ClearPriority®

FIVE CRITICAL STEPS TOWARD BETTER RISK MONITORING

S.A. CLEARPRIORITY N.V.

WATERLOO OFFICE PARK
BUILDING K
DRÈVE RICHELLE 161
B-1410 WATERLOO

PHONE: 32(0)2 352.91.70
FAX: 32(0)2 352.91.79
E-MAIL: info@clearpriority.com
WEB: www.clearpriority.com

TVA/BTW: 0897.676.897
FORTIS BANK: 001-5524603-44

ClearPriority®

The Challenge of Customized Risk Management

In today's global economy, risk has become an everyday part of conducting business. Organizations are subject to hazards unheard of a few years ago -- from supply chain disruption and business continuity risk, to fraudulent transactions and regulatory non-compliance.

The rise of government-mandated compliance regulations, from Sarbanes Oxley to Basel II and Solvency II, is also forcing organizations to adopt Governance, Risk and Compliance (GRC) initiatives and proactively manage their risk exposure.

A multitude of incidents and losses can result from external and internal events -- including risks from people, technology and failed processes. Damage from these risks can be measured in financial terms, loss of customer confidence and brand equity.

These risks, however, can't be entirely eliminated, since they're often at the core of an enterprise's activity. Most of the advances in the economy have been the result of companies taking risks. What organizations should aim for, instead, is making good risk monitoring and management "an organizational imperative". Indeed, risk management can become a key driver of success to minimize losses and improve business performance.

Many organizations approach Governance, Risk and Compliance (GRC) initiatives in a disparate and ad hoc fashion, for example by segregating risk issues by division, line of business, or geography. They struggle, as a result, with a costly patchwork of solutions for every risk or compliance challenge they face. Most of the data associated with these risk events is scattered and isolated in many separate back-end systems and independent applications. What's more, as an organization's risk environment grows in size and complexity, it becomes even harder to monitor the risks that are critical to the enterprise.

This paper discusses the key event monitoring capabilities that are needed to address critical risk vulnerabilities in today's volatile business environment.

ClearPriority®

The Need for a Pragmatic Risk Monitoring Approach

Effective risk management increasingly requires the ability to respond flexibly to changing business conditions. As a result, decision-makers need the capability to actively monitor their risk environment in real-time and all the time.

Today's organizational and IT infrastructures that are dedicated to risk management, however, are increasingly diverse and complicated. Point solutions, for example, have typically been organized around specific regulations and standards frameworks, such as Sarbanes Oxley and Basel II, or MiFID. Because they operate independently -- each with their respective owners and processes -- getting risk event data in and out of these applications to manage critical risks can be inefficient and time-consuming.

Managing risk in a volatile environment thus requires bridging gaps in GRC management coverage across the enterprise, in order to provide broad visibility into those key vulnerabilities that will likely impact the bottom line.

A specific program devoted to monitoring customized, high-impact risks should employ both a top-down and a bottom-up process of risk identification. From a top-down perspective, the company's GRC leadership should identify the critical risks that are large enough in aggregate to threaten the firm with distress in an adverse environment. A bottom-up process, however, should also contribute to senior management planning: business units and functional areas need to assist in identifying material local-level risks. The goal is to aggregate these individual risk events with other events to produce a company-wide risk profile that takes into account correlations among risk events.

This high-impact risk management program also requires a monitoring infrastructure that can collect, correlate and analyze vast sums of data across the enterprise, as well as provide real-time incident response. It should provide Risk Officers with flexible tools to analyze in a reasonable time-frame event data on critical vulnerabilities, and to rapidly implement controls on risks that are not covered by existing solutions – such as supply chain monitoring, non-compliance with corporate policies, or abuse and fraudulent activity.

Such a structured initiative can ensure long-term benefits – such as helping mitigate key risk exposure, ensure that organization-specific risks are covered, and enhance corporate governance.

ClearPriority®

Only An Application-Independent Platform Can Monitor Company-Specific Risks

Today's volatile environment requires the ability to overcome fragmented risk and compliance functions in the enterprise. It calls in particular for a special monitoring infrastructure for centrally viewing, monitoring and analyzing high-impact risks across the organization.

Designed to automate organization-specific monitoring and analytical tasks, this infrastructure should also support continuous monitoring processes to meet the demand for real-time reporting and escalation of risk event information.

Specifically, it should allow quick implementation of controls. Companies need to look at where they can automate controls -- both at company and process levels -- based on their risk objectives. These controls can highlight thresholds in a variety of contexts, such as fraud prevention, or regulatory non-compliance. They should support two distinct objectives:

- *Real-time alerting* that highlights the occurrence of risk events in business or IT domains, so staff can quickly react to and manage incidents, such as regulatory violations or business disruptions.

- *Risk analytics* reflecting the interaction of risks across multiple enterprise domains. Key Risk Indicators (KRIs), in particular, should be used to track the risk exposures linked to each defined risk, and display the associated metrics. These analytics capabilities should be configurable, as no two organizations will have the same set of KRIs and linkages.

In conclusion, this real-time risk monitoring platform must be deployed without change to existing systems and processes. Its full range of capabilities must be put into the hands of non-technical users, enabling them to rapidly respond to a changing risk environment. Risk Officers, for example, should be able to easily update automated controls, and align them with changes and new business demands, such as regulatory changes and new business activities.

Designed to facilitate on-the-fly adaptation to critical risk situations, this customized risk monitoring platform and initiative should support *five fundamental capabilities*:

1 Customized Risk Assessment

Strategic and operational risk management objectives can be extraordinarily diverse, reflecting a broad range of activities in an organization – from quality monitoring to business continuity and compliance management.

Today's fast-moving business environment requires ongoing control monitoring, changing and adjusting to reflect rapidly evolving market conditions. This means that Risk Officers must identify – in a pragmatic manner -- the risks that are most important to their business. For example, they need to

review information from the systems that support critical aspects of the business, and categorize and prioritize key risk vulnerabilities.

With this preparatory assessment, management can identify critical gaps that are not covered by existing solutions. Once these critical vulnerabilities have been identified, it's time to quickly deploy controls at these critical risk points that will continuously validate vital information, processes and key business indicators.

Critical risks may touch different systems within an organization, drawing upon many kinds of data and information. To implement controls on these high-impact risks, Risk Officers need to determine the information sources and the basic data elements that must be extracted and managed across a variety of IT and business applications, systems and databases.

2 Customized Event Data Extraction

As IT systems and applications become increasingly distributed, organizations face complex data integration issues. They can impact the management of Governance, risk and Compliance, since the detection of risk events often spans time and geography, and involves multiple correlations against disparate sources.

A vast array of data from such disparate sources as business and organization-specific systems -- including financial, help desk, supply chain, and sales management applications -- must be sifted in real-time to determine an enterprise's critical risk posture. Some of these sources frequently have different logging formats and reporting mechanisms.

A flexible extraction system is therefore needed to capture data from an organization's assets and resources. Continuous, automated data extraction processes must be capable of interfacing with the IT databases and processes that comprise the organization's knowledgebase.

Some of these processes can leverage a minimally invasive, agent-free approach. Risk event data, for example, is automatically extracted from devices producing this data natively -- including operating systems, ERP and CRM systems.

When it comes to capturing specific or proprietary data, however, extraction agents are the simplest way of feeding this information into an Extractor, Loader and Transformer (ETL). These small programs, supporting such standard interface protocols as XML, Syslog, or SNMP, run on servers, clients, firewalls, and other devices, collecting customized risk data across the enterprise.

In high-risk monitoring environments, this extraction mechanism should be capable of capturing data from disparate sources at speeds reaching thousands of events per second.

3 Customized Extraction, Transformation and Loading

A dedicated Extractor, Transformer and Loader (ETL) simplifies data management, by eliminating the need for costly interfaces needed to pull information from multiple platforms.

ETLs can help manage cross-departmental risk information by unifying information silos. By manipulating risk data effectively -- regardless of format, size, source or target -- they provide a continuous mechanism that enables the automation of monitoring tasks.

An ETL must accommodate high-throughput, real-time analysis of rapid-fire, sequential events. It interprets logs that are produced by standard sources (SAP, Windows, Unix…) and proprietary applications, and filters out irrelevant data.

Transformation rules then convert the data from these different sources into a normalized format that aggregates individual risk event data into critical, corporate-wide vulnerability information.

Finally, once these filtering and normalization operations have been completed, the ETL feeds this normalized risk event data into an analysis environment that's designed to create and execute intelligent analysis processes.

4 Customized, High-Speed Risk Event Analysis

A good customized GRC monitoring platform must be capable of sorting out trends from hundreds of real-time events occurring across many systems and applications.

A powerful analysis environment should provide end-users with a mixed range of tools – including rules design templates and wizards, a real-time rules engine, as well as policy and procedure dictionaries –for identifying all forms of risk, irrespective of type, source and location. The rules engine, in particular, should correlate chains of risk events in real-time and relate them to the appropriate key risk indicators.

By using intuitive editors, Risk Officers can define a variety of business rules based on risk scenarios, and consolidate and prioritize metrics into critical risk categories. This analysis must be flexible enough to cover a wide variety of risk scenarios. For example, it must support complex correlations and cross-references across time, geography and disparate sources to detect complex events. Risk Officers can implement two distinct sets of rules:

- *Alert rules* in order to gather risk event intelligence and provide early warning of changes to factors that could impact the risk environment. These rules should point Risk Officers directly to breakdowns as they occur, and provide context around anomalous risk events for easy reporting and remediation.

- *Analysis rules* to provide the intelligence needed for analytic measurements that are specific to your business. These more complex rules leverage past and present metrics to assess an organization's risk posture, pinpoint exceptions, and highlight potential areas of concern. They generate the streams of data that drive Key Control Indicators (KCIs), Key Risk Indicators (KRIs) or Key Performance Indicators (KPIs) highlighting risk exposure.

Finally, this powerful analysis environment must execute hundreds of complex rules simultaneously in real or near real-time, to detect interrelated risk events.

What KRIs, KCIs and KPIs Can Do For You

A high-impact risk monitoring platform should enable the rapid design and updating of controls across a variety of risk areas to provide the factual basis for decision-making.

Key Risk Indicators, (KRIs), Key Control Indicators (KCIs) and Key Performance Indicators (KPIs), in particular, provide the metrics that are used to help an organization define and measure risk exposure. These measurements, observed or calculated, indicate the presence of conditions or trends that impact certain risks.

These indicators enable data analysis on an ad hoc basis, at regular intervals, or when triggered by a particular risk event.

They provide control points on a wide variety of custom risk events -- from financial transaction associated with people with certain levels of responsibility, to authorized purchases by a given employee in a Purchasing Department -- and optimize operational decisions and business performance.

ClearPriority®

5 Customized Dashboard Creation

A real-time graphical interface is required to provide insight into critical risks across the enterprise.

This interface, via dashboards and executive reports spanning multiple domains across lines of business, should easily display the organization's overall risk posture, including vulnerability and incident management trends.

This reporting capability needs to be flexible, so that risk officers can quickly customize alert displays to identify real-time incidents and escalate alert notifications. For example, these customizable dashboards should combine real-time and historical views of information to provide a basis for pro-active risk analysis, and should also support multiple layout formats.

Alert Management

Whenever a risk event occurs, this portal, should send alerts in real-time, enabling risk officers to immediately deal with a risk incident. An alert dashboard's key attributes may include:

- *Alert highlighting, based on the location and severity of an event*
- *Result prioritization*
- *Instant escalation of critical risk events, allowing risk officers to respond immediately to emerging problems or new opportunities*

KCI, KPI, KRI Management:

Business analysts should also leverage this platform to quickly create and display KCIs, KPIs and KRI metrics used for monitoring business activity. These KCIs must be continuously updated in graphic displays.

A well-defined risk and management dashboard allow Risk Officers to design and highlight the metrics that are important. Decision-makers can quickly determine if a risk posture can be managed to business expectations. Dashboards can typically include metrics on internal controls, credit and market risks, environmental risks, or vertical market regulations.

User-initiated drill down capabilities should let users interact with the system's rules in real-time, and let staff zero in on key vulnerabilities affecting their enterprise.

A level of granularity should be provided so end-users can work at the indicator level, and drill down to refine their analysis to quickly identify problem areas among thousands of processes, risks and controls. A forensic capability should also be provided for statistical and trend analysis activities.

ClearPriority®

The ClearPriority Difference

As the first application-independent risk monitoring platform, ClearPriority introduces a new generation of real-time, risk monitoring solutions. This robust, real-time monitoring infrastructure can be applied to a large number of business and technology solutions across multiple industries.

By leveraging data from an organization's existing Governance, Risk and Compliance technology and tools, ClearPriority allows Risk Officers to rapidly implement organization-specific controls across multiple functional and geographical areas in an enterprise.

ClearPriority fits easily into any GRC program. Its application-independent infrastructure provides the flexibility needed to assess and monitor critical risks in real-time, in ways that were never before possible.

The platform's flexibility allows the real-time monitoring of complex events across multiple risk domains in the enterprise and in accordance with pre-defined business rules. It provides the following facilities in an easy-to-use monitoring environment:

Risk Information Production:

- *Ability to connect to a wide variety of enterprise information sources, such as applications, databases, servers, and network devices in literally hours, using web-based screens*
- *Comprehensive extraction and correlation rule customization via an easy-to-use SDK.*
- *Custom metrics development through wizards and templates*

Risk Information Delivery:

- *Customized reporting via dynamic dashboards, charts ad reports for real-time risk monitoring and analysis*
- *User-defined drill-downs offering the ability to see patterns and risk issues at a granular level*
- *Real-time alerting based on triggers that evaluate when risk indicators are changing out of tolerance with established business rules*

Management and Administration

- *Deployment of a variety of event detection capabilities across diverse legacy systems and enterprise applications*

Deployed as an appliance, ClearPriority features a small footprint, reducing deployment time and avoiding interference with other applications.

The platform provides a flexible way of adapting to today's volatile risk environments. It establishes a clear mechanism for monitoring critical risks, and for bridging Governance, Risk and Compliance management gaps across organizations.

About ClearPriority:

A leader in the field of real-time Governance, Risk and Compliance monitoring solutions, ClearPriority's mission is to help shape the future of risk monitoring through an open and flexible platform supporting a multitude of risks facing enterprises in today's volatile environment.

Headquartered in Waterloo, Belgium, the company delivers the first open and general-purpose monitoring platform designed to facilitate the deployment of customized controls in the enterprise.