OPTIMIZE BOTH THE DETECTION AND TECHNICAL PERFORMANCE OF YOUR FRAUD SOLUTIONS

In an era of ever changing fraud threats, rapid decision making and complex technological solutions, it's not uncommon for expensive investments in fraud detection to fail to reach their maximum potential, or over time to drift away from their ideal settings and processes. Organizations frequently struggle to understand how to create an effective, appropriate and measurable financial crime and fraud prevention operation, maximizing the detection capabilities of the underlying technology.

Our consulting fraud health checks provide actionable insight into the real performance of your existing Actimize Fraud solutions and operations, generating recommendations to improve fraud detection efficiency and reduce operational costs. Health checks also identify technical performance (i.e., throughput) degradation and hardware and software bottlenecks on your existing Actimize solutions, therefore ensuring business performance is not impacted by technical issues derived from your growth or changing information systems environments.

FRAUD CONSULTING HEALTH CHECK

Actimize's fraud health checks help you optimize the performance of your existing Actimize fraud detection solution, identifying and mitigating existing vulnerabilities. Health checks are formed of two optional components: Technical and Business Reviews.

TECHNICAL REVIEW

Technical Reviews (TR) address IT concerns regarding Actimize's solution performance (throughput) and stability.

Review Technical Architecture
- Review current hardware and software configuration, and current software architecture.
- Review integration with data sources and other point/channel solutions.
- Make recommendations for changes, if required.
- Review compatibility of Actimize with current versions of supporting 3rd party software (e.g., database) and required version uplifts.

Review System Logs and Performance
- Review Actimize production logs for errors or performance/bottleneck indicators.
- Review database statistics and logs.
- Identify performance issues –both processing transactions and/or having access to the RCM (alert and case manager) user interface.
- Make recommendations to resolve existing issues derived from system growth or configuration changes, if any.

Review Hardware Sizing
- Review current hardware sizing.
- Collect current volumetric information, planned data volume increases, and data persistence and storage requirements.
- Updated sizing recommendations.

BUSINESS REVIEW

The aim of the Business Review (BR) is to provide the business users in the fraud organization with guidance to improve how the Actimize fraud solution is used and configured. The BR's final objective is to increase the solution's ROI by:

- Reducing fraud losses.
- Increasing fraud detection rates.
- Reducing the operational cost of running the solution.

Review fraud objectives and threats

- Review payment channels, point solutions and types of transactions currently in use, as well as planned ones.
- Assess the suitability of the current solution and configuration for the actual and planned product offerings.
- Discuss current fraud threats and known fraud cases, identifying possible gaps in detection capabilities.
- Review staff resourcing and capacity planning needs.

Review actual metrics and reporting strategies

- Walk through management reports and metrics currently in use.
- Review number and type of fraud cases (both detected and missed), generated alerts and their false positive ratio.
- Discuss client observations.
- Discuss data collection processes which support reporting (for instance, the matching of fraud cases information to Actimize alerts).
- Determine focus areas to be addressed regarding analytics.

Review rules and assess rule strategy

- Review rules currently in use.
- Discuss rationale for each rule.
- Discuss rule performance (if known/measured).
- Identify under-performing rules.
- Recommend rule modifications (or retiring of rules, if appropriate).

Discuss current operational procedures and side-by-side observation

- Live observation and review of fraud analysts operation –"one day in the life of an Actimize user".
- Discuss current monitoring processes.
- Discuss insights from the operations team into model and rule performance.

Review suitability of available transaction and reference data

- Review data received in transactions.
- Assess suitability of received data to address the fraud threats exerted by every payment channel (for instance, in online originated transactions, is malware detection available?).
- Identify data gaps that may affect performance of Actimize's scoring models and policy rules.
- Review reference data available to enrich transactions and support investigations.
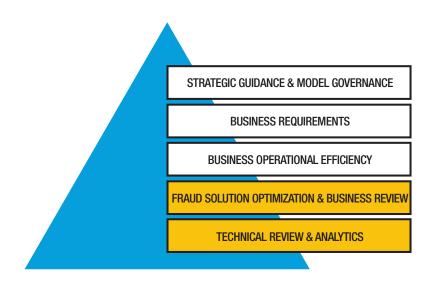
NICE ACTIMIZE FRAUD CONSULTING SERVICES

As organizations face new risks from evolving market conditions, new products, technologies, and fast-spreading fraud threats, they often struggle to create effective, appropriate and measurable financial crime and fraud prevention strategies and operations while maximizing existing systems and team resources.

NICE Actimize Fraud Consulting Services provide expert guidance, insight and knowledge to advise financial organizations on their fraud strategy and operational fraud management processes. Through a rich variety of fraud prevention consulting services, NICE Actimize helps organizations meet their challenges, maximize technology investments and identify and mitigate existing vulnerabilities.

DELIVERING ACTIONABLE INSIGHT

- STRATEGIC GUIDANCE & MODEL GOVERNANCE
- BUSINESS REQUIREMENTS
- BUSINESS OPERATIONAL EFFICIENCY
- FRAUD SOLUTION OPTIMIZATION & BUSINESS REVIEW
- TECHNICAL REVIEW & ANALYTICS

Health Checks are comprised of Business and Technical Reviews, which are part of the rich catalog of NICE Actimize Fraud Consulting Services.