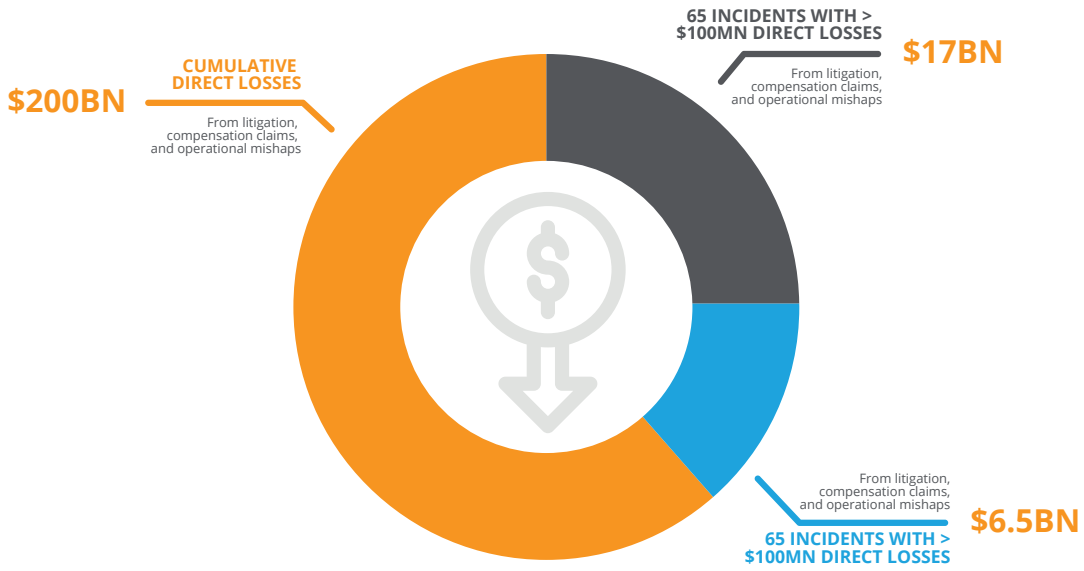
Building a Shareholder Value-Focused Integrated Risk Program

TABLE OF CONTENTS

1. Shareholder Value (Rather Than Financial Loss) Drives Integrated Risk Program Outcomes

Today, financial institutions operate in highly dynamic business environments facing high-impact and very frequent disruptions. "Known unknowns" can come at organizations from anywhere, be it in the form of operational technology outages or extended ecosystem vulnerabilities (To know more, read MetricStream's report GRC 2019: The Known Unknowns). The challenges brought about by these disruptions in business models, customer expectations, technology advancements, and regulatory expectations have significantly increased non-financial risk (NFR) exposures[1]

The direct financial losses and fines from non-financial risk incidents are large and visible. They are also immediate in terms of impact, and are thus reported publicly more frequently. Between 2008 and 2012, the top 10 global banks faced astounding cumulative direct losses of over $200 billion with 17 individual incidents posing direct financial losses of more than $1 billion.



DIRECT NFR RELATED LOSSES[1]
Between 2008-2012 for Top 10 Banks

The much larger impact of non-financial risk incidents lies in the long-term erosion of shareholder value.

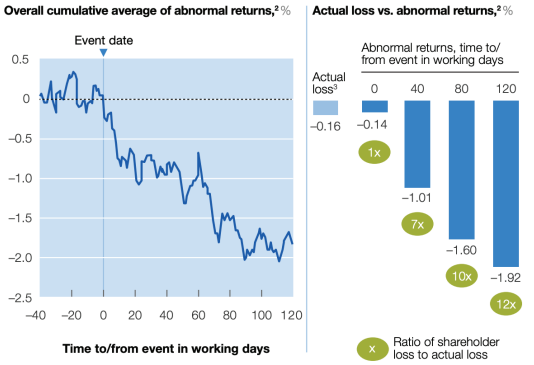
Customers and markets are especially sensitive to non-financial risk events. Therefore, these events often result in the longer-term erosion of shareholder value. In a recent study by McKinsey & Company of more than 350 operational risk incidents at financial institutions in the US and Europe, it was found that the initial declines in the total returns to shareholders (TRS) were in line with the actual fines of $23 billion (from 350 events). However, over the next 120 days, the TRS of the sample taken declined by a staggering $278 billion, more than 12 times the total actual loss of $23 billion.

[1]Nonfinancial risk: A growing challenge for the bank (2016) by Piotr Kaminski, Daniel Mikkelsen, Thomas Poppensieker, and Anke Raufuß. Published by McKinsey & Company.

Exhibit 1

It gets worse.

Impact of operational-risk event on market returns[1]



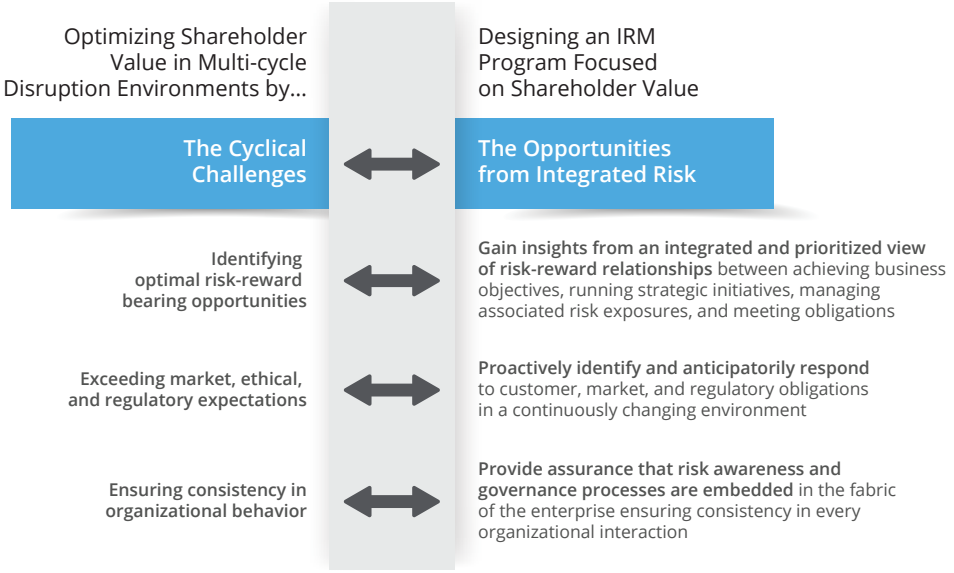
[1]For 350 operational crises experienced by financial institutions in Europe and North America.
[2]Abnormal returns for each stock calculated daily as difference between actual and expected returns, adjusted for movements in broad market index; unweighted average of daily abnormal returns calculated across all operational-risk events to prevent "noise" of particular stocks from distorting overall results.
[3]As share of total market capitalization.
Source: Fitch Ratings; Thomson; McKinsey analysis

A proactive response strategy has a large impact on stemming the erosion of shareholder value.

A deeper understanding of the impact of risk events, coupled with faster communication of the same to customers and markets, helps slow down and lower the erosion of shareholder value. Markets tend to respond to possible future loss scenarios from imminent non-compliance related fines even before they are imposed. Organizations with a proactive response to immediate and possible losses and fines have empirically proven to recover some of the eroded TRS value within three months. In a recent market example, Facebook's stock price declined by 24% as information began to emerge about their data breach involving Cambridge Analytica and 87 million users. However, Facebook swung into proactive action with CEO Mark Zuckerberg communicating that data abuse prevention is a priority (and a mistake made in the past). As news spread of Facebook's commitment to taking down 837 million pieces of spam and 2.5 million pieces of hate speech, while also disabling 583 million fake accounts, and pledging a task force of 20,000 people for security, the company's stocks rebounded by 32% over the next three months.

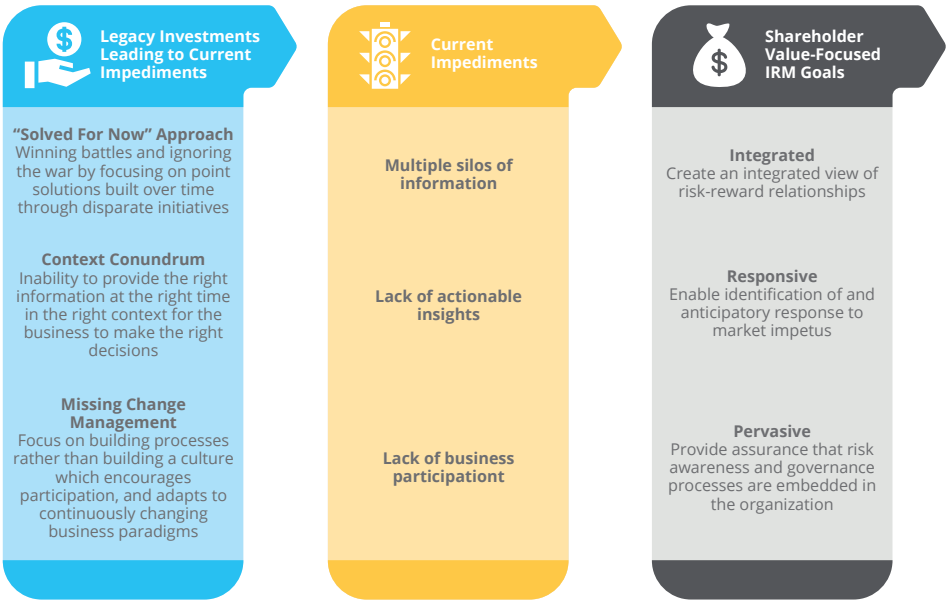
An integrated risk program (IRM), designed to focus on the optimization of shareholder value (and not just direct losses), provides organizations with the unique ability to predictively identify and proactively (possibly pre-emptively) respond to non-financial risk events.

A risk program focused on direct loss only ends up meeting and responding to specific obligations emerging from regulations or policies. On the other hand, a shareholder value-focused integrated risk program is designed with the objectives of (a) gaining insights from an integrated and prioritized view of risk-reward relationships, (b) proactively identifying and anticipatorily responding to obligations, and (c) providing assurance that risk awareness processes are embedded in the fabric of the enterprise. A key differentiator of a shareholder value-focused integrated risk management program is its focus on establishing a relational universe between shareholder value indicators, strategic initiatives driving those indicators, associate material risks facing the initiatives, and market/regulatory obligations aligned to those risks. While most institutions have already implemented some disparate and fragmented elements of an integrated risk program, an effort to place a premium on preserving shareholder value will create additional responsibilities.



2. Shareholder Value-Focused Integrated Risk Management – Bridging The Gaps Between Risk And Shareholder Value

Over the years, organizations focused on shareholder value generation have demonstrated a higher probability of success with their long-term growth strategy. A Harvard Business Review research publication identified that organizations that have created and continue to create shareholder value do so by focusing on some common enterprise strategies. These strategies comprise vision statements, strategic objectives, tactical direction plans, and program governance principles which protect and grow shareholder value. While the implementation of these strategies varies from business to business, the core principles to optimize shareholder value are universally applicable across regions, industries, and organizations.



The risk program landscape within organizations is often fragmented and disjointed. Businesses have made disparate legacy investments in standalone risk programs to meet specific needs arising from changing regulatory requirements. The sole focus is on restricting direct losses. Thus, most organizations today are at a stage where there are multiple silos of information that prevent the business from understanding the impact of material risks and market/regulatory obligations from a shareholder value perspective. Many organizations have understood the need to integrate their risk programs, and some have already embarked on the path towards doing so. Building and aligning an integrated risk program that is focused on shareholder value involves establishing programmatic components which drive the goals of integration, responsiveness, and pervasiveness through certain processes and technology infrastructural capabilities.

The Holy Grail lies in bridging the gaps by building critical capabilities for shareholder value-focused integrated risk management, in terms of both process competencies and technology infrastructure.

The process of bridging the gaps involves integrating the various programmatic components and risk metrics (that are being tracked in the current disparate and direct loss focused risk management program) with the strategic initiatives and objectives which optimize shareholder value. By bridging the gaps, organizations set up an accountability loop to integrate data from the identification and measurement of material risks and market/regulatory obligations across different points of the organization. This data is brought into the current risk program and aligned to the financial and operational metrics that are being tracked by the business for the strategic initiatives driving shareholder value.

In the table below, we look at some of the critical capabilities to bridge the gaps (stated in column 3) which, when implemented, will align the current disparate risk program components and risk measurement metrics (stated in column 2) to the expected outcomes from established industry best practice strategies for optimizing shareholder value (stated in column 1).

Enterprise Strategies to Optimize Shareholder Value[2] *Expected outcomes which drive higher shareholder value*	**Current Disparate Risk Management Program Components and Metrics** *Existing risk measurement processes and metrics*	**Critical Capabilities for Bridging the Gaps between Risk & Shareholder Value** *Capabilities of shareholder value-focused integrated risk programs*
What is the expected outcome? OPTIMIZE FOR EXPECTED VALUE Organizations should evaluate and compare strategic decisions in terms of the expected incremental value of longer-term future cash flows, as opposed to the estimated impact on shorter-term reported earnings ***What is needed to achieve it?*** A sound strategic analysis should produce informed responses to three questions: 1. How do alternative strategies affect value? 2. Which strategy is most likely to create the greatest value? 3. For the selected strategy, how sensitive is the value of the most likely scenario to potential shifts in competitive dynamics and assumptions about technology life cycles, regulatory environments, and other relevant variables?	***What is currently available?*** In terms of risk process capabilities and metrics • The capability to **measure risk exposures in a single isolated context** e.g., risk of disruption for a given technology asset • **Fragmented risk measurement methodologie**s for most risk categories and asset classes without a common taxonomy or universe • **Silos of risk reports** being generated within specific risk tools running within different risk groups	***What is missing?*** AGGREGATE RISK EXPOSURE FOR CURRENT AND ALTERNATIVE STRATEGIC INITIATIVES AND OBJECTIVES ACROSS ALL RISK CATEGORIES AND ASSET CLASSES ***The relational links to be built will:*** • Establish a relationship between organizational objectives, strategic initiatives, material risks, and regulatory/market obligations • Identify, measure, communicate, and evoke responses for risk events and their impact across the correlated risk and business universe, all the way to the business objectives and strategic initiatives • Enable a forward-looking scenario analysis and predictive risk analysis of aggregated and contextualized risk information from multiple risk programs and technology infrastructure using an integrated and federated risk taxonomy and reporting framework ***How to build the relational links?*** "Value discovery and the art of the possible"
What is the expected outcome? MAXIMIZE ASSET VALUE Organizations depend on the resiliency (which is a function of the efficacy, efficiency, and availability) of its multiple revenue-generating assets like financial capital, human capital, technology infrastructure, and process competencies. Protecting and preserving the value of these assets drives long-term growth.	***What is currently available?*** In terms of risk process capabilities and metrics • **Disparate and standalone risk mitigation and control testing programs** focused on individual assets, business units, or processes • **Control assessments and ratings** which cannot be aggregated, compared, or validated for consistency • **Silos of risk mitigation and control test related actions** being tracked by different business and functional units	***What is missing?*** AN INTEGRATED AND FEDERATED RISK MITIGATION AND CONTROL TESTING PROGRAM FOCUSED ON BUILDING THE RESILIENCE AND, HENCE, PERFORMANCE OF CRITICAL BUSINESS SERVICES ***The relational links to be built will:*** • Identify and correlate critical business services, expected performance levels, supporting assets, and their associated controls • Build and automate the control testing program to increase the scope and scale of coverage while predictively identifying trends in business service performance
What is needed to achieve it? A sound strategic analysis should produce informed responses to three questions: 1. Which are the critical services and assets supporting the business? 2. Which assets are likely to under-perform and in which circumstances? 3. How are the critical assets protected from disruption and under-performance, and how does one drive their efficiency and efficacy?		• Measure and report on the efficacy and efficiency of the business resilience program modernizing and rationalizing the control program ***How to build the relational links?*** "Business service resilience focused federated control program design"
What is the expected outcome? REWARD OPERATING-UNIT EXECUTIVES FOR ADDING SUPERIOR MULTI-YEAR VALUE Organizational strategy gets implemented through the business decisions made by the operating unit executives in the front line of the business. Incentive structures and culture-building should encourage the operating unit executives to make decisions balancing long-term growth factors over shorter-term "quick win" metrics ***What is needed to achieve it?*** A sound strategic analysis should produce informed responses to three questions: 1. Are the operating unit executives aware of the long-term growth objectives and strategic vision? 2. Are the operating unit executives able and incentivized to contextualize the long-term growth objectives to tactical level decision-making? 3. Is there an organizational feedback framework which prevents and alerts the business to deviant behavior?	***What is currently available?*** In terms of risk process capabilities and metrics • **Non-contextualized risk and obligation related information from multiple sources** built by the second line of defense functions • **Complicated risk and control assessment capabilities** built for subject matter experts • **Silos of issue reporting and remedial action planning** being tracked by different business and functional units	***What is missing?*** PROVIDING THE FRONT LINE WITH BUSINESS DECISION CONTEXTUALIZED RISK INTELLIGENCE WHILE COLLECTING RISK INFORMATION FROM THEM ***The relational links to be built will:*** • Map front line business operating executives, their supported business services, risks, and obligations associated with the business services • Simplify and enable front line defense functions to pervasively collect risk information while non-obtrusively providing them with risk information in real time and in the right context • Integrate the issue management framework to identify key trends, rationalize remedial actions, and provide senior executives confidence on the activities of the operating units ***How to build the relational links?*** "Crowdsourcing risk data"

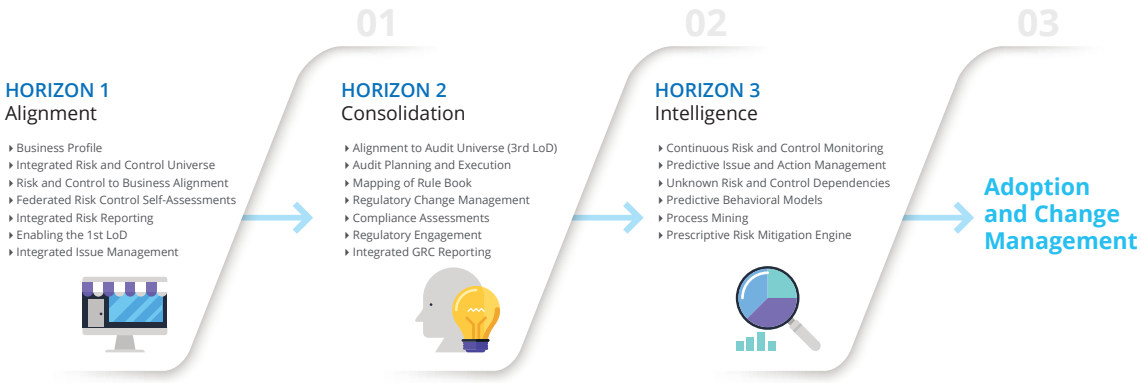
[2]Ten Ways to Create Shareholder Value by Alfred Rappaport. Published By Harvard Business Review

3. Operationalizing the Shareholder Value-Focused Integrated Risk Program – Programs to Bridging the Gaps

3.1 Value Discovery and the Art of the Possible

Current risk programs are at varying levels of maturity and consolidation considering the legacy of disparate investments in "point in time, solve for now" risk programs and their supporting technology infrastructure. With the "value discovery and the art of the possible" framework, organizations should build:

1. A three-horizon growth model which is used to define the outcomes of the integrated risk program across three horizons of growth spread over time and aligned to strategic objectives.

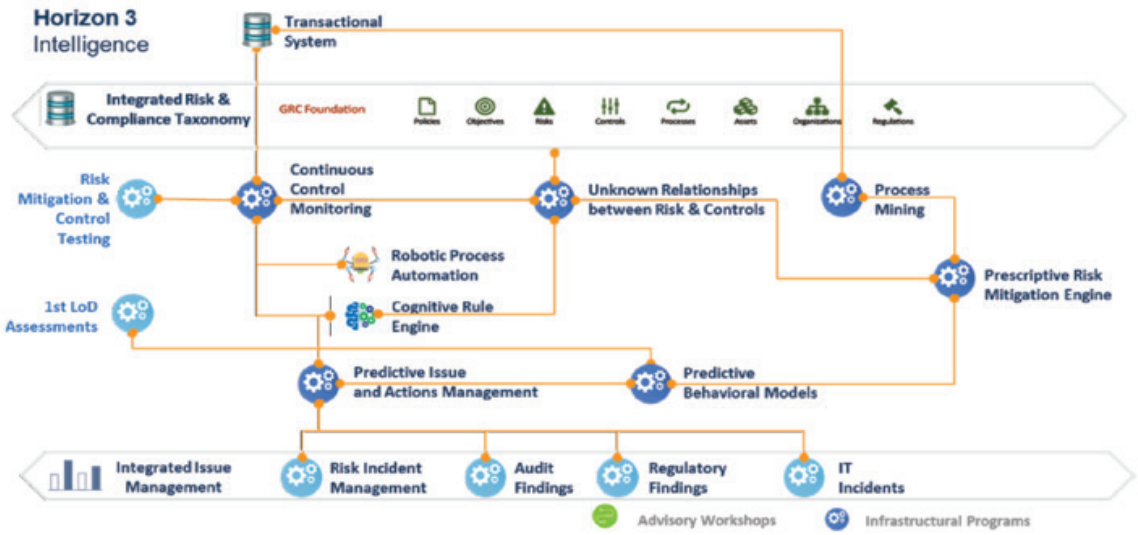


THE 3 HORIZON MODEL
Defining The Possible

Each horizon outcome is defined collaboratively with various stakeholders from business and risk programs, understanding the (1) current risk data maturity, (2) current risk technology infrastructure maturity, and (3) current risk process and skill maturity. Each horizon should be achievable and time-bound.

2. A technology-agnostic IRM program roadmap which lays out the actionable milestones for each horizon in terms of the required process competencies and technology infrastructure. Both factors can be mapped to an existing program or built where there are gaps. The technology agnostic roadmap requires a deep understanding of process-related best practices, the current and future direction of technology capabilities, and the current state of the business and its risk program.

One of the key outcomes of the technology agnostic roadmap is the ability to migrate to a single source of truth from existing multi-point sources of risk and obligations data. Organizations will be able to integrate and rationalize foundational data elements across the organizational hierarchy, associated business objectives, risks, controls, and regulatory requirements.



The other key outcome of this stage is the ability to determine the future of the integrated risk program – i.e., identifying risk and compliance use cases to apply predictive analytics and artificial intelligence (illustrative example above). In this phase, organizations need to design the business user journeys which will define how they interact with the integrated risk program. This will help them further quantify the direct financial benefits from increased efficiency and effectiveness.

3. A value discovery-based business case which quantifies critical risk events, including their impact and frequency on critical business services. Using a unique and proprietary methodology, organizations can calculate the enterprise value at Risk (EVR) from the risk to objective relationships established within the "art of the possible technology agnostic road-map". The roadmap also provides a view of the total cost of the program (COP). Finally, it quantifies the financial benefits (FB) from business user journeys which is a part of the art of the possible workshops. The business case is then developed using the following formula:

Expected Value = Enterprise value at risk (EVR) - total cost of the program (COP) + financial benefits (FB)

3.2 Business Service Resilience Focused Integrated Control Program

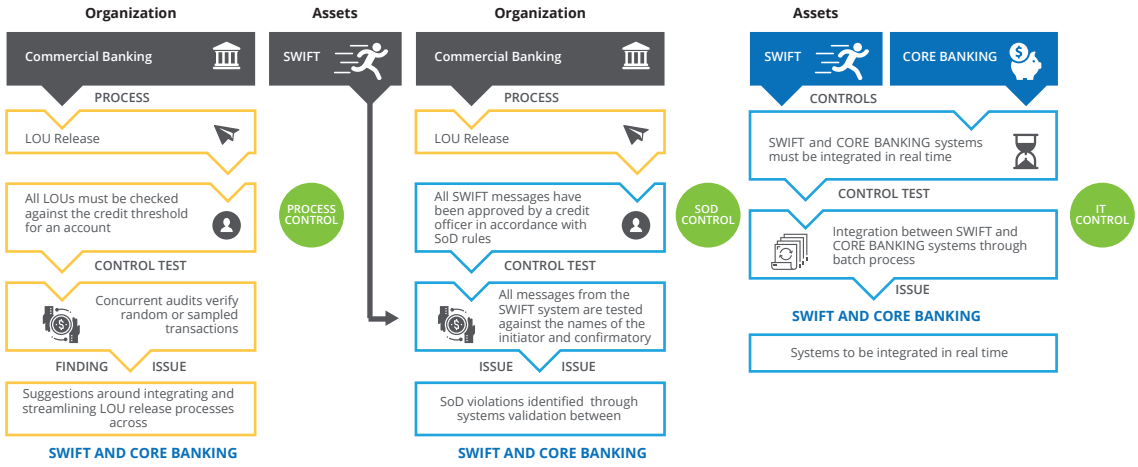
Most organizations have control programs that are defined but dispersed within business and functional units without any integration between them. This approach often leads to redundancies and inconsistencies. Without a focus on and alignment to critical business services, controls often operate as "orphans," unable to fulfil the business requirement of increasing resilience (which is a function of the efficacy, efficiency, and availability of a revenue generating asset). With a "business service resilience focused integrated control program framework," organizations can enable

1. Control mapping and a federated control program design which maps the various control landscapes within individual 1st line of defense business units, 2nd line of defense functional units, and 3rd line of defense assurance functions. The multi-dimensional relationships of this integrated control landscape are then linked to the risk data universe (risk appetite, risks, controls, KRIs/KPIs/KCIs, scenarios, losses), organizational structures (business units, legal entities, etc.), business objectives (financial performance indicators, performance goals, strategic objectives, etc.), compliance mandates (areas of compliance, requirements, standards, policies, etc.), audit constructs (audit entities, findings, work papers, etc.), legal information (cases, incidents, etc.) and IT assets (assets, threats, vulnerabilities, etc.).

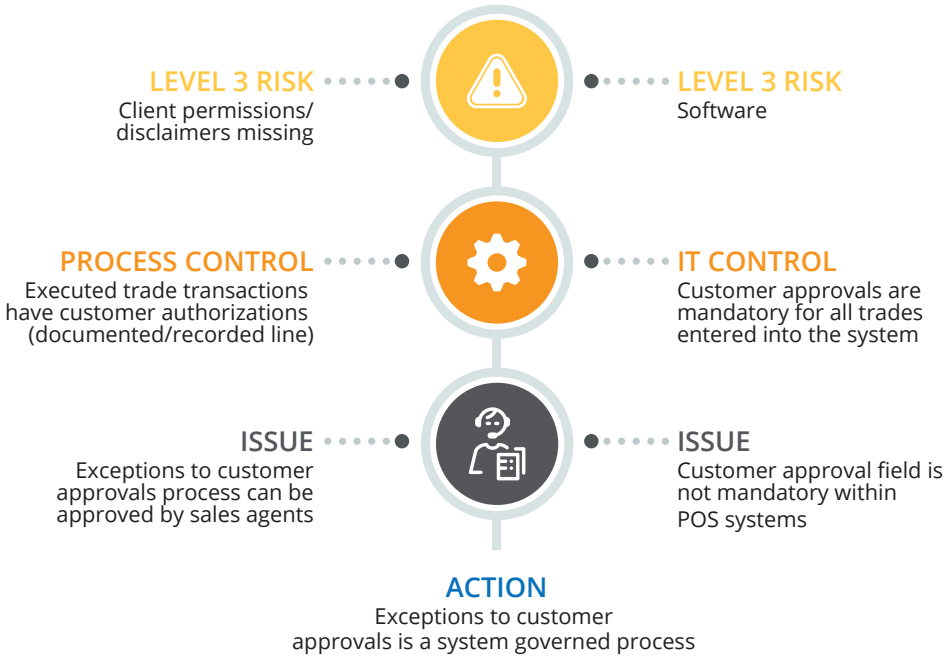
The idea is to create an integrated, federated control universe and framework which can be used by all the three lines of defense functions as a single source of truth. Each line of defense continues to independently test controls using different control testing methodologies, but within an integrated control taxonomy.

2. Maximized asset resilience though control rationalization using the multi-dimensional relationships established between the control universe and other universes, including the risk, organizational, business objective, and compliance universes. This approach allows organizations to:

• **Understand the dependency and correlation among controls and their test results**. In the following example, three different control tests generate three different issues, but all of them point to the same deficiency around the lack of integration between the SWIFT and CORE BANKING systems.



• **Rationalize issues and actions** In the following example, one action can address both the issues identified from two different control tests.



• **Rationalize controls.** Multiple controls often address the same control objective, and can therefore be rationalized.

3.3 Crowdsourcing Risk Data

The empowerment of the front line provides a framework which defines both process competencies and the technology infrastructure required to collect and disseminate risk information from and to the front line of the business. With this framework, organizations can build:

A pervasive, integrated, and intelligent issue management program design which enables the front line to manage issues and related actions -- critical parts of any integrated risk program. Issues are control deficiencies or process weaknesses that directly inform the overall risk level of the firm. The larger the control or process issues, the higher the risk level and the more the chance of a risk limit/ appetite breach.

The KNOWN UNKNOWN problem is often the lack of data which impacts organizations in the following ways:

(1) Management and boards cannot ascertain whether they have complete information when making decisions around a policy, product, or risk;

(2) Heads of business units are unable to effectively allocate resources for problem-solving because they don't have sufficient data on issues.

A pervasive, integrated, and intelligent issue management program will provide management and boards with transparency, as well as the certainty that the aggregated risk and issue data presented to them is complete, appropriately risk-rated, and has been challenged and quality assured by second- and third-line units. Heads of business units can use the issue data to allocate technology or human resources towards ensuring that the firm keeps unintended costs or damages to a minimum, and stays within their risk appetite.

As a part of the pervasive, integrated, and intelligent issue management program, there are **3 Future State Pillars** which can guide firms to success: data capture, management and tracking, and insight delivery.

Future State of Data Capture: In the future, there will be two primary sources to capture issue data:

(a) Human input: All employees will know and understand their roles and responsibilities, as well as how to execute them. They will also feel safe in doing so. Simple, jargon-free technology will be leveraged to raise issues with management. Artificial intelligence (AI) or natural language processing (NLP) will translate the unstructured text into structured data for review by management.

(b) Machine input: AI or machine learning (ML) engines will scour the internal datasets of the company—including the loss event database and control test results—looking for weaknesses or breakdowns. They will suggest themes and possible new issues arising from the data. AI will also scan external feeds, and cross-reference them with internal data for similar risks or issues. Highly visible events that damage third-party reputations will be cross-referenced to check for similar internal issues. Using this data, management can act swiftly to contain the issues before they spiral out of control. AI will also look at internal data, and identify themes—including whether or not similar types of issues have been logged independently across different departments or in the past. This data will then be flagged with management for a review.

Future State of Management and Tracking: First line of defense teams will use technology to track remediation activities, ensuring completeness and sign-off from management. Issues will be linked to the related processes, risks, or controls to enable richer analytics. The enterprise risk management (ERM) and compliance groups will validate issue data and remediation activities, and will challenge the issue rating independently. Internal and external auditors will ensure quality assurance, and will independently leverage AI in executing their responsibilities.

Future State of Insights Delivery: Data will be available in real time in both structured and natural language formats depending on the recipient. Board reporting processes in natural language will be highly automated based on the underlying linked and validated structured data. Management will attest to the board that the data is complete and driven by first line of defense perspectives. The power of AI will provide new insights, break down siloes, and remove biases where possible. Regulatory bodies will have appropriate access to the insights through various channels.

The outcomes from the three future state pillars will enable the board of directors and heads of business units to gain faster and richer insights which they can then use to manage risks more effectively, thereby avoiding certain losses, and in turn, increasing shareholder value.

For more details contact:
subharun@metricstream.com