

Enhancing Revenue Assurance

through AI-Driven Fraud Management

How stc Integrated Machine Learning into Operational Fraud Detection

TM Forum Case Study - (Draft).

Prepared by:

stc (Saudi Telecom Company)

Digital and telco leader, enabling the society and economy to thrive, in KSA and beyond.

Project Focus:

Revenue Assurance • Fraud Management • Artificial Intelligence • Machine Learning • Business Assurance • Autonomous Operations

Prepared for:

TM Forum Inform

Research & Analysis – Case Study Submission - 2026

Keywords

Artificial Intelligence (AI) • Machine Learning (ML) • Revenue Assurance • Fraud Management • RAID-FMS • Business Assurance • Digital Transformation • Operational Excellence • eTOM • TM Forum

Document Classification

Case Study - Draft

Prepared in accordance with the TM Forum Case Study Guidance.

This document has been prepared as a draft for review and discussion purposes. Business figures, percentages, timelines, and executive quotations are subject to final validation prior to publication.

WHO • WHAT • HOW

WHO:

stc (Saudi Telecom Company)

stc is a leading digital enabler and telecommunications provider in the Kingdom of Saudi Arabia and the wider region. Through continuous investment in digital transformation, operational excellence, and emerging technologies, stc is committed to delivering innovative services while enhancing customer experience, protecting business revenues, and enabling intelligent operations.

As part of its strategic transformation journey, stc continues to adopt Artificial Intelligence (AI), Machine Learning (ML), and advanced analytics across its operational domains to improve business resilience, operational efficiency, and service quality. This case study highlights one of these strategic initiatives within the Fraud Management and Revenue Assurance (RAFM) domain.

WHAT:

stc successfully deployed Artificial Intelligence (AI) and Machine Learning (ML) capabilities within its operational Fraud Management and Revenue Assurance (RAFM) environment to strengthen fraud detection effectiveness, reduce revenue leakage, improve operational efficiency, and establish a scalable hybrid fraud detection framework capable of addressing increasingly sophisticated fraud scenarios.

HOW:

The initiative was implemented by integrating Machine Learning models into the existing RAID-FMS fraud management platform while preserving and enhancing traditional rule-based fraud controls.

A hybrid detection architecture was established by combining:

* Machine Learning Models
* Traditional Rule-Based Detection
* Behavioural Analytics
* Anomaly Detection
* Large-Scale Traffic Pattern Analysis

Initially, three AI-driven production use cases were deployed:

*** IRSF – ML**

*** Bypass – ML**

*** Wangiri – ML**

The deployment followed a phased implementation approach covering assessment, model development, platform integration, validation, and operational rollout. Throughout the project, operational processes continued to align with TM Forum best practices and frameworks, particularly **eTOM**, building upon stc's previous TM Forum conformance certification in Application Operations (OSO).

Executive Summary:

Artificial Intelligence is rapidly transforming the telecommunications industry by enabling Communication Service Providers (CSPs) to improve operational intelligence, automate decision-making, and strengthen business assurance capabilities.

Recognizing the growing complexity of fraud threats and the increasing limitations of conventional rule-based detection methods, stc initiated a strategic program to integrate Artificial Intelligence and Machine Learning into its operational Fraud Management and Revenue Assurance environment.

Rather than replacing existing operational processes, the initiative introduced a hybrid detection architecture that combines proven rule-based controls with advanced Machine Learning models. This approach enables the identification of complex behavioural patterns, emerging fraud scenarios, and anomalies that are difficult to detect using traditional techniques alone.

The implementation demonstrates how AI can be embedded into operational environments in a practical and scalable manner while maintaining governance, operational stability, and alignment with internationally recognized industry frameworks.

The initiative has delivered measurable business outcomes, including approximately:

* 15% improvement in fraud detection effectiveness.

* 7% reduction in revenue leakage.

* 35% earlier identification of fraud incidents.

* 20% reduction in investigation effort.

In addition, Machine Learning-generated cases accounted for approximately 31.8% of all fraud cases generated during the monitored period in 2026, demonstrating the increasing contribution of AI-driven analytics to operational fraud detection.

Beyond measurable performance improvements, the project establishes a strong foundation for future AI-enabled Business Assurance, intelligent operational decision-making, and the continued evolution toward Autonomous Operations.

This case study demonstrates how Communication Service Providers can successfully modernize Fraud Management and Revenue Assurance by combining Artificial Intelligence, advanced analytics, and TM Forum operational best practices to deliver tangible business value while supporting long-term digital transformation objectives.

Main Narrative

Background:

As one of the leading digital and telecommunications providers in the Middle East, stc continues to invest in operational excellence, intelligent automation, and advanced digital capabilities to strengthen business resilience and deliver sustainable value to customers, shareholders, and the broader digital ecosystem.

The rapid evolution of telecommunications services, together with the accelerated adoption of digital channels, cloud-based platforms, 5G connectivity, Internet of Things (IoT), and digital financial services, has significantly increased the complexity of operational environments. At the same time, these advancements have introduced new opportunities for increasingly sophisticated fraud schemes, requiring Communication Service Providers (CSPs) to modernize their Fraud Management and Revenue Assurance capabilities.

Historically, fraud detection within telecommunications environments has relied heavily on predefined business rules, thresholds, and expert-defined detection scenarios. While these approaches continue to provide strong protection against known fraud patterns, they often struggle to identify previously unseen behaviours, evolving attack techniques, and complex anomalies hidden within rapidly growing volumes of operational data.

Recognizing these industry challenges, stc identified Artificial Intelligence (AI) and Machine Learning (ML) as strategic enablers capable of complementing traditional operational controls and strengthening the organization’s ability to proactively detect, analyze, and respond to increasingly dynamic fraud threats.

This initiative forms part of stc's broader digital transformation strategy, which focuses on embedding intelligent technologies across operational domains to improve decision-making, increase automation, enhance operational efficiency, and accelerate the evolution toward data-driven and autonomous operations.

By integrating Machine Learning directly into the operational Fraud Management and Revenue Assurance (RAFM) environment, stc sought not only to improve fraud detection performance but also to establish a scalable framework capable of continuously adapting to new fraud patterns while maintaining operational governance and alignment with internationally recognized industry standards.

Industry Context:

Across the global telecommunications industry, Communication Service Providers are increasingly adopting Artificial Intelligence to enhance operational assurance, automate complex analytical processes, and strengthen business protection capabilities.

TM Forum has consistently highlighted Artificial Intelligence as a key enabler of Autonomous Operations, emphasizing the importance of intelligent decision-making, predictive analytics, standardized operational processes, and data-driven assurance capabilities.

Within this context, Revenue Assurance and Fraud Management represent some of the highest-value operational domains for AI adoption due to the significant financial impact associated with fraud incidents, revenue leakage, and operational inefficiencies.

As fraud techniques continue to evolve at an unprecedented pace, organizations require operational models capable of learning from historical data, recognizing emerging behavioural patterns, and continuously improving detection accuracy without relying exclusively on manually maintained business rules.

The implementation described in this case study reflects this industry direction by demonstrating how Artificial Intelligence can be embedded into an existing operational environment while preserving governance, operational stability, and alignment with TM Forum best practices.

The Challenge:

Like many leading Communication Service Providers worldwide, stc faced a rapidly evolving fraud landscape characterized by increasing complexity, larger volumes of operational data, and the growing sophistication of fraudulent activities.

Several strategic and operational challenges were identified:

* Increasing complexity of fraud scenarios and attack techniques across digital services.

* Continuous growth in transaction volumes requiring highly scalable analytical capabilities.

* Difficulty identifying previously unknown fraud patterns using traditional rule-based detection alone.

* The need to minimize revenue leakage while maintaining high levels of operational accuracy and customer trust.

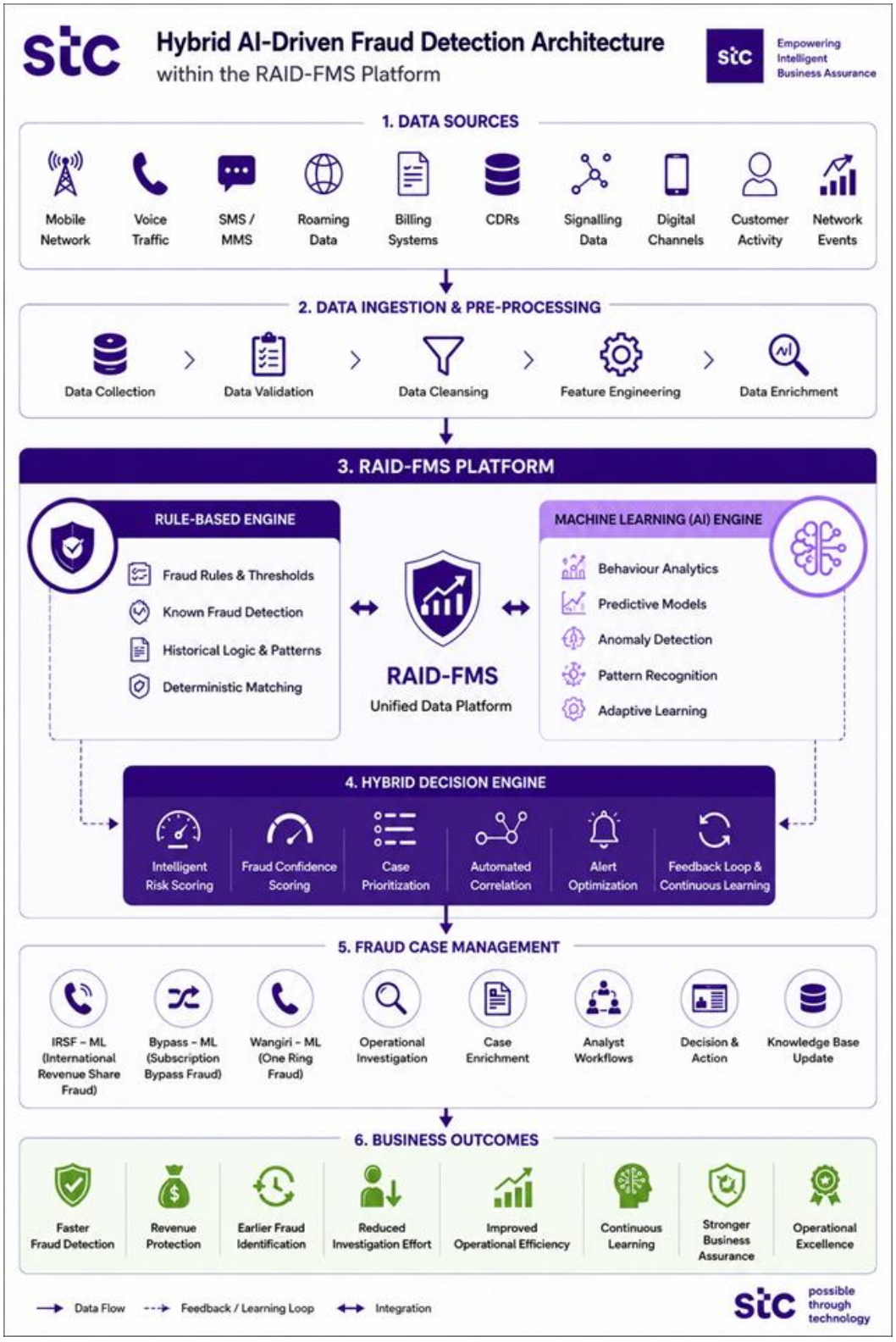
* Increasing pressure to improve investigation efficiency and reduce the time required to identify and respond to fraud incidents.

* The desire to transition from reactive fraud detection toward proactive, predictive, and intelligence-driven operational assurance.

In addition, operational teams recognized that future fraud management capabilities would require a balanced combination of human expertise, standardized operational processes, and Artificial Intelligence working together to deliver sustainable improvements in Business Assurance performance.

These challenges ultimately provided the strategic foundation for launching an AI-enabled transformation initiative aimed at modernizing stc’s Fraud Management and Revenue Assurance environment while supporting the organization’s long-term vision for intelligent and autonomous operations.

The Solution:



To address the identified operational and business challenges, stc implemented a strategic enhancement of its **Fraud Management and Revenue Assurance (RAFM)** environment by integrating **Artificial Intelligence (AI) and Machine Learning (ML)** capabilities into its existing **RAID-FMS** platform.

Rather than replacing the established fraud detection framework, the objective was to augment it through intelligent analytics capable of identifying behavioural anomalies, learning from historical data, and detecting sophisticated fraud patterns that may remain undetected using traditional rule-based techniques alone.

This approach resulted in the creation of a **hybrid fraud detection architecture**, combining the stability and transparency of deterministic business rules with the adaptability and predictive capabilities of Machine Learning models.

The hybrid architecture integrates multiple analytical components, including:

* Traditional rule-based fraud controls for detecting known fraud scenarios.

* Machine Learning models trained using historical fraud datasets and operational intelligence.

* Behavioural analytics to identify abnormal customer and network activity.

* Anomaly detection techniques capable of recognizing previously unseen fraud patterns.

* Large-scale traffic analysis supporting continuous monitoring of high-volume telecommunications transactions.

By combining these complementary capabilities, the platform is able to deliver more accurate, scalable, and proactive fraud detection while reducing dependency on manual rule creation and maintenance.

AI Use Cases Deployed into Production:

As part of the implementation, **three Machine Learning-powered fraud detection use cases** were successfully deployed into the production environment.

IRSF – Machine Learning:

Machine Learning models were introduced to enhance the detection of **International Revenue Share Fraud (IRSF)** by analysing complex international traffic patterns and identifying suspicious behaviours that may indicate fraudulent revenue-sharing activities.

The AI models continuously evaluate historical calling behaviour, destination trends, and traffic anomalies to improve detection speed and reduce false positives.

Bypass – Machine Learning:

Artificial Intelligence capabilities were deployed to strengthen the identification of **Bypass Fraud**, where unauthorized routing mechanisms are used to circumvent legitimate telecommunications infrastructure.

The Machine Learning models analyse routing behaviour, signalling characteristics, and traffic deviations to identify suspicious bypass activities that may not be fully visible through conventional rule-based controls.

Wangiri – Machine Learning:

Machine Learning algorithms were implemented to improve the detection of **Wangiri Fraud**, a fraud scheme characterized by missed-call campaigns designed to encourage customers to return premium-rate international calls.

Using behavioural analytics and anomaly detection, the solution identifies unusual calling patterns, evaluates risk indicators, and enables earlier detection of fraudulent campaigns before they generate significant financial impact.

Building an Intelligent Hybrid Detection Framework:

The deployment of these three AI-driven use cases marked a significant evolution in stc's fraud management capabilities.

Instead of relying solely on predefined rules, the organization established a data-driven operational model capable of continuously learning from new fraud behaviours while preserving the governance, transparency, and operational reliability of existing fraud management processes.

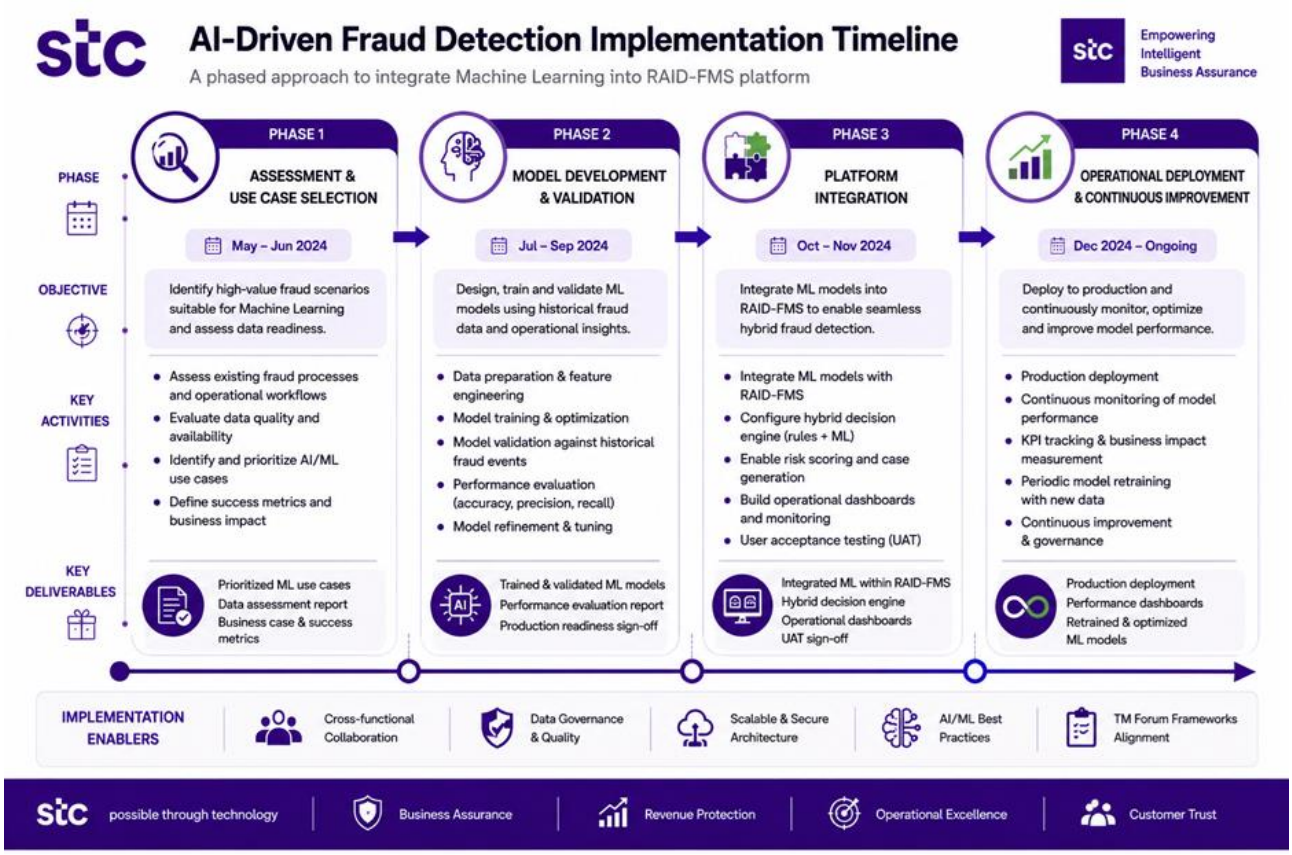
The resulting hybrid framework provides greater analytical depth, faster detection of emerging threats, improved scalability, and a strong foundation for future AI-enabled Business Assurance initiatives.

Furthermore, the architecture was designed with extensibility in mind, allowing additional Machine Learning use cases to be incorporated as fraud scenarios evolve and new operational requirements emerge.

Hybrid Fraud Detection Architecture

Purpose: Illustrates how the RAID-FMS platform integrates Rule-Based Detection, Machine Learning Models, Behavioural Analytics, and Anomaly Detection into a unified hybrid architecture supporting intelligent fraud detection and revenue protection.

Implementation Approach:



The successful deployment of Artificial Intelligence within stc's Fraud Management and Revenue Assurance (RAFM) environment was achieved through a structured and phased implementation methodology designed to minimize operational risk, ensure business continuity, and maximize long-term value realization.

The implementation was led through close collaboration between business, operational, and technology teams across stc, bringing together expertise in Fraud Management, Revenue Assurance, Data Analytics, AI Engineering, and IT Operations. This multidisciplinary approach ensured that business objectives, operational requirements, and technical capabilities remained fully aligned throughout the project lifecycle.

Rather than introducing a disruptive technology replacement, the project focused on progressively enhancing the existing RAID-FMS environment by embedding Machine Learning capabilities alongside established fraud detection mechanisms. This approach enabled stc to preserve operational stability while introducing intelligent analytics capable of continuously learning from evolving fraud behaviours.

Phase 1 – Assessment and Use Case Selection:

The first phase focused on identifying operational areas where Artificial Intelligence could deliver the highest business value.

Key activities included:

* Assessment of existing fraud management processes and operational workflows.
* Identification of high-value fraud scenarios suitable for Machine Learning implementation.
* Evaluation of historical fraud datasets and operational data quality.
* Prioritization of AI use cases based on business impact, feasibility, and expected operational benefits.

This assessment resulted in the selection of three initial Machine Learning use cases:

* IRSF – ML
* Bypass – ML
* Wangiri – ML

These use cases were chosen because of their high operational importance, measurable business value, and suitability for behavioural analytics and predictive modelling.

Phase 2 – Model Development and Validation:

Following the assessment phase, Machine Learning models were designed, trained, tested, and validated using historical fraud datasets and operational intelligence collected from the RAFM environment.

The development process included:

* Data preparation and feature engineering.
* Machine Learning model training and optimisation.
* Validation against historical fraud events.
* Performance evaluation using operational accuracy metrics.
* Continuous refinement to improve precision and reduce false positives.

Particular attention was given to ensuring that AI-generated insights complemented existing operational controls rather than introducing unnecessary complexity into the investigation process.

Phase 3 – Platform Integration:

Once the Machine Learning models had successfully completed validation, they were integrated into the existing RAID-FMS platform.

The integration strategy focused on maintaining compatibility with current operational processes while enabling AI-generated intelligence to become part of day-to-day fraud detection activities.

The hybrid architecture enabled:

* Seamless interaction between rule-based controls and Machine Learning models.
* Centralised case generation within the existing operational platform.
* Unified operational monitoring and investigation workflows.
* Consistent governance across AI-generated and rule-generated fraud cases.

This integration ensured that operational users could adopt AI capabilities without significant changes to their existing investigation procedures.

Phase 4 – Operational Deployment and Continuous Improvement:

Following successful integration, the Machine Learning models were deployed into the production environment.

Operational deployment included:

* Continuous monitoring of AI model performance.
* Measurement of operational KPIs and business outcomes.
* Performance tuning based on operational feedback.
* Periodic model retraining to reflect emerging fraud behaviours.
* Ongoing governance to maintain model effectiveness and reliability.

This continuous improvement cycle ensures that the AI solution evolves alongside changing fraud patterns, allowing the organization to sustain long-term operational effectiveness while reducing the risk of model degradation over time.

Alignment with TM Forum Best Practices:

Throughout every stage of the implementation, stc maintained alignment with internationally recognized operational frameworks and best practices.

The project was developed in accordance with TM Forum principles, particularly:

* **eTOM (Enhanced Telecom Operations Map)** for standardized operational processes.

* **Application Operations (OSO)**, building upon stc's previously achieved TM Forum Conformance Certification.

* **Business Assurance principles** supporting revenue protection and operational governance.

* **Autonomous Operations** concepts through the introduction of AI-enabled decision support and intelligent operational analytics.

By embedding Artificial Intelligence into an operational framework already aligned with

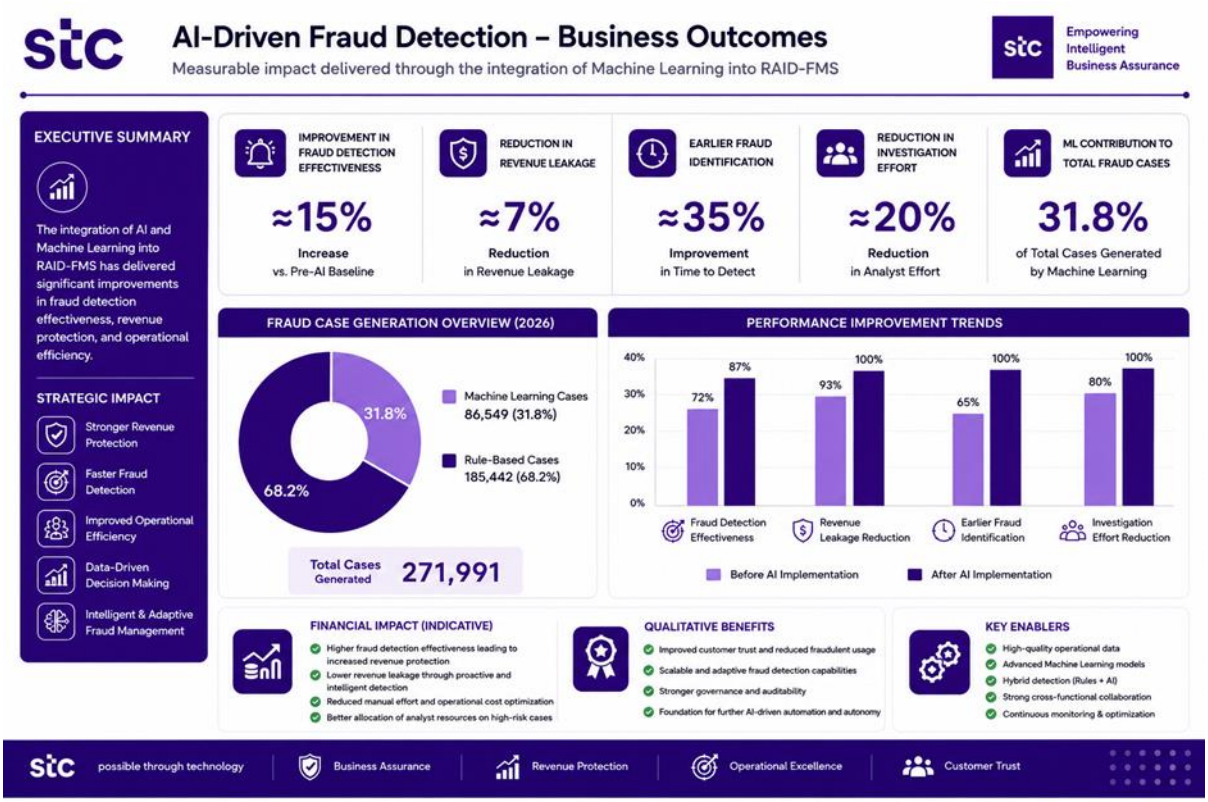
TM Forum standards, stc ensured that innovation was introduced in a controlled, scalable, and governance-driven manner, supporting both immediate business objectives and the organization's long-term digital transformation strategy.

Project Timeline:

Purpose: Illustrates the four

implementation phases-from Assessment and Use Case Selection, through Model Development and Platform Integration, to Operational Deployment and Continuous Improvement-highlighting the structured delivery approach adopted by stc and its alignment with TM Forum operational best practices.

Business Benefits:



The integration of Artificial Intelligence (AI) and Machine Learning (ML) into stc's Fraud Management and Revenue Assurance (RAFM) environment has delivered measurable business and operational improvements, demonstrating the value of combining intelligent analytics with established operational processes.

Beyond enhancing fraud detection capabilities, the initiative has contributed to strengthening Business Assurance, improving operational efficiency, and reducing the financial impact of increasingly sophisticated fraud activities.

The implementation has enabled operational teams to make faster, more informed decisions while improving the organization's ability to identify emerging fraud scenarios before they result in significant revenue leakage.

By embedding Machine Learning directly into the operational workflow, stc has established a scalable, data-driven fraud detection model that continues to evolve as new fraud patterns emerge.

Measurable Business Outcomes:

Following the deployment of the hybrid AI-enabled fraud detection architecture, several measurable improvements have been observed across the operational Fraud Management environment.

The initiative delivered approximately:

* **15% improvement in fraud detection effectiveness**, enabling operational teams to identify a greater proportion of fraudulent activities through the combined use of Machine Learning and traditional rule-based controls.

* **7% reduction in revenue leakage**, achieved through earlier fraud detection, faster operational response, and enhanced analytical capabilities.

* 35% earlier identification of fraud incidents, significantly reducing the time between fraudulent activity and operational intervention.

* **20% reduction in investigation effort**, allowing fraud analysts to focus on higher-risk cases while reducing manual analysis through AI-assisted prioritization.

In addition to these measurable performance indicators, the project generated several broader operational benefits that continue to support stc's digital transformation objectives.

Operational Benefits:

The implementation has strengthened operational capabilities across multiple dimensions, including:

* Increased operational efficiency through AI-assisted fraud analysis.

* Improved scalability to support continuously growing transaction and network traffic volumes.

* Enhanced detection of previously unknown and evolving fraud patterns.

* Faster operational response to emerging fraud incidents.

* Better prioritization of investigation activities through intelligent risk assessment.

* Reduced dependency on manual rule creation and maintenance.

* Improved collaboration between operational teams and advanced analytics functions.

* Stronger governance through the integration of AI within existing operational processes.

Collectively, these improvements have increased the overall maturity of the Fraud Management and Revenue Assurance function while supporting more proactive and intelligence-driven operational decision-making.

Strategic Business Value:

Beyond immediate operational improvements, the initiative establishes a strategic foundation for future Business Assurance innovation.

By integrating Artificial Intelligence into an operational environment already aligned with TM Forum frameworks, stc has demonstrated that AI can be successfully introduced without disrupting existing operational governance or established business processes.

The project illustrates how Machine Learning can complement—not replace—human expertise by providing operational teams with intelligent insights that enhance analytical capabilities, improve decision quality, and accelerate response times.

This hybrid operating model supports long-term business resilience while creating opportunities for further automation, predictive analytics, and AI-driven operational optimization across additional assurance domains.

Supporting Operational Statistics:

Operational statistics collected during the monitored period in 2026 further demonstrate the successful adoption of Machine Learning within the RAID-FMS platform.

Key operational indicators include:

Result	Operational Metric
271,991	**Total Cases (Alarms) Generated**
86,549	**Total ML Cases (Alarms) Generated**
31.8%	**ML Contribution to Total Cases**

These results demonstrate that Machine Learning has become an integral component of stc's operational fraud detection process, contributing significantly to overall case generation while working in conjunction with traditional fraud detection mechanisms.

The increasing proportion of AI-generated fraud cases provides strong evidence of the operational maturity of the hybrid detection framework and its growing role in supporting intelligent Business Assurance.

Business Impact Summary:

The success of this initiative demonstrates that Artificial Intelligence can generate measurable business value when implemented within a structured operational framework.

The combination of improved fraud detection effectiveness, reduced revenue leakage, earlier fraud identification, and increased operational efficiency provides a compelling business case for the continued expansion of AI capabilities across Revenue Assurance and Fraud Management functions.

Moreover, the initiative reinforces stc's commitment to operational excellence, digital transformation, and continuous innovation while supporting the organization's long-term vision for intelligent and autonomous operations.

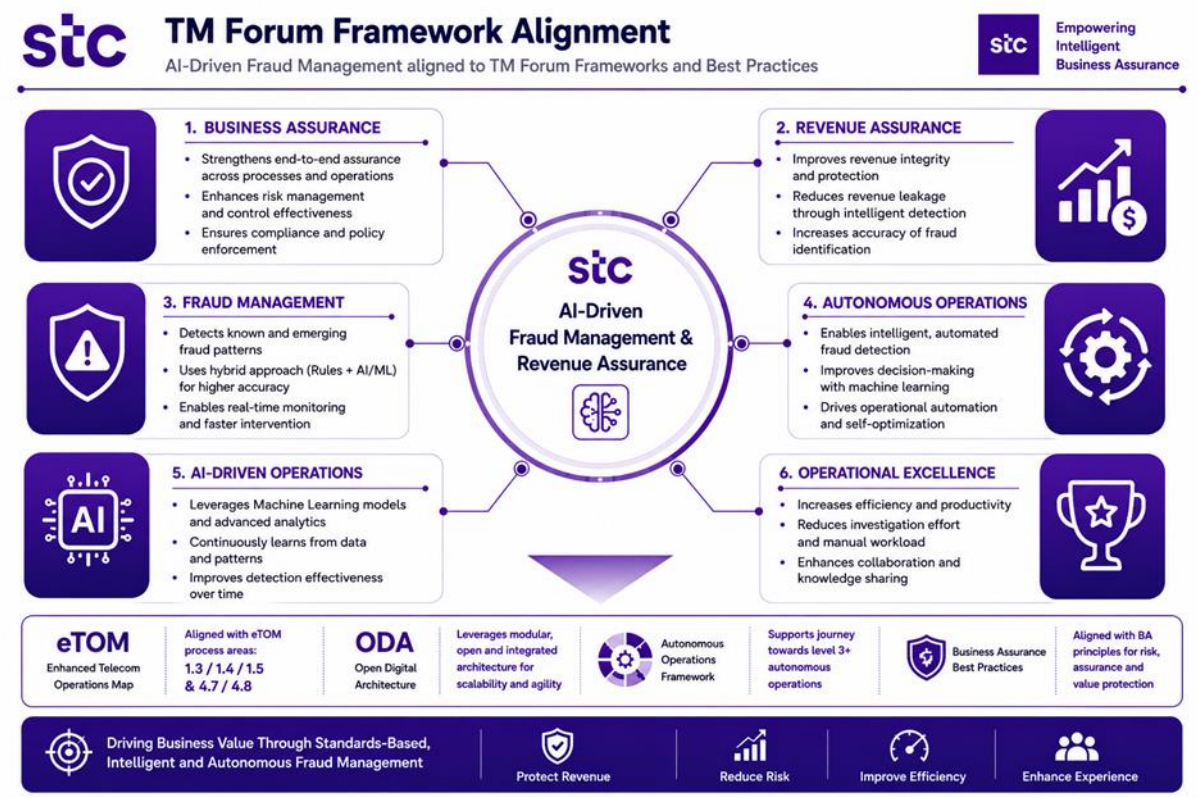
Business Outcomes Dashboard

Purpose: Present the project's key business outcomes through an executive dashboard highlighting:

* **15% Improvement** in Fraud Detection Effectiveness
* **7% Reduction** in Revenue Leakage
* **35% Earlier** Fraud Identification
* **20% Reduction** in Investigation Effort
* **31.8% ML Contribution** to Total Fraud Cases (2026)

The dashboard should use stc brand colors, executive-style KPI cards, and infographic elements consistent with TM Forum publication standards, enabling readers to quickly understand the measurable business impact of the initiative.

Alignment with TM Forum Frameworks:



A key success factor behind this initiative was the alignment of the implementation with internationally recognized operational frameworks and industry best practices promoted by **TM Forum**.

From the outset, the project was designed not only to improve fraud detection performance, but also to ensure that the adoption of Artificial Intelligence was governed through standardized operational processes, clear business accountability, and scalable architecture principles.

Rather than introducing AI as a standalone technology initiative, stc positioned Machine Learning as an operational capability embedded within existing Business Assurance processes. This approach ensured that innovation complemented established governance while supporting long-term operational sustainability.

The project demonstrates how AI can be integrated into a mature operational environment without compromising process consistency, auditability, or operational control.

Supporting Business Assurance Transformation:

The implementation directly supports the evolution of **Business Assurance** by strengthening the organization's ability to proactively protect revenues through intelligent analytics and data-driven decision making.

Machine Learning enables operational teams to identify behavioural anomalies, prioritize high-risk fraud cases, and respond more rapidly to emerging threats.

This shift from reactive detection toward predictive operational intelligence represents an important step in the modernization of Business Assurance functions.

By embedding AI into day-to-day operational activities, stc has enhanced the maturity of its assurance capabilities while creating a scalable foundation for continuous improvement.

Alignment with Revenue Assurance:

Revenue Assurance remains a strategic capability for Communication Service Providers seeking to protect revenues while maintaining operational efficiency.

The AI-powered fraud detection framework contributes directly to Revenue Assurance objectives by:

* Improving fraud detection effectiveness.
* Reducing revenue leakage.
* Accelerating fraud identification.
* Increasing investigation efficiency.
* Supporting data-driven operational decisions.
* Enhancing revenue protection across digital services.

The initiative demonstrates that Artificial Intelligence can significantly strengthen Revenue Assurance without replacing existing operational controls, instead complementing them through intelligent analytics and continuous learning.

Alignment with TM Forum eTOM:

Throughout the implementation, operational processes continued to align with the **TM Forum Enhanced Telecom Operations Map (**eTOM), ensuring that new AI capabilities were introduced within a standardized operational framework.

The project builds upon stc's previously achieved **TM Forum Conformance Certification** for **Application Operations (OSO)**, reinforcing the organization's commitment to internationally recognized operational practices.

By integrating AI into existing eTOM-aligned operational workflows, stc maintained consistency in process governance while enabling more intelligent operational decision making.

This alignment ensured that innovation supported, rather than disrupted, established business processes.

Supporting Autonomous Operations:

One of the strategic objectives of this initiative is to contribute toward the industry's broader vision of **Autonomous Operations**.

Although human expertise continues to play a critical role in operational decision making, Artificial Intelligence now provides intelligent recommendations, behavioural insights, predictive analytics, and automated prioritization that significantly enhance operational effectiveness.

The deployment therefore represents an important progression along the journey toward increasingly autonomous operational environments where AI augments human expertise rather than replacing it.

As Machine Learning models continue to evolve, the organization expects additional opportunities to automate repetitive analytical activities while enabling operational teams to focus on higher-value investigative and strategic tasks.

Open Standards and Scalable Architecture:

The implementation also reflects the principles of open and scalable operational architecture promoted by TM Forum.

Rather than developing isolated AI capabilities, the project integrated Machine Learning within an existing enterprise operational platform, enabling interoperability with established fraud management processes, governance models, and operational workflows.

This architectural approach provides several long-term advantages:

* Preservation of existing technology investments.

* Incremental AI adoption with minimal operational disruption.

* Scalable deployment of future Machine Learning use cases.

* Simplified governance and operational oversight.

* Greater flexibility to support future digital transformation initiatives.

By combining standardized operational processes with intelligent analytics, stc has created an extensible operational framework capable of supporting future innovation across Business Assurance and Operational Excellence domains.

Industry Contribution:

Beyond its internal business value, this initiative contributes to the wider telecommunications industry by demonstrating a practical and repeatable model for AI adoption within Fraud Management and Revenue Assurance.

The experience gained through this implementation illustrates how Communication Service Providers can progressively introduce Artificial Intelligence while maintaining governance, operational stability, and alignment with internationally recognized frameworks.

The project therefore serves as an example of how AI can deliver measurable business outcomes while supporting the broader industry transition toward intelligent, standards-based, and autonomous operations.

TM Forum Alignment Framework

Purpose: Illustrate how the initiative aligns with TM Forum frameworks and strategic domains, showing the relationship between:

*** Business Assurance**

*** Revenue Assurance**

*** Fraud Management**

*** eTOM**

*** Application Operations (OSO)**

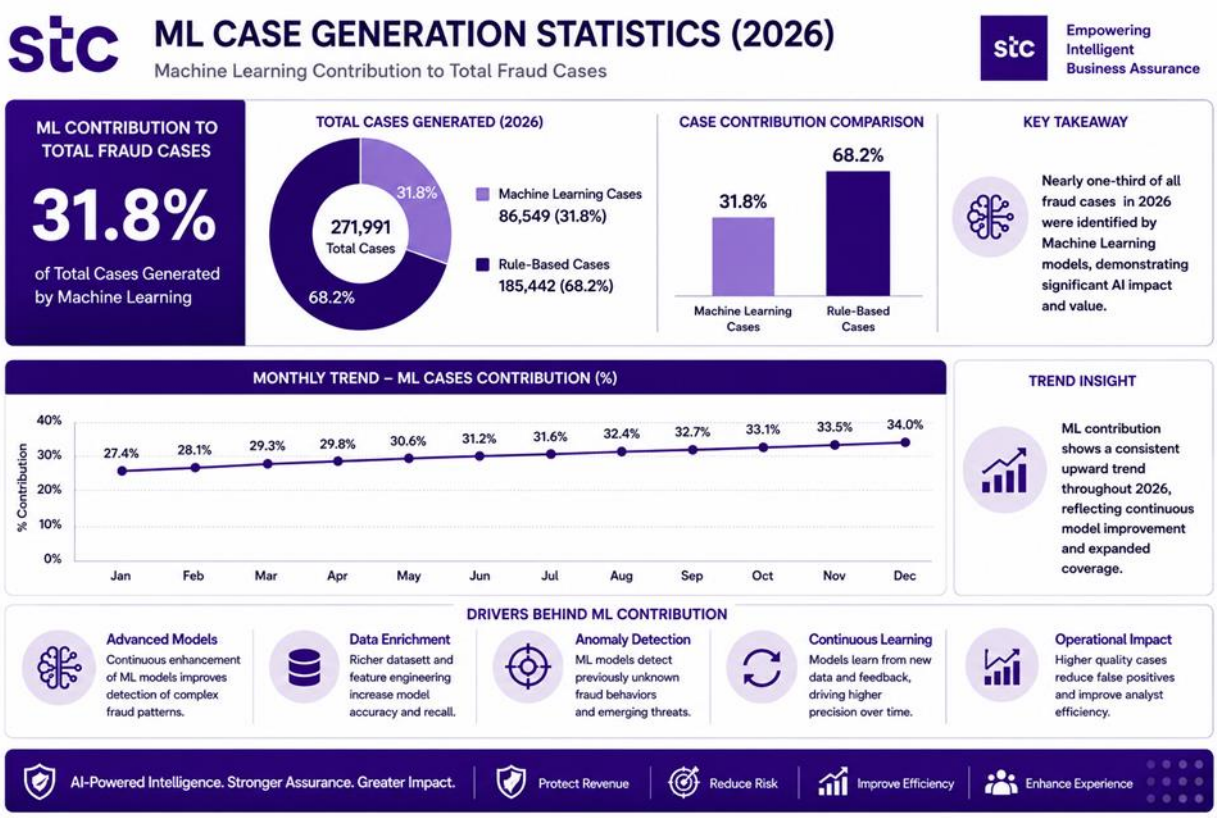
*** AI-Driven Operations**

*** Autonomous Operations**

*** Operational Excellence**

The infographic should position **AI & Machine Learning** at the center, demonstrating how these capabilities enable the evolution of Business Assurance while remaining fully aligned with TM Forum operational frameworks and open standards.

Lessons Learned and Operational Insights:



The successful deployment of Artificial Intelligence within stc's Fraud Management and Revenue Assurance (RAFM) environment generated valuable operational insights that extend beyond the immediate business outcomes.

Throughout the implementation journey, the project demonstrated that successful AI adoption depends not only on advanced technology, but also on strong governance, high-quality operational data, cross-functional collaboration, and continuous performance improvement.

These lessons now serve as guiding principles for future AI initiatives across Business Assurance and other operational domains.

Data Quality is the Foundation of AI Success:

One of the most significant lessons learned during the implementation was the critical importance of data quality.

Machine Learning models are highly dependent on accurate, complete, and well-governed operational data.

Considerable effort was invested in validating historical fraud datasets, improving data consistency, and ensuring that operational information accurately represented real fraud scenarios before model training commenced.

This investment significantly improved model accuracy while reducing false positives and increasing confidence in AI-generated recommendations.

Hybrid Detection Delivers Better Business Outcomes:

Rather than replacing traditional fraud detection methods, the project demonstrated that combining Machine Learning with rule-based controls delivers superior operational performance.

Traditional rules remain highly effective for detecting known fraud scenarios, while Machine Learning complements these controls by identifying emerging behaviours, previously unseen anomalies, and complex fraud patterns that are difficult to define through static business rules alone.

The hybrid approach has therefore provided a balanced operational model that combines explainability, governance, adaptability, and analytical intelligence.

Continuous Learning is Essential:

Fraud techniques continue to evolve rapidly across modern telecommunications environments.

Accordingly, Artificial Intelligence should not be viewed as a one-time deployment but as an evolving operational capability requiring continuous monitoring, periodic retraining, performance evaluation, and ongoing optimization.

stc established governance processes to ensure that Machine Learning models continue learning from new operational data while maintaining high levels of accuracy and reliability.

This continuous improvement approach enables the fraud detection environment to evolve alongside changing fraud behaviours.

Business and Technology Collaboration:

The initiative also reinforced the importance of close collaboration between operational, business, and technology teams.

The successful deployment of AI required expertise from Fraud Management specialists, Revenue Assurance professionals, Data Scientists, IT Operations teams, and AI engineers working together toward common business objectives.

This multidisciplinary collaboration accelerated implementation, improved solution quality, and ensured that Machine Learning capabilities addressed genuine operational challenges rather than purely technical objectives.

AI Augments Human Expertise:

Another key lesson from the project is that Artificial Intelligence delivers the greatest value when it supports, rather than replaces, experienced operational analysts.

Machine Learning provides intelligent recommendations, behavioural insights, anomaly detection, and case prioritization, enabling analysts to focus their expertise on higher-value investigations and complex decision-making activities.

The project therefore reinforces the principle that successful Business Assurance combines human expertise with intelligent automation to achieve optimal operational performance.

Operational Machine Learning Results (2026):

The operational statistics collected during the monitored period in 2026 provide clear evidence of the successful adoption of Machine Learning within the RAID-FMS fraud detection platform.

Operational Statistics:

Result	Performance Indicator
271,991	**Total Cases (Alarms) Generated**
86,549	**Total ML Cases (Alarms) Generated**
31.8%	**ML Contribution to Total Cases**

The results demonstrate that Machine Learning has become a core operational capability within stc's fraud detection ecosystem.

With nearly one-third of all generated fraud cases originating from AI-powered models, the initiative illustrates the growing operational maturity of intelligent fraud detection and the increasing role of Artificial Intelligence in supporting Business Assurance activities.

These statistics also validate the effectiveness of the hybrid detection architecture by demonstrating that AI-generated cases now represent a significant component of the overall fraud investigation workload while operating seamlessly alongside traditional rule-based detection mechanisms.

Preparing for the Next Stage of AI Evolution:

The operational experience gained through this initiative provides a strong foundation for expanding Artificial Intelligence across additional Revenue Assurance and Business Assurance domains.

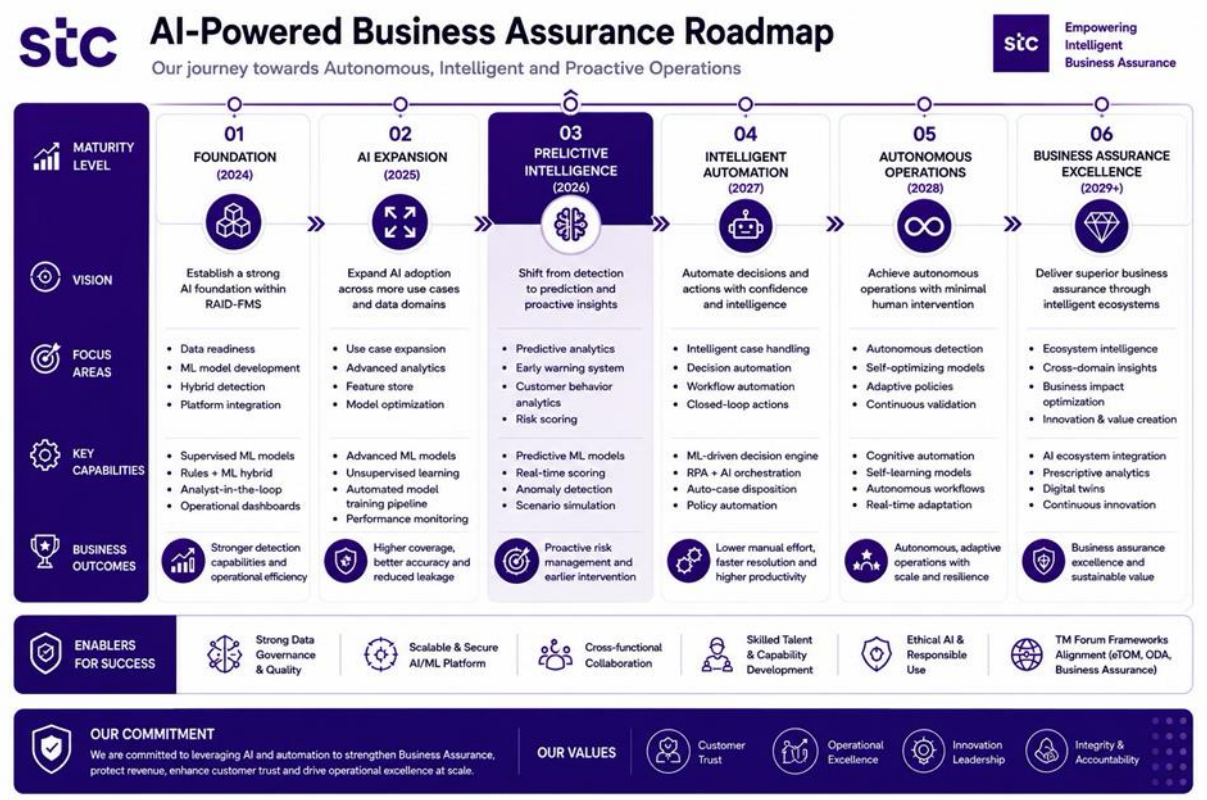
The lessons learned, governance model, and technical architecture established during this project can now be leveraged to accelerate future AI deployments while maintaining consistency with TM Forum best practices and operational standards.

AI-Driven Fraud Detection Workflow

Purpose: Illustrate the end-to-end operational lifecycle of AI-enabled fraud detection within the RAID-FMS platform, showing how data flows from network events through Machine Learning analysis, risk scoring, case generation, analyst investigation, and continuous model learning.

This infographic should emphasize the collaboration between AI and human analysts while highlighting the continuous improvement cycle that strengthens Business Assurance over time.

Executive Perspective:



The successful integration of Artificial Intelligence and Machine Learning into stc's operational Fraud Management and Revenue Assurance environment represents a significant milestone in the organization's digital transformation journey.

The initiative demonstrates that AI can generate measurable business value when implemented within a structured operational framework supported by strong governance, high-quality data, and cross-functional collaboration.

Rather than viewing Artificial Intelligence as a standalone technology, stc has positioned AI as a strategic operational capability that strengthens Business Assurance, enhances decision-making, and supports the long-term evolution toward intelligent and autonomous operations.

This project illustrates how Communication Service Providers can adopt AI in a practical, scalable, and standards-aligned manner while preserving operational stability and maximizing return on investment.

Executive Quote:

“The integration of Artificial Intelligence and Machine Learning into our operational Fraud Management environment represents an important milestone in stc’s journey toward intelligent operations. By combining advanced analytics with established operational practices, we have strengthened our ability to protect business revenues, improve fraud detection effectiveness, and accelerate operational decision-making. This initiative demonstrates how AI can complement human expertise while supporting the continued evolution of Business Assurance and Autonomous Operations.”

Organization Systems Operations

IT Operation Center

Service Excellence & Assurance

Technology

stc Group.

Future Outlook:

Building on the success of this initiative, stc continues to explore new opportunities to expand the application of Artificial Intelligence across Revenue Assurance, Fraud Management, and broader operational domains.

The experience gained through this project provides a scalable foundation for future innovation while supporting the organization’s long-term digital transformation strategy.

Future priorities include:

* Expanding Machine Learning capabilities to additional fraud scenarios.
* Introducing more advanced predictive analytics across Business Assurance processes.
* Increasing operational automation through AI-assisted decision support.
* Enhancing intelligent case prioritization and automated investigation workflows.
* Integrating additional data sources to improve fraud detection accuracy.
* Strengthening governance for AI model lifecycle management.
* Supporting the organization’s progression toward higher levels of Autonomous Operations.
* Continuing alignment with TM Forum frameworks, open standards, and industry best practices.

As Artificial Intelligence capabilities continue to mature, stc expects AI to become an increasingly integral component of operational excellence, enabling faster decisions, stronger revenue protection, improved customer trust, and greater organizational agility.

Industry Contribution:

Beyond the direct benefits achieved within stc, this initiative contributes to the broader telecommunications industry by demonstrating a practical implementation model for AI-enabled Fraud Management and Revenue Assurance.

The project provides evidence that Machine Learning can successfully coexist with traditional operational controls, creating a hybrid framework capable of delivering measurable business improvements while maintaining governance, transparency, and operational consistency.

By sharing this experience through TM Forum, stc aims to contribute to industry collaboration, encourage knowledge exchange, and support the adoption of intelligent operational practices across the global telecommunications community.

Closing Statement:

Artificial Intelligence is no longer a future ambition for telecommunications operators—it is becoming an essential capability for protecting revenues, strengthening operational resilience, and enabling intelligent decision-making.

This case study demonstrates how stc successfully transformed its Fraud Management capabilities through the practical application of AI and Machine Learning, delivering measurable business outcomes while remaining aligned with TM Forum frameworks and the industry's vision for Autonomous Operations.

The initiative establishes a strong foundation for continued innovation and reinforces stc's commitment to operational excellence, digital transformation, and leadership in AI-driven Business Assurance.

AI Roadmap – The Future of Intelligent Business Assurance

Purpose: Illustrate stc's future AI roadmap using a clean, executive-style roadmap aligned with the company's digital transformation strategy.

The roadmap should highlight the evolution from the current implementation toward future capabilities:

* **Current State** → AI-Enabled Fraud Detection (Completed)
* **Next Phase** → Expanded Machine Learning Use Cases
* **Future State** → Predictive Business Assurance
* **Advanced Stage** → Intelligent Automation
* **Target Vision** → Autonomous Operations aligned with TM Forum

The roadmap should use **stc's visual identity** (purple palette, clean icons, modern typography) and present a forward-looking vision that concludes the case study with a strategic message suitable for TM Forum publications.

References, Supporting Information and Publication Notes:

References:

The preparation of this case study was informed by internationally recognized telecommunications frameworks, operational best practices, and project documentation developed during the implementation of the AI-enabled Fraud Management initiative.

Primary reference sources include:

* TM Forum – Business Assurance Framework

* TM Forum – Enhanced Telecom Operations Map (eTOM)

* TM Forum – Autonomous Operations Framework

* TM Forum – Open Digital Architecture (ODA)

* TM Forum – AI and Data Analytics Best Practices

* stc Internal Revenue Assurance & Fraud Management Project Documentation

* RAID-FMS Operational Reporting and Machine Learning Performance Statistics (2026)

Supporting Operational Statistics:

The following operational statistics were extracted from the RAID-FMS production environment during the monitored period in 2026 and were used to support the business outcomes presented in this case study.

Value	Operational Indicator
271,991	**Total Cases (Alarms) Generated**
86,549	**Machine Learning Cases Generated**
31.8%	**ML Contribution to Total Cases**
≈15%	**Improvement in Fraud Detection Effectiveness**
≈7%	**Reduction in Revenue Leakage**
≈35%	**Earlier Fraud Identification**
≈20%	**Reduction in Investigation Effort**

The above figures are based on production operational monitoring and represent approximate business outcomes achieved during the observed reporting period.

Graphics and Illustration Sources:

To comply with TM Forum Case Study guidance, all graphics included in this document should reference their originating data sources.

Source	Graphic
Created from stc Solution Architecture (RAID-FMS)	**Hybrid Fraud Detection Architecture**
Based on stc Project Implementation Plan	**Project Timeline**
Based on validated project KPI measurements	**Business Outcomes Dashboard**
Based on TM Forum eTOM, Business Assurance and Autonomous Operations frameworks	**TM Forum Alignment Framework**
Created from operational Fraud Management processes	**AI-Driven Fraud Detection Workflow**
Developed from stc AI Strategy and Digital Transformation roadmap	**AI Roadmap – Future Vision**

Technologies Used:

The implementation incorporated a combination of advanced operational technologies, including:

* Artificial Intelligence (AI)

* Machine Learning (ML)

* RAID-FMS Fraud Management Platform

* Behavioural Analytics

* Anomaly Detection

* Predictive Analytics

* Big Data Analytics

* Revenue Assurance Processes

* Business Assurance Frameworks

* TM Forum eTOM

* Application Operations (OSO)

* Operational Performance Monitoring

Document Status:

Document Title:

Enhancing Revenue Assurance through AI-Driven Fraud Management: How stc Integrated Machine Learning into Operational Fraud Detection

Document Type:

TM Forum Case Study Draft

Prepared By

stc (Saudi Telecom Company)

Version:

Draft v1.0

Publication Status:

Internal Review Draft

Confidentiality Statement:

This document has been prepared solely for the purpose of developing a TM Forum Case Study submission.

Business metrics, implementation details, timelines, executive quotations, and supporting statistics are based on internal project information and remain subject to final business validation and approval prior to external publication.

No part of this document should be considered as an official public statement until formally approved by the relevant business stakeholders.

Acknowledgements:

stc would like to acknowledge the valuable contribution of the multidisciplinary teams whose expertise and collaboration supported the successful delivery of this initiative.

Special appreciation is extended to colleagues from:

* Revenue Assurance
* Fraud Management
* IT Operation Center
* Data Analytics
* Artificial Intelligence & Machine Learning Teams
* Digital Transformation
* Technology Operations
* Business Assurance
* Project Management
* Executive Sponsors

Their collective efforts enabled the successful deployment of AI-powered Fraud Management capabilities while supporting stc's ongoing digital transformation journey.

Conclusion:

This case study demonstrates how stc successfully integrated Artificial Intelligence and Machine Learning into its operational Fraud Management and Revenue Assurance environment to address evolving fraud challenges, strengthen Business Assurance, and deliver measurable business value.

Through the adoption of a hybrid fraud detection architecture, alignment with TM Forum frameworks, and a structured implementation approach, the initiative achieved improvements in fraud detection effectiveness, reduced revenue leakage, accelerated fraud identification, and enhanced operational efficiency.

Beyond the measurable results, the project establishes a scalable foundation for future AI-driven innovation and contributes practical experience to the wider telecommunications industry as it progresses toward intelligent, standards-based, and autonomous operations