unlawful gains or depriving the victim of a legal right.
Identity Theft	A crime where personal information, such as ID numbers or credit card details, is obtained and used for fraudulent purposes.
International Organization for Standardization (ISO)	An independent, non-governmental international organization that develops and publishes standards across a wide range of industries and practices.
Phishing Attack	A type of fraud where the attacker impersonates a legitimate organization via email or text messages to steal sensitive information such as passwords, personal details, or confidential data.
Fraudulent deceptive	A dishonest scheme or trick aimed at deceiving a person to steal something valuable, often money or personal information.
Social Engineering	The psychological manipulation of individuals to perform actions or reveal confidential information, commonly used in various types of online and offline fraud.
Association of Certified Fraud Examiners (ACFE)	The world's largest anti-fraud organization, focusing on fraud monitoring, investigation, and prevention through training, certifications, and research.
Basel Committee on Banking Supervision (BCBS)	An international committee established to develop global banking supervision standards and improve the quality of banking oversight worldwide.
Fraud Triangle	A framework used to explain the factors leading to fraud, consisting of three elements—opportunity, motivation, and justification—that are believed to contribute to fraudulent behavior.
National Institute of Standards and Technology (NIST)	A U.S. government agency that develops and enhances measurement standards and technology to improve innovation, economic security, and quality of life.

Term	Definition
Digital Fraud Risks	The potential for fraudulent activities conducted through digital means, including technological platforms, digital transactions or digital communication channels. This includes the threat faced by individuals or entities in terms of financial loss, reputational damage, or legal consequences resulting from deceptive practices involving digital systems.
Digital Fraud Maturity Level (Emerging)	Irregular practices used to manage digital fraud operations, lacking clear processes, relying on individual efforts without a fixed framework.
Digital Fraud Maturity Level (Developing)	Some basic processes are implemented but poorly documented. The organization relies on individual expertise, leading to inconsistent application.
Digital Fraud Maturity Level (Capable)	Anti-Digital fraud operations are regularly implemented. Systematic practices are in place to identify, assess, and manage digital fraud risks.
Digital Fraud Maturity Level (Advanced)	Operations are systematically managed and monitored. Data is used to assess performance and make decisions.
Digital Fraud Maturity Level (Exemplary)	A strong focus on continuous improvement by leadership. The Anti-Digital Fraud culture is reinforced across all levels of the entity and is considered part of the overall strategy.
Data Consolidation	The process of combining data from multiple sources, cleaning and verifying it by removing errors, and storing it in a single location, such as a data warehouse or database.

Table (6)- Table of Definitions6 Table of Definitions

10. References and Relevant Regulations:

1. Fraud Risk Management Control Framework according to ISO 37003 Standard:

The Fraud Risk Management Control Framework according to the ISO 37003 standard provides guidelines and best practices for organizations to identify, assess, and mitigate fraud risks. It offers a structured approach to managing fraud risks, helping institutions implement effective controls and processes for fraud prevention and detection. The document is still in the consultation stage, but no significant changes are expected to the current draft.

2. Fraud Prevention Standard for Anti- Fraud Professionals:

This standard outlines the criteria and guidelines for professionals involved in anti-fraud activities. It aims to enhance the capabilities of anti-fraud practitioners by providing a structured approach to managing fraud risks and implementing effective fraud prevention measures.

3. European Commission's Anti-Fraud Strategy Action Plan:

The European Commission's Anti-Fraud Strategy Action Plan outlines strategic objectives and necessary measures to combat fraud targeting the European Union's budget and financial interests. It includes fraud prevention, detection, investigation measures, and initiatives to enhance cooperation between EU institutions and member states in fighting fraud.

4. BIS Discussion Paper on Digital Fraud Risk Management:

The BIS (Bank for International Settlements) Discussion Paper on Digital Fraud Risk Management explores challenges and best practices related to managing digital fraud risks in financial institutions and beyond. It discusses emerging trends, technologies, and regulatory considerations in Anti-Digital Fraud and response.

5. Saudi Central Bank (SAMA) Anti-Fraud Framework:

The Saudi Central Bank (SAMA) has developed an anti-fraud framework to enable regulated institutions to identify and address fraud-related risks effectively, establishing a common approach for managing fraud risks within member institutions.

6. Saudi Central Bank (SAMA) Cyber Security Framework:

This framework is designed to assist financial institutions in addressing cybersecurity elements and reducing digital fraud risks.

7. The Essential Cybersecurity Controls from the National Cybersecurity Authority (NCA):

A set of essential controls suitable for the cybersecurity needs of all entities and sectors in Saudi Arabia, contributing to the effective reduction of digital fraud risks.

8. Internal Control - Integrated Framework by the Committee of Sponsoring Organizations (COSO):

A comprehensive framework for managing internal fraud controls, offering an integrated approach to risk management, including digital fraud.

9. Fraud Risk Management Framework from the Association of Certified Fraud Examiners (ACFE):

A comprehensive resource that defines the strategies and techniques needed to identify, assess, and mitigate digital fraud risks, covering aspects such as prevention, detection, investigation, and response.

10. Cybersecurity Framework by the National Institute of Standards and Technology (NIST):

A framework aimed at helping organizations manage and monitor cybersecurity risks, including those related to digital fraud, widely used by governments and private sector institutions.

11. Risk Management and Business Continuity Controls for Digital Government:

A regulation within the digital government regulatory framework, aiming to enhance the maturity of services and strengthen the entity's ability to proactively identify risks and threats through the development of a risk management and business continuity system. This document includes a matrix to determine the impact of digital government service disruptions.

12. Guideline for Risk Management and Business Continuity in Digital Government:

A guideline outlining key instructions for designing and implementing the framework and basic components of the risk management and business continuity management systems in line with the operations of the government agency.

13. Royal Decree No. (M/19) dated 09/02/1443 AH (Personal Data Protection Law and The Implementing Regulation):

A law dedicated to the protection of personal data related to individuals in Saudi Arabia.

14. Royal Decree No. M/17 dated 08/03/1428 AH (Anti-Cyber Crime Law):

This law aims to limit cybercrime occurrences by defining these crimes and specifying the penalties for each.

15. Royal Decree No. (M/72) dated 10/09/1442 AH (Anti-Financial Fraud and Breach of Trust Prevention Law):

This law addresses anti-financial fraud and breach of trust, stipulating penalties for those who unlawfully seize others' money, as well as those who unlawfully appropriate property entrusted to them that is not public funds. It also outlines the penalties for inciting others to commit the crimes specified in this system, penalties for attempted crimes under this system, aggravating circumstances, confiscation of tools, instruments, and proceeds derived from such crimes, penalties related to defamation, exemptions from penalties, and stipulates that the Public Prosecution is the authority responsible for investigation and prosecution, in addition to provisions on publication and enforcement.

16. Controls for the classification of sensitive digital government services and verification levels issued by the Digital Government Authority:

It contributes to determining appropriate verification levels and techniques for government entities based on the sensitivity of their digital services, enabling users to benefit from digital government services and ensuring the continuity of these services and that they are not impacted.

11. Appendix:

Annex A - Initial Self-Assessment of Digital Fraud Risks

Annex B - Fraud Incident Case Studies

Annex C - Digital Fraud Survey by Design

Annex D - Professional Certifications Table

Annex A - Initial Self-Assessment of Digital Fraud Risks

The form below contains guiding questions designed to help decision-makers better identify and assess the current institutional maturity level in mitigating, managing, and monitoring digital fraud risks. These questions aim to assist in determining self-assigned likelihood, impact, and speed ratings. Based on the overall risk classification, government entity managers may choose to implement more detailed frameworks for digital fraud risks or update existing procedures to address any remaining risks, based on the defined risk tolerance data.

Number	Element	Category	Questions	Yes/No	Please Clarify Your Answer
1	Prevention	Process	Do you consult with experts in digital fraud, risk management, or cybersecurity during the design phase of your digital products?		
2		Process	Do you provide training to your employees and customers on digital fraud risks and how to prevent them?		
3		Process	Does your organization have clear, documented policies and procedures for addressing digital fraud?		
4		Process	Do your internal control plans include specific measures to mitigate digital fraud?		
5		Technology	Do you have mechanisms in place to control and monitor access to sensitive digital information, preventing its misuse in fraudulent activities?		
6		Technology	Do you have systems or tools to protect your brand?		
7	Detection	Process	Has your organization, its users, or beneficiaries been affected by any digital fraud incidents in the past?		
8		Process	Do you identify and document potential digital fraud risks your organization might face?		
9		Process	Do you have a system in place for classifying security incidents, allowing you to identify and categorize digital fraud cases?		
10		Technology	Do your systems undergo regular vulnerability assessments to identify weaknesses that could be exploited in digital fraud?		
11		Technology	Do you have a complaint management system that records cases of fraud related to individuals through fake government services?		
12		Technology	Do you have specific protocols for identifying digital processes with a high risk of fraud?		
13	Response	Process	Do you have a documented response plan for digital fraud incidents?		
14		Process	Do you have escalation procedures in place for handling digital fraud incidents?		
15		Process	Do you have a process for notifying affected customers or users in the event of a digital fraud incident?		
16		Process	Do you investigate reports of suspicious activities, whether reported by beneficiaries or employees?		
17		Human Resource	Does your incident response plan include notifying other government entities when a potential digital fraud incident occurs?		
18		Technology	Do you have an automated alert system that activates when suspicious activity is detected, initiating the security incident response process?		

Number	Element	Category	Questions	Yes/No	Please Clarify Your Answer
19	Continuous Improvement	Process	Do you analyze lessons learned from the evolving nature of digital fraud risks and use these insights to improve your security procedures?		
20		Process	Are digital fraud incidents considered when designing new digital products and services?		
21		Technology	Do you have ready-to-deploy technological solutions for comprehensive internal education on Anti-Digital Fraud?		
22		Human Resource	Do your digital fraud risk managers receive ongoing training to stay updated on developments in the field?		
23		Human Resource	Do you collaborate with other relevant organizations regarding digital fraud operations?		
24		Human Resource	Does senior management regularly evaluate the organization's performance in managing digital fraud risks?		
25	Reporting	Process	Do you record or report the number of digital fraud incidents?		
26		Process	Do you record or report incidents of digital fraud related to potential government services?		
27		Process	Do you provide senior management with regular reports on key digital fraud risk indicators in an easily understandable and standardized format?		
28		Human Resource	Do you notify the relevant national regulatory authorities when a digital fraud incident occurs?		
29		Process	Are there established measurement standards for monitoring, guiding, and enhancing Anti-Digital Fraud and detection?		
30		Technology	Do you have a centralized security incident logging system that allows for reporting of digital fraud cases?		
31	Governance	Process	Do you have a governance framework that addresses the management of digital fraud and deception risks?		
32		Process	Is there an executive or board member responsible for overseeing the management of digital fraud risks?		
33		Process	Are your policies and procedures related to digital fraud aligned with relevant regulatory and industry standards?		
34		Process	Do you consider potential digital fraud scenarios when designing and implementing internal controls and monitoring product quality?		
35		Process	Do you have a clear and defined statement outlining your organization's acceptable level of digital fraud risk, along with the necessary controls and procedures to address these risks?		
36		Human Resource	Does the board review digital fraud risks and strategies for mitigating their impact on a regular basis?		

The previous questions are intended to serve as an initial set for determining the extent to which Anti-Digital Fraud principles by design are applied, though they are not exhaustive. The more "Yes" answers provided, the higher the maturity level of the organization regarding the principles of Anti-Digital Fraud by design.

Based on the questions posed, risk management professionals within the organization should be able to assess the likelihood of exposure to digital fraud risks and evaluate its potential impact. Due to the rapidly evolving nature of these risks, the speed of their emergence is not considered during the initial self-assessment of digital fraud risks.

The table below is used as a temporary tool to measure preparedness, rather than a comprehensive risk analysis. These efforts can provide an initial estimate of probabilities and impacts, contributing to a more complete assessment of digital fraud risks.

METRICS - Self-Assessment by Entities on Anti-Digital Fraud

Anti-Digital Fraud Framework Initial Self-Assessment	Anti-Digital Fraud Self-Assessment					
	Element	0 Questions answered Yes	2 Questions answered Yes	3 Questions answered Yes	4-5 Questions answered Yes	6 Questions answered Yes
		Emerging	**Developed**	**Established**	**Advanced**	**Exceptional**
	Prevention					
	Detection					
	Response					
	Reporting					
	Continuous Improvement					
	Governance					

Appendix B – Examples

Deep Fake - Ferrari NV Incident

Background

- In a recent attempted scam incident, Ferrari NV narrowly avoided falling victim to a sophisticated deepfake scam. This scam involved the use of advanced AI technology to create a convincing imitation of Ferrari's CEO, Benedetto Vigna. The perpetrators aimed to fraud the company by posing as Vignain virtual meetings and communications.

Implications

Although there was no immediate impact the incident itself implies that the organization is being targeted by well-organized threat factors.

Lessons Learned

Executive that was targeted did the right thing and asked a unique question based on his relationship with CEO.

Incident Overview

- A senior executive in the board of Ferrari received a WhatsApp message purporting to be the CEO Benedetto Vigna.
- The messages came from a number that was not the CEO's usual number.
- The message indicated that the reason that a separate number was being used was because an acquisition is being made in China and it required utmost discretion.
- The perpetrator then insisted on organizing a call - the voice impersonating Vigna was extremely convincing and was tuned to a south Italian accent.
- The perpetrator began explaining needed to discuss something confidential - a deal that could face some China-related snags and required an unspecified currency-hedge transaction to be carried out.

At this point, the executive in question got suspicious and posed a question - the perpetrator was asked to name the book that the CEO had recommended to the executive - at that point, the call stopped.

Access Control Failure - Société General

Background

- The 2008 Société General rouge trading incident, centered around trader Jérôme Kerviel, stands as a significant example of how failures in access control can lead to catastrophic outcomes in the financial industry. Kerviel joined the company working in compliance and had access to compliance systems that he retained when he joined the trading division.

Implications

The failure of access controls allowed Kerviel to build unauthorized positions that ultimately led to a € 4.9 billion loss when they were unwound.

Lessons Learned

The incident had widespread implications for the banking industry and remains a cautionary tale of the potential risks associated with modern financial markets.

Incident Overview

- Manipulating Internal Systems: Kerviel exploited his continued access to the compliance systems, allowing him to create fictitious trades and backdate transactions.
- This manipulation was made possible because the bank's access controls did not sufficiently segregate duties between his former compliance role and his new trading responsibilities.
- Proper access control typically involves the segregation of duties to prevent conflicts of interest and unauthorized actions.

In Kerviel's case, he was able to perform tasks that should have been segregated - such as initiating trades, booking them, and then manipulating records to conceal the true level of risk.

Government Impersonation – USA

Background

- One notable incident of government impersonation fraud occurred during the COVID-19 pandemic in the US. Scammers took advantage of the confusion and fear surrounding the pandemic to impersonate government officials and agencies.

Implications

Between October 2020 and September 2021, the Federal Trade Commission estimated that 2 billion USD was defrauded of beneficiaries by impersonating government entities.

Lessons Learned

Extensive brand protection mechanisms and awareness campaigns need to be deployed in times of social turmoil.

Incident Overview

- Criminal threat actors used various methods, such as phone calls, emails, and text messages, to trick people into believing they were interacting with legitimate government representatives. Most often criminal threat actors posed as:
- Internal Revenue Service (IRS): Scammers often posed as IRS agents, threatening victims with arrest or fines if they didn't pay supposed back taxes or provide personal information.
- Social Security Administration (SSA): Fraudsters claimed that the victim's Social Security number had been suspended due to suspicious activity and demanded personal information to "reactivate".
- Centers for Disease Control and Prevention (CDC): Scammers sent fake emails and messages claiming to be from the CDC, offering information about COVID-19 or requesting donations.
- Federal Trade Commission (FTC): Impersonators used the FTC's name to lend credibility to their scams, often involving fake sweepstakes or grants.

Use of Notification Systems to Combat Fraud

Background

- In 2015, the U.S. Office of Personnel Management (OPM) revealed that its systems had been breached resulting in the theft of sensitive personal information of over 21 million current, former, and prospective federal employees, making it one of the largest and most significant government data breaches in U.S. history.

Implications

The user notification system was critical in informing the affected individuals and providing them with the necessary resources to mitigate the risks associated with the breach.

Lessons Learned

The incident had severe implications but due to a sophisticated, well-developed user notification system it is estimated that a significant amount of digital fraud was avoided.

Incident Overview

Once the breach was discovered, OPM implemented a comprehensive user notification system to alert affected individuals. This notification process included several steps that effectively mitigated somewhat the digital fraud risk posed by this data breach:

- Email Notifications: OPM sent out millions of emails to affected individuals, notifying them of the breach and providing information on what data had been compromised.
- Postal Notifications: For those whose email addresses were not available or up-to-date, OPM sent out physical letters to inform them of the breach.
- Dedicated Website and Hotline: OPM set up a dedicated website and a toll-free hotline where individuals could verify whether they were affected by the breach and receive guidance on steps to protect themselves, such as enrolling in identity theft protection services.
- Identity Theft Protection and Monitoring: As part of the notification, OPM offered affected individuals free credit monitoring, identity theft insurance, and other protective services for several years.
- Public Announcements: In addition to direct notifications, OPM made public announcements and updates through press releases, media briefings, and their official website to keep the general public informed about the incident.

Use of Data Analytics To Combat Fraud

Background

- Tax fraud has long been a significant problem for the IRS, with criminals filing fraudulent tax returns to claim refunds they aren't entitled to. As digital filing became more common, fraudsters increasingly used stolen personal information to submit fake returns. The scale of the problem grew with the rise of identity theft and other sophisticated tactics.

Implications

The application of data analytics resulted in the prevention of billions of dollars in fraudulent tax refunds. IRS reported that its analytics-driven fraud detection system helped stop over $4 billion in fraudulent refunds in 2016.

Lessons Learned

Extensive and widespread application of data analytics can yield excellent results when combating fraud on a government level.

Incident Overview

The IRS implemented advanced data analytics to detect and prevent fraudulent tax filings. The agency utilized predictive modeling, machine learning, and big data analysis to scrutinize tax return data in real-time.

•Pattern Recognition: The IRS developed models that could identify suspicious patterns in tax filings, such as anomalies in income reporting, deductions, and filing history. These models flagged returns that deviated significantly from established norms.

•Anomaly Detection: Analytics tools were used to detect anomalies in taxpayer behavior, such as unusual filing times, IP address inconsistencies, and mismatched financial information. These anomalies often indicated potential fraud.

•Data Integration: The IRS integrated various data sources, including previous filing histories, third-party financial data, and information from other government agencies, to create a more comprehensive view of each tax return. This helped in cross-referencing and verifying the authenticity of the data provided in the filings.

•Machine Learning: Machine learning algorithms continuously improved the fraud detection models by learning from both successful and unsuccessful fraud attempts. This adaptive approach allowed the IRS to stay ahead of evolving fraud tactics.

•Collaboration with External Partners: The IRS collaborated with financial institutions, payroll providers, and state tax agencies to share data and identify fraud patterns more effectively. This multi-stakeholder approach expanded the data pool and enhanced the analytics capability.

Template for Reporting Digital Fraud Incidents

Background

- Explain the background of the incident.

Implications

The core implications.

Lessons Learned

The key improvements that have been implemented.

Incident Overview

Write an Incident Overview

Appendix C - Anti Digital Fraud by Design Questionnaire

Number	Questions	Yes/No
1	Do you perform digital fraud risk assessments associated with the use of your products?	
2	Is there a mandatory for digital fraud risk experts to participate in the requirements development stage of a beneficiary-oriented product?	
3	Is there a minimum fraud risk impact threshold in place to differentiate between high and low risk digital fraud applications?	
4	Is there a mandatory requirement for all beneficiary-oriented products, apps and services to undergo digital fraud risk assessments?	
5	Are apps, products and services required to have an incident reporting functionality embedded within the UX?	
6	Do apps, products and services have encrypted notification functionality?	
7	Are apps, products and services designed in a way that enables them to adapt to active control environments?	
8	Is a unique identifier assigned during the design of digital government services so that incidents can be linked to key products, apps and services?	
9	Do your products, apps and services equipped with the capability to effectively disrupt high-impact digital fraud incidents?	
10	Is there a design requirement mandating the use of encrypted communication channels in all high-risk apps, products and services?	

The previous questions are intended to serve as an initial set for determining the extent to which Anti-Digital Fraud principles by design are applied, though they are not exhaustive. The more "Yes" answers provided, the higher the maturity level of the organization regarding the principles of Anti-Digital Fraud by design.

Appendix D - Professional Certification Schedule

#	Qualification/Program Name	Granting Authority
1	Professional Certification in Fraud Prevention	CIFAS
2	Professional Certification in Fraud Investigation	CIFAS
3	Certified Anti-Fraud Specialist	CIFAS
4	Certified Anti-Digital Fraud Practitioner	CIFAS
5	Digital Forensics Specialist	SANS
6	Certified Fraud Prevention Professional	ACFE
7	Certified Fraud Auditor	ACFE
8	Certified Anti-Fraud Specialist	CFS
9	Certified Specialist in Financial Crimes	ACFE
10	Certified Cybercrime Investigator	ACFCI

هيئة الحكومة الرقمية
Digital Government Authority

DGA.GOV.SA