Hype Cycle for Risk Management, 2020

Published: 9 July 2020 **ID:** G00448047

Analyst(s): Jie Zhang

In 2020, CEOs continue to rank risk management as one of their top business priorities. Security and risk management leaders must rise to the challenge by equipping senior executives and board members with the practical risk management tools and advice highlighted in this year's research.

Table of Contents

Analysis....3
- What You Need to Know....3
- The Hype Cycle....3
- The Priority Matrix....4
- Off the Hype Cycle....5
- On the Rise....6
  - FinDRA....6
  - Cybersecurity Maturity Certifications....7
  - IT Risk Appetite Statements....9
  - Digital Risk Management....10
  - Blockchain for Data Security....12
- At the Peak....13
  - Cyber-Risk Quantification....13
  - Breach and Attack Simulation....15
  - Application Security Requirements and Threat Management....17
  - Privacy Impact Assessments....19
  - Security Rating Services....20
  - Continuous Controls Monitoring....22
  - Data Classification....24
- Sliding Into the Trough....26
  - Integrated Risk Management....26

IoT Security..... 28
Data and Analytics Governance..... 30
Unified Endpoint Management..... 32
Business Process Risk Modeling..... 34
Environmental, Social & Governance..... 35
IT Vendor Risk Management..... 37
End-to-End Supply Chain Risk Management..... 39
Operational Technology Security..... 42
Climbing the Slope..... 44
Crisis/Emergency Management Solutions..... 44
Hazard/Threat Intelligence..... 46
IT Risk Management Solutions..... 48
Business Continuity Management Program Solutions..... 50
Cloud Access Security Brokers..... 52
Enterprise Legal Management..... 54
Cybersecurity Maturity Assessments..... 56
Emergency/Mass Notification Services..... 57
Ethics and Compliance Management..... 60
Entering the Plateau..... 61
Qualitative Risk Matrices..... 61
Appendixes..... 63
Hype Cycle Phases, Benefit Ratings and Maturity Levels..... 64
Gartner Recommended Reading..... 65

List of Tables

Table 1. Hype Cycle Phases..... 64
Table 2. Benefit Ratings..... 64
Table 3. Maturity Levels..... 65

List of Figures

Figure 1. Hype Cycle for Risk Management, 2020..... 4
Figure 2. Priority Matrix for Risk Management, 2020..... 5
Figure 3. Hype Cycle for Risk Management, 2019..... 63

Analysis

What You Need to Know

As the year 2020 has unfolded, the world has reacted to COVID-19 on a global scale. CEOs began to understand the impact of the unexpected set of operational challenges and further cut budgets ahead of them. An economic recession will continue to hit the majority of industry sectors and businesses in the coming year. There will be a new focus on operational risks and resilience, such as supporting a sudden growth of remote workers, responding to supply chain disruptions and optimizing budgets for already-launched digital projects. The path ahead is a tough period of restructuring and resetting business goals. One of the most important measures of the CEO's success will be how they deal with the inevitable recession. In Gartner's 2020 CEO survey, which was conducted before COVID-19, when asked directly about recession risks, half of respondents anticipated some impact, but only 9% were expecting it to be severe. (See "2020 Gartner CEO Survey: The Year of Recession.") This percentage would have been significantly higher if the survey were conducted post-COVID-19.

As a practice functioning across multiple disciplines, risk management is a major undercurrent for the CEOs' top business priorities in innovation, operational automation and new technology adoption. Risk management continues to evolve to support the speed and scale required by CEOs' digital business strategies and operational resilience. Gartner's research relies on constant scanning of the market and continuous capturing of new relevant risk management concepts and technology adoption trends.

(For more information about how peer infrastructure and operations [I&O] leaders view the technologies aligned with this Hype Cycle, see "2020-2022 Emerging Technology Roadmap for Large Enterprises.")

The Hype Cycle

The Hype Cycle for risk management describes the related concepts, methods, processes, software solutions and services that organizations can use to develop programs to withstand risk events or seek risk-related opportunities. In short, risk management programs mitigate the impact of uncertainty on business operations and outcomes. Gartner recommends an integrated risk management (IRM) strategy to align with an organization's maturity of risk management and resilience-building. This strategy should be underpinned and implemented with evolving risk assessment processes, risk owner's skills and process automation that supports digital business development at the required speed and scale (see "6 Principles for Digital Business Risk Assessment").

This Hype Cycle also demonstrates organizations' need to understand a broad scope of risk, by having a comprehensive view across business units and risk and compliance functions, as well as key business partners, suppliers and outsourced entities. At the same time, there is no silver bullet — that is, no single approach to assessing risk or managing risk that works for everyone. As a result, new technology solutions are emerging to increase the collaborative nature of risk management to support data-driven decision making, within and external to an organization. The

technologies covered in this Hype Cycle provide the risk insights that are required to create strategies to build successful digital business processes.

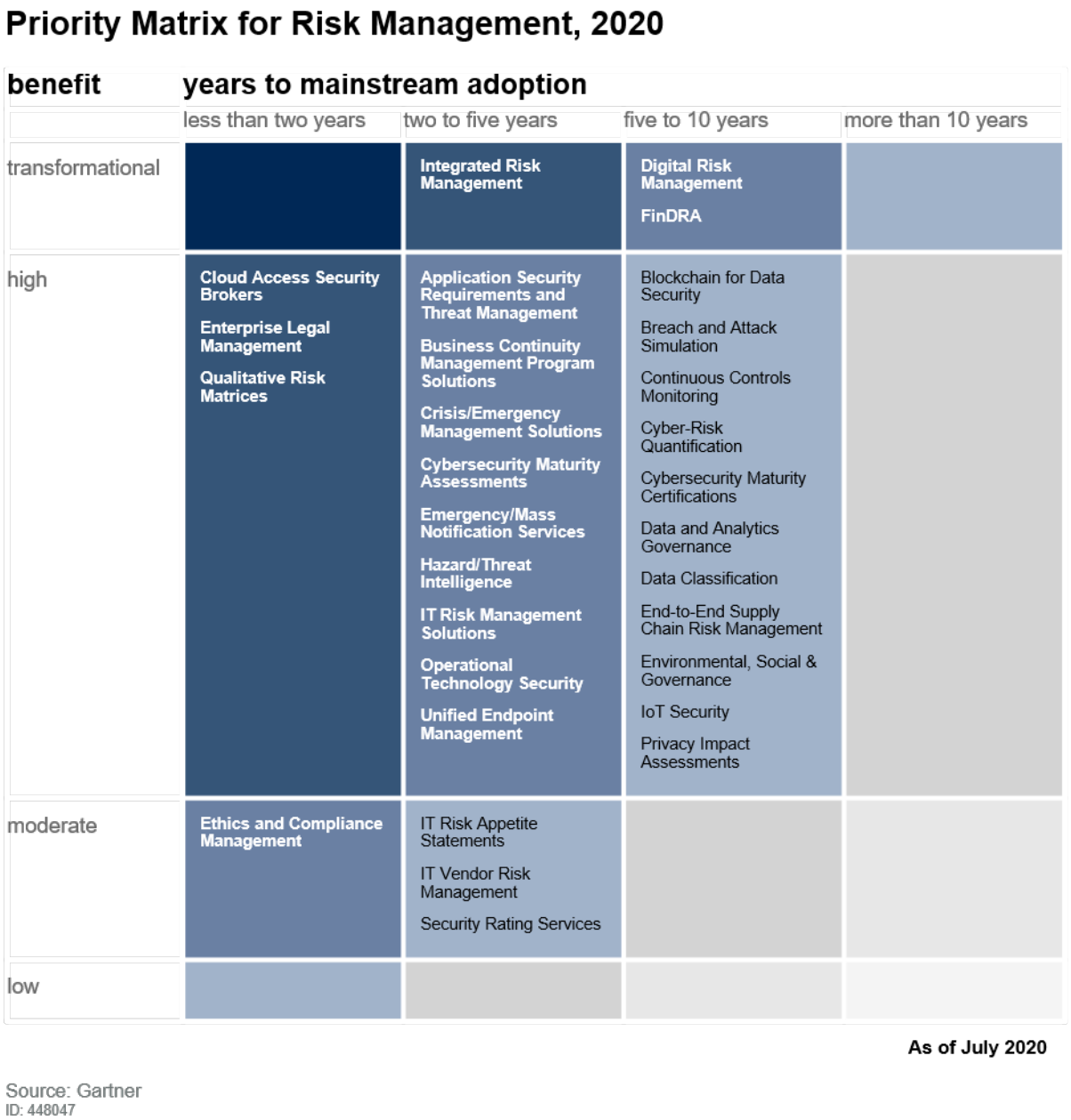
Figure 1. Hype Cycle for Risk Management, 2020

Source: Gartner
ID: 448047

The Priority Matrix

The color and position of the concepts and technologies on this Hype Cycle tell the story of an evolving and maturing set of risk-management-related concepts and technologies that are rapidly becoming enterprise best practices in their applicable areas. Concepts and technologies with transformational or high benefit, such as digital risk management (DRM), Internet of Things (IoT) security and privacy impact assessments highlight the areas that may provide innovation benefits for organizations looking to elevate risk management maturity. Other concepts and technologies, such as breach and attack simulation, continuous controls monitoring (CCM), business process risk modeling and end-to-end supply chain management offer assurances to operational resilience and compliance. Reacting to crises such as the globally scaled COVID-19, technologies such as business continuity management program (BCMP), and environmental, social and governance solutions provide unique insights into risk events that could cause significant business operation disruptions.

Figure 2. Priority Matrix for Risk Management, 2020



Source: Gartner
ID: 448047

Off the Hype Cycle

A number of innovation profiles are introduced in this iteration of the Hype Cycle. Some reflect the increased market hype, such as cyber-risk quantification and cybersecurity maturity certifications. Others fulfill requirements in a more representative overall risk management discipline and market, such as business process risk modeling, continuous controls monitoring, qualitative risk matrices, IT

risk appetite statements and IT vendor risk management. Several BCMP-related innovation profiles have been added due to their close alignment with risk management. At the same time, some former innovation profiles are no longer linked to this Hype Cycle, because they are only indirectly relevant to risk management programs.

On the Rise

FinDRA

Analysis By: Brian Lowans; Khushbu Pratap; Alan D. Duncan

Definition: Financial-based data risk assessment (FinDRA) provides a method to prioritize financial investment opportunities for data based on balancing monetization options against business risks. FinDRA uses infonomics to analyze the business risks identified through data security governance and then prioritize the financial impact of each business risk caused by security, privacy or processing incidents.

Position and Adoption Speed Justification: Every digital business project can exploit the untapped value opportunities for data. But this desire is accompanied by prolific growth of business risks that may create financial impacts. Unfortunately, business leaders continue to separate the decision processes for data investments and monetization opportunities from the associated costs or liabilities. FinDRA is an early-stage methodology that can be used jointly by business leaders, such as chief data officer (CDO), chief information security officer (CISO) and chief privacy officer (CPO). FinDRA creates a defensible strategy and budget for data security, privacy and data management.

User Advice: There is rarely, if ever, any discussion about the financial impacts that can result from investment decisions on how to use data. Therefore, the liabilities of opportunity costs, waste and risk are not assessed, resulting in overly optimistic financial forecasts. An incident such as a data breach, privacy enforcement, noncompliance or even accidental processing incidents can create financial impacts to a business in different ways that can be short-term “volatile” or longer-term “persistent” costs. Use infonomics to evaluate the tangible and intangible liabilities of managing, storing, analyzing and protecting the data. Then evaluate FinDRA as a five-step process:

- Establish the data security governance (DSG) framework to identify all essential datasets and associated business risks.
- Apply an evolving data risk assessment (DRA) to identify how inadequate data security or privacy may create business risks.
- Use infonomics to evaluate how the business risks for each dataset affect revenue or net asset value.
- Use FinDRA to prioritize business risks according to financial metrics.
- Use FinDRA to establish a defensible security budget to mitigate prioritized business risks that result from an evolving DRA.

The relative financial impacts can be represented by a financial risk prioritization that compares net "asset" value against "liability" impact. An investment decision can then be prioritized according to relative ratios of assets and liabilities, opportunity cost, return on investment (ROI), etc. This allows for a relative comparison of how business initiatives affect each dataset, and a prioritization can be created for investment or for incurring a reactive cost, for example, in terms of security or divestment. The aim of this approach is to create a relative evaluation of datasets instead of an actuarial calculation.

Business Impact: The ability to assess, prioritize and then mitigate selected business risks associated with data management and monetization projects will be significantly enhanced by FinDRA. Some vendor products are available that analyze cyber-risk quantification and only focus on the financial liabilities. Organizations have an opportunity to use FinDRA as a repeatable, consistent financial risk methodology to enable direct collaboration between CISOs and other business leaders such as the CDO. This can help create data security and data management strategies with board-level approval of defensible security budgets and investments.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Arx Nimbus; Axio; Corax; Emergynt; Guidewire; Nehemiah Security; RiskLens

Recommended Reading:

"Use Infonomics to Quantify Data Monetization Risks and Establish a Data Security Budget"

"Develop a Financial Risk Assessment for Data Using Infonomics"

"Use the Data Security Governance Framework to Balance Business Needs and Risks"

Cybersecurity Maturity Certifications

Analysis By: Claude Mandy; Sam Olyaei

Definition: Cybersecurity maturity certifications are the emerging subset of organizational security certifications that are intended to independently attest to an organization's achievement of a certain level of maturity in their cybersecurity practices and processes. These certifications combine a graduated level of security controls that build on each other with process maturity levels and are independently reviewed by accredited certification providers to provide independent verification that organizations have achieved the desired maturity level.

Position and Adoption Speed Justification: The focus on cyber-risk and the reliance on third parties and vendors for services, and solutions outside the organization's core business continues to increase. At the same time, supply chain attacks continue to grow. This has created an urgent requirement to not only understand the capabilities of third parties and vendors but enforce

minimum standards. Traditional organizational security certifications have been common in the industry for more than 15 years and continue to provide insight and independent verification into vendor cybersecurity controls and process. These certifications have typically been focused on the existence of specific controls and not the overall maturity of the cybersecurity function.

Using maturity models as the basis for organizational cybersecurity certification is recent and emerging from the increasing usage of levels and tiers in certifications. Early examples include certifications based on HITRUST CSF and the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool. Starting sometime in 2020, Cybersecurity Maturity Model Certification (CMMC) third-party assessors will start testing and certifying whether contractors to the U.S. Department of Defense can support defense contracts based on independent assessment of their maturity level. This is the start of what is expected to be a flurry of maturity certifications from various industries and profiles of business.

User Advice: The demand and need for cybersecurity maturity certifications, such as CMMC, will be driven by customer demand, business environment and regulatory enforcement. Security and risk management (SRM) leaders should consult with business leaders and other C-suite members to assess the value of such certifications in terms of long-term organizational benefits. SRM leaders can further supplement this view of value by leveraging surveys or questionnaires from their customers to gauge demand for these certifications. Similarly, engagement with sales and marketing teams can assess whether these certifications can increase the trustworthiness and relative desirability in the eyes of prospects. In areas where certifications are mandated by law/regulation, leaders should work to ensure that there is a balance between the value that this generates for the business versus the effort and resources allocated to this project.

Regardless of the demand and value for the certification itself, Gartner recommends that SRM leaders should assess the maturity of their current security posture to plan strategic improvements. SRM Leaders can leverage Gartner's IT Score for Security and Risk Management, a diagnostic tool intended to provide program-level maturity assessment. However, this is not a substitute for a certification or audit (see "IT Score for Security & Risk Management").

Business Impact: The use of cybersecurity maturity certifications may increasingly become a prerequisite to provide services or products in certain industries and sectors. By YE20, contracts with the U.S. Department of Defense may require CMMC certification that will disqualify uncertified or less mature organizations from competing. This is likely to have significant implications for all organizations involved in provided services in these sectors.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Recommended Reading:

"Top Security and Risk Management Trends"

"IT Score for Security & Risk Management"

"Security Program Management 101 — How to Select Your Security Frameworks, Controls and Processes"

IT Risk Appetite Statements

Analysis By: Jeffrey Wheatman

Definition: An IT risk appetite statement is a working document that defines the amount and type of IT or technology risk that an organization is willing to take in order to achieve its strategic objectives. The IT risk appetite statement should articulate how the organization will balance the need to protect the business from IT risk and the need to run the business.

Position and Adoption Speed Justification: In theory, an IT risk appetite statement provides the basis for consistent and defensible decision making. In practice, while most security and risk management leaders state that they want to manage against their risk appetite, when asked what their risk appetite is, they rarely have an answer that is usable. There are several reasons for this gap:

- Many organizations don't have an enterprisewide risk appetite statement to build on
- Many IT risk appetite statements are overly specific and too quantitative to be useful in practice
- The lack of a track record to measure success against the activities that support the IT risk appetite discussion leads to a perception that the work arbitrary

Gartner has seen recent improvement in engagement with business and other stakeholders which should accelerate the value and usefulness of IT risk appetite efforts.

User Advice: To improve the value of IT risk appetite efforts, Gartner recommends taking a multifaceted approach:

- Articulate and socialize the concepts of risk appetite and risk tolerance with technology and business stakeholders. This is critical for the higher level of engagement required for success.
- Leverage the risk appetite work done in other areas of the business. Many organizations have done extensive risk appetite work within the domains of enterprise risk, operational risk, legal and compliance risk, and the outcome of that work can provide a strong base for building an IT risk appetite.
- Recognize that the most effective IT risk appetite statements are qualitative in nature. They will be supported by tactical activity and quantitative measures, but the base will be "softer."
- Engage business stakeholders in workshops to discuss the current risk landscape, possible scenarios for current and future business initiatives that may lead to excessive risk and how to assess risk prioritization.
- Create simple, practical and pragmatic risk appetite statements that are linked to business goals and risk treatment plans.

- Keep in mind, IT risk appetites are often a moving target. Take a plan, build, monitor approach. Build on existing work and implement a process for continuous management and refinement.

Business Impact: Security programs built on well-considered and well-constructed risk appetite statements will provide the following benefits:

- **Optimizes business performance —** Serves as a summary of risk management policies; clarifies the risks the organization is willing to take, will helps leaders identify appropriate risk trade-offs.
- **Improves risk management processes —** Helps leaders make informed decisions about risk treatment; fosters a risk-aware culture; ensures senior leadership agrees on the organization's risk-taking posture
- **Helps achieve external stakeholder expectations —** Tool for communicating to regulators, rating agencies and shareholders about the information risks the organization is willing to undertake and enhances the corporate governance of the organization.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Recommended Reading:

"Risk Appetite Learning Tool"

"Sample Risk Appetite Statements"

"Ignition Guide to Drafting Risk Appetite Statements"

"A Decision Model to Optimize Risk, Value and Cost"

"Risk Appetite Trade-Offs (Hydro One)"

Digital Risk Management

Analysis By: John A. Wheeler

Definition: DRM is an emerging IRM use case that facilitates risk awareness, understanding and decision making associated with the convergence of the digital and physical through cloud, mobile, social, big data and IoT.

Position and Adoption Speed Justification: DRM technology addresses internal and external risk in terms of an internet-facing infrastructure and an infrastructure that is occasionally or never connected to the internet. However, it is well-connected to infrastructure elements that, in turn, are exposed to the internet. The capabilities of DRM solution providers today do not represent the full scope of organizations' DRM needs. DRM capabilities are now highly fragmented among a host of vendor solutions. No single vendor currently provides a comprehensive offering that can provide a

full view of the digital risks across social, mobile, big data, cloud, third-party technology, OT and IoT. However, key integration points with some of the IRM solution vendors include cloud security intelligence, mobile device management (MDM), social media surveillance, information governance, e-discovery and operational intelligence. Demand for DRM solutions will increase as businesses address COVID-19-related need for digital business transformation.

User Advice: Much like traditional IRM solution offerings, these new technologies will support the integration of IT risk subsystems to mitigate risk via "command and control" across the wide array of digital assets. In addition, DRM will aggregate risk profile data to enable risk-based decision making and the prioritization of risk management resources to create an agile and resilient enterprise. The hype around these DRM solutions will increase quickly as more companies adopt digital business technologies in the next few years. Users should look to augment relevant digital risk visibility and reporting needs in existing IT risk management (ITRM) capabilities of their IRM solutions. Only then should users fill the gaps with niche DRM solutions based on business needs. Therefore, users should first assess the capabilities of their current IRM solution technology vendors to meet these new demands before investing in new technology solutions. Companies that do not have an IRM solution should consider an IRM vendor's DRM vision and R&D commitments before making a purchasing decision.

Business Impact: Because digital business initiatives span the entire enterprise and cross industry lines, the business impact of DRM will be significant. The ability to gain visibility into IRM solution requirements associated with new digital business investments will prove valuable as companies enter a new world of complex digital risk. To make crucial business decisions related to the veracity of ongoing digital business, operations will generate high demand for these software solutions.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Arx Nimbus; Axio; Balbix; Digital Shadows; PwC; RiskLens; RSA; ZeroFOX

Recommended Reading:

"Market Insight: Fuel Digital Business Transformation via a Digital Risk Management Solution Stack"

"How to Get Your CEO to Embrace Digital Risk Management"

"Technology Outlook for Integrated Risk Management"

"Market Trends: GRC Era Is Over as Customers Adopt Integrated Risk Management"

"Emerging Technology Analysis: Digital Risk Management"

"Coronavirus (COVID-19) Resource Center Primer for 2020"

Blockchain for Data Security

Analysis By: David Mahdi

Definition: Blockchain-enabled data security applications leverage blockchain's decentralization capabilities to offer alternative methods to establish data protection, with minimal reliance on centralized arbiters. Blockchain-enabled data security methods can enhance use cases involving chain of custody ensuring data integrity, as well as encryption, (e.g., offering a decentralized key repository for decentralized PKI).

Position and Adoption Speed Justification: At the core of blockchain is the ability to ensure that participants with no other trust relationship have access to identical ledgers. This property provides two key data security attributes to the ledger data: integrity and availability. An additional property, confidentiality (i.e., data encryption), is typically done as an additional step to ensure data protection. Data protection methods can be completed on-chain or using integrated off-chain methods, but leverage blockchain technology to ensure all aspects of confidentiality, integrity and availability. However, there are vendors such as ALTR that provide aspects relating to integrity, availability and confidentiality by leveraging blockchain technology.

Overall, leveraging blockchain core decentralization capabilities, combined with complementary data security approaches, offers IT leaders new methods to ensure integrity, availability and, in some cases, transparency.

User Advice: To illustrate a blockchain-based approach to data security, consider ensuring data integrity for a dataset. By storing a representation of the dataset (i.e., a hash) in the blockchain, all nodes will now be aware of the status. Any attempt to change the data will require consensus among the nodes. Therefore, any data logged in the blockchain becomes a part of the immutable decentralized ledger. Common data security approaches that may benefit from a blockchain-based approach, such as PKI, key management and tokenization, can all gain resilience, reliability, transparency and trust due to blockchain's ability to decentralize these functions.

Data security leaders should familiarize themselves with blockchain through early stage research. One such approach is by following publicly known proofs of concept. In doing so, leaders can gain insight into new ideas and approaches that may be relevant. A number of new and well-established vendors are experimenting with data security applications in areas such as:

- Ensuring the integrity of data and/or devices (e.g., things in the IoT)
- Data transparency (e.g., smart contracts or land registries)
- Mitigating trust issues (e.g., distributed/decentralized authority)

Data security leaders should work with developers/architects to establish at least a high-level position on blockchain's relevance and a vision for future adoption. Blockchain-based data security initiatives differ dramatically from legacy business technology and processes. Therefore, data security leaders should take a bimodal approach and experiment with blockchain-based initiatives as Mode 2 projects.

Business Impact: Blockchain has the potential to increase resilience, reliability, transparency and trust in a variety of common data security functions that hinge on centralization such as public-key infrastructure (PKI), key management and tokenization. Blockchain applied to data security applications offers alternative methods that allow businesses to gain further trust in their data by ensuring integrity and availability. This can be enhanced further by layering in data protection techniques, such as data encryption, that could be done off-chain.

An example is in securing and sharing public records such as a land registry digital document. The traditional approach is to host the document in a central database maintained by a select number of administrators. This model potentially suffers from weaknesses with resilience and transparency. What is to stop a malicious actor from modifying the land registry? In contrast, if the document or a pointer to the document was stored in a blockchain, then availability, transparency and integrity are maintained via the distributed cryptographic nature of blockchain. Any change or attempt to change the document is evident and requires consensus among the nodes. Most important, all of these transactions are made public via the nature of blockchain.

This is in direct contrast to traditional approaches that would have the data stored in a central repository that typically doesn't require multiple parties to manipulate the data. As such, Gartner has witnessed increased client interest in leveraging blockchain to establish integrity and overall trust in data.

Finally, due to the absence of meaningful regulation or standards, governance must be exercised to limit risk within organizational tolerance and also must ensure that enterprise risk appetite will allow for experimentation and eventual adoption of the new technology.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: ALTR; Guardtime; IBM; Remme

Recommended Reading:

"Innovation Insight for Blockchain-Enabled Data Security Applications"

"Innovation Insight for Blockchain Security"

"Evaluating the Security Risks to Blockchain Ecosystems"

At the Peak

Cyber-Risk Quantification

Analysis By: Khushbu Pratap; Sam Olyaei; Jeffrey Wheatman

Definition: Cyber-risk quantification is a method for expressing risk exposure from interconnected digital environments to the organization in business terms. Such exposure can be expressed in currency, market share, customer/beneficiary engagement and disruption in products/services over a chosen period. Defensible exposure value ranges are determined using a combination of business logic, mathematical model(s), loss event history and current risk assessment.

Position and Adoption Speed Justification: Defensible and scalable cyber-risk quantification is an emerging initiative. Quantification approaches are in their infancy in terms of suitability to apply at scale, and fit into use cases for utilities, government, retail, technology, telecom, manufacturing, healthcare and higher education. There is mixed feedback from a variety of organizations that have invested in cyber-risk quantification services and solutions regarding usefulness of results in business decision making beyond periodic board reporting. A variety of approaches exists, but none is proven defensible and scalable yet. There are publicly available assessment approaches such as FAIR and OCTAVE, and proprietary models combine principles from FAIR, OCTAVE, operational risk management models in insurance and financial services and weather-forecasting models.

Fit-to-purpose solutions and higher adoption should be achievable within five years by focusing on data quality (relevant updated internal and external loss event history), automated input from financial systems and business applications, and setting up capabilities for continuous risk assessment. Increased defensibility should be achievable by:

- Decreasing reliance on variable subjective inputs and irrelevant loss events from incident databases
- Creating strong linkages between risk scenarios and business outcomes

User Advice: CISOs, digital risk leaders, CIOs, or executive management accountable for technology, resilience, and information risk management considering use of cyber-risk quantification offerings should:

- Identify the best-value use case for applying cyber-risk quantification — the most common use cases with positive feedback are procuring or renewing cyber insurance and assisting in ROI calculation of security investments as a result of digital initiatives.
- Articulate the assumptions of the chosen model and approach to account for different contexts, such as acquisition/merger/divestiture, posture assessment, justification for business strategy, or simply risk treatment.
- Invest in cyber-risk quantification only if it justifies the cost of trainings, workshops, subscription and full-time equivalents (FTEs) combined, to offer significantly more confidence in business decision making or specific risk treatment as against qualitative judgment.
- Not confuse cyber-risk quantification with use of security rating services or risk quantification solutions that offer a single score or index. Solutions that distill cyber-risk exposure down to a score are ancillary data points in risk decision making, not primary defensible inputs.
- Link cyber-risk scenarios to business outcomes and verify the linkages with senior management and subject matter experts before making investments in capabilities, services and tooling.

- Account for model risk and assumptions made regarding data inputs; solutions in the current market are still evolving.

Business Impact: Cyber-risk quantification can be applied to address challenges of

- Risk prioritization
- Communicating confidence levels in cyber-risk decision making to executive management and board members

Specifically leveraging cyber-risk quantification before mergers, acquisitions and divestitures can offer a higher level of assurance to due diligence activities along with a technical security risk assessment. Cyber-risk quantification is also being applied to justify spend on modernization of infrastructure and legacy applications. Risk quantification outcomes can be used in tactical decisions related to potential ransomware payment, insurance premiums and coverage, and high-level response planning to business disruption. As risk quantification approaches evolve and buyers fully recognize that cyber risk is part of operational risk, defensible quantification results will result in risk-informed decision making.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Acuity Risk Management; Arx Nimbus; Axio; Cyber Innovative Technologies; Emergynt; Nehemiah Security; RiskLens

Recommended Reading:

“The Urgency to Treat Cybersecurity as a Business Decision”

“Lessons From the Virtual Workshop on Risk Quantification”

“Cyber Judgment: Navigating the Era of Distributed Risk Decision Making”

“Cyber Judgment Benchmarking Report”

Breach and Attack Simulation

Analysis By: Jeremy D’Hoinne

Definition: Breach and attack simulation (BAS) technologies allow enterprises to continually and consistently simulate multiple attack vectors against enterprise infrastructure. BAS includes external and insider threats, lateral movement and data exfiltration, and its deployment uses software agents, virtual machines and other means. Using BAS removes the risks to production environments inherent with other testing approaches. It overlaps with, but cannot fully replace, red teaming or penetration testing.

Position and Adoption Speed Justification: The breach and attack simulation market is growing, with leading vendors expanding their customer base by more carefully targeting the security control assessment use cases. The ability to provide continuous and consistent testing with limited risk is the key advantage of BAS technologies. Weekly, and sometimes daily, tests are used to alert IT and business stakeholders about existing gaps in the security posture or validate that security infrastructure, configuration settings and detection/prevention technologies are operating as intended. BAS can also be used to validate if security operations and security operations center (SOC) staff can detect specific attacks when used as a complement to red team or penetration-testing exercises.

The most successful use case for attack simulation tools is the automated testing and assessment of existing security controls as well as the appropriate configuration settings for email and web security gateways, firewalls and web application firewalls (WAFs), and ACLs. To expand beyond a niche market, BAS vendors will need to prove the value and accuracy of the security assessment resulting from simulated attacks. BAS vendors must overcome deployment and maintenance challenges, and beat competition from adjacent markets with overlapping objectives, features or functionality, such as penetration testing, application security testing (AST), vulnerability management or SOC training tools. BAS can positively contribute to risk assessment and help prioritize remediation. However, BAS also needs to evolve, notably its reporting, to be more relevant for the nontechnical stakeholders.

User Advice: Because breach and attack simulation relies on simulated attacks, the first thing to evaluate is the capability of a BAS technology to accurately and safely emulate attacks to mimic the risks faced by the organization. BAS deployment options influence what can or cannot be emulated. The size and frequency of updates for the portfolio of simulated attacks determine the value of repeating the security assessment using BAS versus a point-in-time approach such as a penetration test.

Once validated, risk management professionals must evaluate the ability of the tool to derive meaningful results beyond the technical metrics. BAS tools should go beyond diagnostic and be prescriptive in a way that helps prioritizing remediation and adapting to the evolution of a previously assessed risk.

BAS vendors are addressing a variety of use cases in their solutions, including attack path modeling, security control testing and efficacy, and automated penetration testing. Prospective buyers should prioritize their use cases, and then assess the BAS vendors' capabilities against them to determine which BAS would improve their existing security risk assessment, threat monitoring and vulnerability management practices. Organizations should also evaluate the number of attack scenarios the provider can provide and the frequency at which these simulations are updated to reflect real-world attacks. Organizations in regulated environments should discuss with their auditors to determine whether BAS technology can be used as a means to validate the efficacy of existing security controls.

Mostly automated penetration testing tools overlap with BAS when it comes to assessing the attack surface for a category of assets. In some situations, automated penetration tests might be the second step following an initial assessment through simulated attacks. However, being the precursor to a penetration-testing engagement is not the most frequent use case for attack

simulation tools, which shine more when performing regular tests and highlighting new threats going through existing defense layers or security configuration issues.

Business Impact: SRM leaders looking to build a proactive and safer risk assessment program can use BAS tools to test the efficacy and configuration of their existing security controls. BAS allows organizations to automate a security evaluation process that otherwise would have had less frequent and more point-in-time cadence associated with other security assessment approaches such as penetration testing. The ability to evaluate and assess a larger percentage of an organization's assets on a more frequent basis is a strength of BAS platforms.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: AttackIQ; Cymulate; FireEye; Picus Security; SafeBreach; Spirent; XM Cyber

Recommended Reading:

"Cool Vendors in Monitoring and Management of Threats to Applications and Data, 2017"

"Cool Vendors in Application and Data Security"

"Cool Vendors in Security Operations and Threat Intelligence"

Application Security Requirements and Threat Management

Analysis By: Dale Gardner; Frank Catucci

Definition: Application security requirements and threat management (ASRTM) helps automate generating security requirements, risk assessments and threat models. Output of ASRTM can integrate with SDLC tools to manage tasks, workflow and validation. Vendors update security requirements and threat models by tracking changes to regulations, platforms, frameworks, and evolving threats. ASRTM dynamically highlights potential security ramifications of requirements and recommends appropriate secure coding practices or architectural counter measures.

Position and Adoption Speed Justification: Threat modeling and security requirements gathering are advocated as secure design practices which help application teams anticipate — and eliminate — potential threats and design flaws before code is written. Despite this, the time required to carry out these activities as manual tasks makes them a poor fit for agile and DevOps practices. This, coupled with a general lack of application security skills and expertise, has resulted in few organizations routinely including formal (versus ad hoc) threat modeling in application development projects. Security requirements are often broadly set across all projects instead of adapted to the specifics of each application technology stack, overburdening low-risk projects and not properly securing high-risk ones. These requirements are often not updated to reflect new technologies or are not detailed enough to cover technology specific implementation details and secure coding

practices. Automation addresses time constraints by dramatically reducing the time and security knowledge needed for up-to-date threat-modeling and security-requirements-gathering tasks, and helps minimize human error. ASRTM can be integrated into a wide variety of software development life cycle (SDLC) tooling, as well as with governance, risk and compliance (GRC) tools, helping to bridge the gap with GRC teams. Subsequent nonfunctional security and vulnerability testing such as AST and VA can help validate that security requirements have been properly implemented.

The main challenge these tools face today continues to be their visibility with clients, resulting in only a modest uptick in adoption. However, tools continue to increase in maturity, such as increased support for validation that requirements have actually been incorporated in written code. And the movement toward agile and DevOps methodologies will help highlight the value in automating security requirements and threat modeling generation tasks and accelerate adoption over the next five years. Alternatively, AST vendors, particularly those offering a suite of tools, have aggressively targeted the "push security left" mantra and could start offering similar integrated capabilities in their solutions.

User Advice: SRM leaders should leverage ASRTM tools to automate what are otherwise manual or overlooked efforts, in order to bake threat modeling and security requirements generation activities into their SDLC process and development workflow. Threat modeling, security requirements generation and enforcement are best practices within a secure SDLC model. These tools can be leveraged to automate these tasks — even incrementally as applications are updated — while incorporating content knowledge from the tool vendors on emerging threats and security requirements. The capability of these tools to automate the process can greatly reduce the time needed to devote to these tasks. Results can be integrated into application life cycle management, as well as GRC tools with the output tracked and validated throughout the development project.

Business Impact: An important benefit of ASRTM is the reduction of security risk through the automation of important secure design activities that are often skipped due to time and resource constraints. These solutions empower development teams to better anticipate, and code or architect around, potential vulnerabilities, which would otherwise be identified through testing and require remediation later in the cycle or would be missed entirely. These tools are also useful in early identification of design flaws. Enabling development teams to proactively model threats and generate subsequent security requirements early in the development process, while shortening the time required to execute these tasks, will yield reduced risk and enhanced security assurance for application development projects. The positive effects these tools can have on the implementation of a secure SDLC by automating otherwise manual tasks result in a moderate benefit rating.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: foreseeti; IriusRisk; Microsoft; OWASP Foundation; Security Compass; ThreatModeler; we45

Recommended Reading:

“A Guidance Framework for Establishing and Maturing an Application Security Program”

“12 Things to Get Right for Successful DevSecOps”

“How to Deploy and Perform Application Security Testing”

“Integrating Security Into the DevSecOps Toolchain”

Privacy Impact Assessments

Analysis By: Bart Willemsen

Definition: Privacy impact assessments (PIAs) enable organizations to identify and treat privacy risk. Typically conducted before implementing new processing activities and/or major changes, the assessment starts with a quick scan (containing process owner and description, types of data processed for specific purposes, and retention periods per purpose). A full PIA adds envisaged risks to and impacts on data subjects, combined with mitigating measures to ensure a controlled personal data processing environment.

Position and Adoption Speed Justification: Made mandatory via enhanced privacy laws, such as General Data Protection Regulation (GDPR) and the Lei Geral de Proteção de Dados (LGPD), PIAs are a best practice for deliberate, secure and purposeful use of personal data. PIAs are slowly transitioning to the mainstream. Often required reactively (for example, as prerequisite to the introduction of new technology), it is best practice to also proactively revisit previous PIAs periodically (at least every year and more frequent with high-risk processing activities). PIAs enable a responsible operation, substantially reducing privacy risk. Additionally, they deliver insight into authorization and access management, purposeful processing, data minimization options, and data life cycle control requirements. With an increasing need for PIAs, there is proportional demand for automation rather than a manual approach, as they vary in length and complexity. Automated processes and tools — though different in scope and function — are evolving and increasingly available.

Although freemium models have emerged, the administrative burden and (misperceived) operational lack of value has slowed down widespread adoption of structurally implemented PIAs, leaving it only a little post-peak right now.

User Advice: PIAs require the participation of multiple stakeholders, including legal counsel, the privacy officer and the decision-making business (process) owner. Sometimes considered a tedious process, the PIA enables organizations to safeguard individual privacy and in the process avoid reputational damage, and costly, embarrassing or damaging incidents; reduce liability; and enhance informed decision making. It provides insight into the deliberate, purposeful use of personal data and allows organizations to prevent (internal) abuse of such data. Where personal data is used for purposes that are incompatible with the original processing purpose for which the data was obtained, negative and privacy-invasive effects can be expected.

PIA models and templates, such as those provided by various data protection authorities, continue to vary in scope and granularity. However, automated processes and tools are emerging. Using

these tools, organizations create their own internal workflow process to conduct PIAs. Precedent-shaping impactful incidents and (regulatory) rulings will influence adoption of the PIA process internationally, but these take time to have an effect on both market demand and availability.

Recommendations:

- Appoint and mandate business process owners with responsibility over their respective personal data processing activities.
- Require PIAs to be conducted as a mandatory, frequently reiterated activity.
- Include PIA's results — especially from large projects — in the corporate risk register for monitoring and follow up.
- Demand service providers to conduct DPIAs as part of your ongoing engagement.
- Provide for a PIA model centrally (for example, as an internal automated workflow process) or require it to be conducted as a manual exercise when a less mature procedure suffices.

Business Impact: Conducting PIAs frequently, such as at the onset of every personal data processing activity implementation and at major changes, or at least annually, maintains control over an organization's personal data management. By implementing the results in the operational environment, organizations may find that they can reduce risk and liability by purging excess data.

The result of a PIA enables regulatory compliance, improves control over personal data throughout the data life cycle, and determines authorization and access management. It collaterally assists in the prevention of (internal) data breaches and personal data misuse or abuse. Importantly, it helps SRM leaders to quantify risk to the individual and timely apply suitable mitigating controls. Conducting PIAs frequently and consistently provides the basis of responsible and transparent personal data management.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: AuraPortal; OneTrust; Privaon; SoftLab; SureCloud; TrustArc

Recommended Reading:

"Privacy as a Partner: Building Citizen Trust in Public-Private Partnerships"

"Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria"

"Toolkit: Assess Your Personal Data Processing Activities"

Security Rating Services

Analysis By: Christopher Ambrose; Sam Olyaei

Definition: Security rating services (SRS) for cybersecurity provide continuous, independent, cybersecurity scoring and rating for enterprises with a visible presence on the internet. The services gather data from public and private sources via nonintrusive means, analyze the data and rate entity security posture using their own scoring methodologies. These tools are used for internal security, cyberinsurance underwriting, due diligence in mergers and acquisitions, and third-party/vendor cybersecurity risk assessments and monitoring.

Position and Adoption Speed Justification: There is an increased focus on cybersecurity threats and data privacy regulations, and reliance on third parties and vendors for services and solutions. This is true especially (but not exclusively) for cloud service providers, which are creating a growing need to understand internal and external threats and security postures. Traditional approaches for assessing third-party security controls have limitations, especially when hundreds or even thousands of external parties are involved. Third-party security assessments or certifications provide point-in-time snapshots, but are not always available or shared by third parties. The other common alternative, using questionnaires based on common standards or frameworks, is also point-in-time, and is highly subjective, labor-intensive, and inefficient for infosec departments and the vendors asked to complete the assessments.

Gartner also hears from clients that they are being asked to provide measures to senior management and to their customers indicating how secure their own organization is, ideally in comparison with peers and competitors. SRS represents an independent source of data to support these increasingly important use cases. However, these services don't provide a complete assessment of security controls, as their information is primarily publicly sourced (from accessing internet IP addresses, for example). Some SRS attempt to supplement their "outside-in" passive internet scanning models with assessment data that they or their customers collect.

User Advice: Enterprises can use SRS to:

- Evaluate the security posture of a cloud service, or other organization, when considering a new or more intimate relationship
- Do a better job managing third-party security risks, including continuous monitoring and alerting on the security status of key business partners and service providers
- Provide business leadership with an independent assessment of their own security posture, and compare their posture with that of their peers or competitors
- Demonstrate your relative security posture to prospective customers — you can share your score, but licensing restrictions probably restrict sharing the scores of your competitors
- Evaluate — initially and continuously — the security posture of organizations in support of the cyber insurance underwriting process
- Inform merger and acquisition (M&A) decisions

SRS products are relatively easy to use. Purpose-built services are subscription-based, and most operate by assessing from the "outside-in," without the need to deploy equipment on-site or configuring devices. Prospective customers should take the time to understand both the capabilities

and limitations of these services. No single service or solution has yet matured to provide ratings that have been consistently time-tested, and some may not have full visibility in cloud environments, especially SaaS. Although we see these services as important innovations in improving an enterprise's ability to assess and monitor the potential for cybersecurity vulnerabilities, they are not a replacement for good due diligence and assessment of internal or third-party controls. Prospective buyers should evaluate multiple vendors to see how well their offerings, scoring models and licensing fit their requirements.

Business Impact: Security and risk management leaders under pressure to demonstrate the status of their program to senior leadership can obtain an objective evaluation of a company's cybersecurity posture for a relatively low cost. Gartner clients report that use of SRS improves the senior leadership confidence in the security program, and facilitates ongoing program investment.

Organizations with many partners or heavily dependent on third parties for critical business services can leverage SRS, saving money earmarked for more expensive, third-party risk management efforts and improving the ability to manage third-party risks in near real time. Service providers can use SRS to support their sales and business development efforts by demonstrating that they are practicing good security, while helping their customers more efficiently and effectively manage their own third-party risks. While the use cases for these solutions are documented here, Gartner expects that additional use cases will emerge to address the growing demands for measuring and monitoring cybersecurity controls. Additionally, Gartner expects to see more M&As in this market, which continues to expand with limited differentiation among new entrants.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: BitSight; CipherCloud; FICO; McAfee; Netskope; NormShield; Panorays; RiskRecon; SecurityScorecard; UpGuard

Recommended Reading:

"Innovation Insight for Security Rating Services"

"How to Evaluate Cloud Service Provider Security"

Continuous Controls Monitoring

Analysis By: Jie Zhang; Elizabeth Kim

Definition: CCM is a set of technologies that automates the assessment of operational controls' effectiveness and the identification of exceptions.

Position and Adoption Speed Justification: Part of the operational assurance function is to ensure appropriate controls are in place and to assess control effectiveness. CCM technology automates and facilitates this effort by analyzing data from key business operation technologies such as ERP,

financial, infrastructure, systems and other applications to identify exceptions to policies, business rules and built-in application controls. CCM is runtime and transaction-level monitoring and is most useful for operational controls. It differs from control testing and reporting capabilities embedded in GRC or audit software. The latter is typically used through post-transaction and manually scheduled effort. CCM technology has several functions, including controls monitoring, exception and remediation management, reporting and analytics, and workflow:

- Controls monitoring functions automatically and periodically import data from ERP, financial, infrastructure, systems and other applications, and apply a set of predefined audit analytics to identify control exceptions.
- Exception and remediation management supports tracking the response to identified control failures and other deficiencies, along with the process of addressing exceptions.
- Reporting and analytics support trending and audit analysis, audit trails, dashboards and the generation of reports.
- Workflow supports notifications, alerts, reviews, approvals and other process automation needs.

The concept and the technology supporting CCM is relatively mature, but the end-user adoption of CCM is not yet pervasive. This is partially due to lower maturity of operational-level, continuous control assessment. Furthermore, from the competitive landscape, CCM capabilities are typically embedded within a broad solution, such as a GRC/IRM offering, but only a few vendors offer CCM as part of their broader GRC/IRM solution suite. Hence, CCM is just entering the Trough of Disillusionment.

User Advice: Assurance functions responsible for testing controls or gathering relevant assessment data from operational teams to support compliance, cost optimization related to COVID-19, audit and risk management activities:

- Use industry frameworks or standards, such as NIST CSF, ISO 27001, COSO, COBIT and PCI, as the foundations of controls, if you don't want to start from scratch. Adopt only what is needed for your operations.
- Identify processes that are repeatable, consistent and predictable to determine where CCM technologies can be applied.
- Evaluate CCM software vendors based on their scope and use case.

Business Impact: The challenge of operational teams being pulled into control testing and audits is common across industry sectors and organization sizes, which makes the business impact widespread. Regular testing and auditing of controls often derived from frameworks or regulatory obligations such as NIST CSF, ISO 27001 and PCI are useful to ensure satisfactory compliance outcomes. However, this effort is usually burdensome to operational teams because there is a high level of manual interaction to transform data on the effectiveness of the controls from the source to the risk and compliance management tools. CCM aims to automate the manual processes involved in data collection and identification of control exceptions and control failures. In turn, the application

of CCM will help the organization save time and cost of assurance. The benefit also includes improved overall risk management through a more continuous visibility of the organization's control effectiveness and compliance status.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: BAP; Deloitte; Panaseer; Resolver; SAP; ServiceNow

Data Classification

Analysis By: Alan Dayley; Bernard Woo; Bart Willemsen

Definition: Data classification is the process of organizing information assets using an agreed-upon categorization, taxonomy or ontology. It enables effective and efficient prioritization for data and analytics governance policies that spans value, security, access, usage, privacy, storage, ethics, quality and retention. Data classification typically results either in the development of a large repository of metadata useful for making further decisions, or applying a "tag" to a data object to facilitate use and governance of data during its life cycle.

Position and Adoption Speed Justification: There are many reasons to classify data, and the decisions about who or what system establishes and enforces classification differ accordingly. Approaches include categorization by data type, owner, regulation or classification by data sensitivity or retention requirements. Data classification momentum continues for digital business transformation, artificial intelligence/machine learning (AI/ML), security concerns and increased regulations and concerns for privacy. Data protection regulations have added needs to classify data around individuals and entities, with privacy-centric classification efforts, and as a foundation for data life cycle management. Datasets residing and migrating across on-premises and multicloud has thrust data classification into the forefront for both organizations and cloud providers.

Data risk and value assessments rely heavily on data classification. For example, security teams use classification technology to assign risk profiles to data. Likewise, the emerging field of infonomics requires classification capabilities to assign value and liability to varying datasets.

Data classification has been around for some time, just not widely adopted. The position in the Hype Cycle reflects a majority of partial or siloed adoption, and still developing capabilities.

User Advice: Data classification attempts can be difficult at best: to identify, tag and store all of an organization's data, without first taking into account the utility, value and risk of that data. To start, organizations should assess information assets for value and risk — for example, using infonomics measures. The purpose is to isolate the data that has minimal or no value to the organization, optimize data management costs and address any archival, retirement, destruction, risk and security requirements. Use an ongoing, adaptive and iterative approach instead of one-off or intermittent audits, continued discovery of data assets helps to perpetuate the process and help

with cross-organizational engagement. The key is to start somewhere that will have a business impact and build out the data catalog over time.

Data classification must also be an ongoing aspect of changing organizational behavior within the data-driven culture, and be supported by data governance and metadata management. SRM leaders and CDOs should collaboratively architect and use classification capabilities.

Data classification recommendations include:

- Implement data classification as part of a funded data and analytics governance program.
- Determine organizationwide classification use cases and efforts, and, at a minimum, keep all stakeholders informed.
- Combine privacy regulation adherence efforts with the security classification initiatives overseen by the chief information security officer (CISO). As such, information can be categorized by nature (e.g., what is PII, PHI or PCI), or by type (e.g., contract, health record, invoice). Regardless, records should also be classified by risk categories to indicate the need for confidentiality, integrity and availability. Finally, records can be indicated to serve specific purposes. Both CIA and purpose classifiers may change during the record life cycle.

Business Impact: Targeted classification, combined with the capabilities of various data management tools, will enable organizations to produce faster, more reliable and efficient data use for discovery, risk reduction, value assessment and analytics. This enables organizations to focus security and analytics efforts primarily on their important datasets. Identity-centric classification efforts can assist when managing concerns for the European GDPR, the California Consumer Privacy Act (CCPA) and other privacy regulations.

Classification enables CDOs to drive information asset management as a value-adding opportunity to support better business outcomes, rather than being an approach driven by compliance and records-keeping requirements. In addition, CDOs, CISOs, compliance and other involved functions should work with each other and other pertinent functions to ensure mutual awareness of classification activities.

Data classification can be used to support a wide range of use cases:

- Privacy compliance
- Risk mitigation
- Master data and application data management
- Data stewardship
- Content and records management
- Data catalogs for operations and analytics
- Data discovery for analytics and application integration

- Efficiency and optimization of systems, including tools for individual DataOps

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Boldon James; Collibra; Dathena; IBM; Informatica; Microsoft; Netwrix; OpenText; Titus; Varonis

Recommended Reading:

"How to Overcome Pitfalls in Data Classification Initiatives"

"Ignition Guide to Data Classification"

"Building Effective Control Documents for Sensitive Data Classification and Handling"

"Market Guide for Enterprise Data Loss Prevention"

"How to Successfully Design and Implement a Data-Centric Security Architecture"

Sliding Into the Trough

Integrated Risk Management

Analysis By: John A. Wheeler; Elizabeth Kim

Definition: Gartner defines IRM as practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks. A key distinction in Gartner's definition of IRM is the integration with enterprise risk management (ERM) relating to strategic risks impacting operational and technology risk management objectives.

Position and Adoption Speed Justification: IRM solutions deliver the combined technology, processes and data that fulfill the objectives of enabling the simplification, automation and integration of strategic, operational and technology risk management across an organization. This includes using consulting service providers to deliver IRM services and content to clients. The IRM solution market was formerly known as GRC. It has evolved to encompass risk and compliance management across a spectrum of risk domains, including technology risk and security services, hence, the name change. This offering is now falling into the Trough of Disillusionment.

Adoption, which includes both risk and security analysis and insight, is still growing, as end users look for opportunities to streamline and simplify their risk management and compliance-related activities. Many organizations are interested in reducing their overall spending by replacing multiple risk management solutions with a single, integrated solution, especially in the COVID-19 economic downturn. Other organizations are looking to improve their understanding of risks through system

integration with operational-level data sources, supported by consulting engagements, as well as augmentation of risk expertise and content through managed services.

User Advice: Organizations' adoption and understanding of strategic-level risk management specifically related to operational and technology risks are being motivated by executives and boards of directors. Building on the integration of monitored security data at the execution layer, IRM provides a much-needed management layer of integrated data to support decision making. Gartner's coverage of IRM solutions includes a focus on the core strategic, operational and technology core solution components supported by four IRM business case objectives across eight risk management use case domains (see "Technology Outlook for Integrated Risk Management").

The IRM business case objectives include performance, assurance, resilience and compliance (PRAC). The use case domains are digital risk, vendor/third-party risk, quality risk, business continuity, internal audit, environment, health and safety, ethics and compliance, and legal risk. Integration of data and processes across these eight use case domains can prove to be highly valuable in proactively managing risk, as well as generating cost savings by eliminating spend-redundant processes and technology.

Buyers and influencers include chief risk officers, chief information security officers, chief compliance officers, chief legal officers, chief information officers, chief procurement officers, chief financial officers and chief operating officers. Large enterprise buyers are currently focused on replacing, upgrading and connecting a broad array of legacy IRM tools and/or services. Midsize enterprises are looking to buy single-vendor IRM solutions to simplify and automate their risk management processes.

Business Impact: Complexities in risk management, such as regulatory compliance, digital business transformation, speed of organizations being hacked, and magnitude of information derived from monitored risk and security activities are driving skills-starved organizations to benefit from this solution set. Once the relevant data has been integrated and analyzed, IRM solutions will give clients a deeper understanding of their risk environment.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Deloitte; EY; Galvanize; LogicManager; NAVEX Global; PwC; Riskonnect; RSA; SAI Global; ServiceNow

Recommended Reading:

"Technology Outlook for Integrated Risk Management"

"Emerging Technology Analysis: Digital Risk Management"

"Competitive Landscape: Integrated Risk Management"

“Magic Quadrant for Integrated Risk Management Solutions”

“Critical Capabilities for Integrated Risk Management Solutions”

“Coronavirus (COVID-19) Resource Center Primer for 2020”

IoT Security

Analysis By: Barika Pace

Definition: IoT security works addresses software, hardware, network and data protection for digital initiatives involving IoT. The term is most often used in the context of business or marketing efforts, as opposed to cyber-physical systems security, which is a more descriptive and pragmatic term for security and risk practitioners. IoT security shares many of the same technologies and processes as IT, operational technology (OT) and physical security. IoT security provides safety, privacy and resilient for digital systems.

Position and Adoption Speed Justification: IoT security technologies and services are progressing, but through the lens of a converging security ecosystem with end users and vendors seeking higher levels of integration with IT, OT and CPS solutions. IoT security continues to move at a modest pace. Areas such as digital trust, tamper-resistant device hardening techniques in hardware and firmware, secure cloud integration, remote access, device discovery, event detection and response systems, and improved consulting and system integration are contributing to the progress. Larger security providers continue to enter the market space and offer slightly higher levels of security product integration with IoT solutions.

New IoT security technologies continue to emerge primarily as part of existing IT, OT and physical security technology refreshes. Increasing regulations (for example, GDPR and California’s new SB-327 cybersecurity law) will continue to spur demand for IoT security products and services over the years to come. Over the past year these regulations and compliance requirements have fueled adoption. While merges and acquisitions this past year left some end users slower to adopt, the past is expected to remain on track through this current period. Furthermore, as the threat landscape continues to evolve, IoT security is maturing rapidly to address and adapt to the new threats, thus leading it into the adolescent phase, as demonstrated by increasing maturity in areas of safety and reliability.

User Advice: Security and risk management leaders, including business executives, chief digital officers, chief risk officers, chief information security officers (CISOs) and CIOs, should:

- Establish proofs of concept to discover, classify and manage all connected devices to ascertain risk landscape, raise organizational awareness and create business value by onboarding visibility tools that can have dual purpose for operational team
- Determine design gaps in capability, skills and infrastructure
- Elevate IOT security requirements into their enterprise risk management efforts by adopting an integrated security strategy across IT, IOT and CPS.

- Account for data privacy concerns brought about by the increasing regulations for IoT devices that process personal data
- Record all IoT assets, from sensors to large industrial equipment, and create visibility into their IoT networks and topologies
- Include IoT security into the expanding scope of responsibility now and into the future
- Prepare for increasing regulations by focusing on safety and privacy in IoT designs that safeguard data, people and the environment
- Analyze regulatory exposure to IoT security requirements
- Work on developing in-house IoT security expertise, including coordination with environmental, health and safety subject matter experts
- Invest in DRM to properly plan for IoT security in digital transformation projects
- Change governance and oversight of IT and OT projects to accommodate specific digital risk concerns that lead to IoT security decisions
- Restructure skill sets and support resources (that is, organizational accountability and responsibility) to accommodate differences in deployment and operation of digital initiatives requiring secure IoT systems
- Incorporate regulatory compliance requirements for IoT technologies within existing IT, OT, CPS and physical security regulation tracking and management

Business Impact: High-profile cyberattacks can create compromises in verticals such as telecommunications, government, transportation, energy and utilities, and healthcare. Initiatives such as connected homes, smart cities, connected automobiles and medical devices are vulnerable as well. Cyberattacks have driven early IoT security spend in these verticals and initiatives. Growing attention and pressure from different layers of government may lead to potential regulations. The effects of cyberattacks also highlight the overlapping safety regulation and general safety management impacts of IoT security. In the short term, IoT security will continue to be the No. 1 barrier to entry to the IoT. In the longer term, these emerging security technologies will enable the IoT.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Sample Vendors: 802 Secure; Armis; Darktrace; Forescout Technologies; Infineon Technologies; IOActive; Microsoft Azure; Prove & Run

Recommended Reading:

"How to Secure the Enterprise Against the Internet of Things Onslaught"

“IoT Solutions Can’t Be Trusted and Must Be Separated From the Enterprise Network to Reduce Risk”

“Market Trends: IoT Edge Device Security, 2020”

“Market Insight: Tech CEOs Must Act Before Convergence Kills Your Stand-Alone OT/IoT Product Solution”

“Focus More on the Realities of Cyber-Physical Systems Security Than on the Concepts of IoT”

Data and Analytics Governance

Analysis By: Saul Judah; Andrew White; Debra Logan

Definition: Gartner defines data and analytics governance as the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, access, analysis, consumption, retention and disposition of all information assets. Data and analytics governance includes the principles, guidelines, standards, policies, procedures and links to outcomes and metrics that ensure the effective and appropriate use of data and analytics in enabling an organization to achieve its goals.

Position and Adoption Speed Justification: The outbreak of COVID-19 has led data and analytics leaders to focus their attention and effort on data and analytics for mission-critical operations. Therefore, the extent to which data and analytics have invested in improving their governance practices and expanding its scope within their enterprise has been very limited. Though there is much hype in this area, its progress on the Hype Cycle has slowed. However, once recovery begins, we expect to see organizations increasing attention on improving their data and analytics governance capability.

COVID-19 aside, we have seen growing hype and interest in AI model governance, analytics governance in data warehouses/lakes, trust-based governance, IoT data governance and ethics as a discrete policy. In addition to this, organizations are slowly beginning to recognize the need for a contiguous approach to governance, rather than taking their current silo-based (e.g., data governance, analytics governance) approach. Furthermore, organizations that are more mature in data and analytics show continuing interest in taking a more unified approach beyond just data and analytics governance, and are exploring unified governance, spanning quality, privacy, security and others. However, the scope of data and analytics governance remains all data and analytics: application data, content, records, external social data, master data, metadata, algorithms and AI models, analytics models, and KPIs or metrics.

User Advice: Data and analytics governance is complex, organizationally challenging and politically sensitive. It is often difficult to get executive-level consensus for governance programs, since too many organizations wrongly equate governance with compliance. As a result, too few initiatives are outcome-driven. Aim to govern the least amount of information, with the least amount of effort that results in maximum business impact, paying close attention to managing your risk. Rather than taking a one-size-fits-all approach, use adaptive data and analytics governance to apply different governance styles to your different business scenarios.

Data and analytics leaders should take the following steps:

- Identify critical business outcomes that need good data and analytics to be successful. Focus your data and analytics governance work on this, developing a business case if needed.
- Actively engage key business stakeholders in sponsoring and driving the initiative, alongside the CDO.
- Focus on the "least amount of data with the maximum business impact," to embed the work of D&A governance in the business context.
- Clearly define the scope of work related to D&A governance: policy evaluation and setting, policy interpretation and enforcement, and policy execution. The first two need to be led by business and the latter can be managed by IT.
- Link data and analytics governance to corporate governance and enterprise digital governance initiatives.
- Consider how data standards and metadata management can be used to implement data and analytics governance in the enterprise. Though business leaders may not fully understand their importance, an industrial governance capability needs enterprise-scale data and analytics capabilities.

Business Impact: Since most business goals rely on good data and analytics to be achieved, effective data and analytics governance is critical to the organization. Successful implementation of data and analytics governance will allow organizations to balance the strategic needs for data and analytics with the needs of business-area leaders. At the enterprise level, strategic goals require consistent data and analytics governance across multiple organizational and interenterprise silos. At the business-area level, it should act in a consultative manner, encouraging innovation, facilitating and supporting the governance needs of business leaders in their organizational areas.

Data and analytics governance can extend across all aspects of the data and analytics ecosystem, including:

- Abstractions — Such as metadata, analytics and algorithms
- Formats — Structured versus unstructured information
- Functions — For example, authorship, access and discovery
- Life cycles — Inception, storage, persistence, analysis, archival, disposal
- Media — Paper versus electronic
- Usage — Such as transactional/operational and analysis
- Domains — Financial data and customer data
- Types — Application data, transaction data, analytical data, files, documents, images, digital, master data, metadata, etc.

Starting with business outcomes leads to a more direct connection with the instruments of governance (e.g., policies and standards) leading to identification of the right data and analytics metrics to enable those outcomes.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Recommended Reading:

"7 Must-Have Foundations for Modern Data and Analytics Governance"

"Use Gartner's Value Pyramid to Connect Data and Analytics to Business Value"

"Reset Your Information Governance Approach by Moving From Truth to Trust"

"Data and Analytics Leaders Must Use Adaptive Governance to Succeed in Digital Business"

Unified Endpoint Management

Analysis By: Dan Wilson; Chris Silva

Definition: Unified endpoint management (UEM) is a set of offerings that comprise MDM and personal computers via traditional client management technology (CMT) or modern OS management. This is through a single console that combines the application of data protection, device configuration and usage policies. UEM tools use analytics and telemetry from users, apps and devices to inform policy and related actions; and integrate with Unified Endpoint Security (UES) tools to enhance policy management and enable frictionless authentication.

Position and Adoption Speed Justification: Gartner has long described the evolution to UEM as a journey through three waves:

- Using separate tools for PCs and mobile devices (traditional management)
- Using the same management product, but different processes, for PCs and mobile devices
- True convergence — PCs and mobile devices are managed through the MDM APIs provided by the OS, whether it's Apple iOS or macOS, Google Android, or Microsoft Windows.

Now we are seeing UEM expand beyond the management of PCs and mobile devices to offer deeper insights through endpoint analytics and deeper integration with identity and access management and unified endpoint security tools. In addition to the base UEM capabilities, many vendors are expanding their offering to differentiate. Although Gartner is seeing some clients embrace UEM tools and modern OS management, most organizations are still seeing UEM as a roadmap item to be addressed in the next few years. In preparation for UEM, organizations should:

- Modernize application stacks, removing dependencies of critical apps on a specific platform or a specific browser/runtime environment

- Consolidate mobile and endpoint management teams to eliminate political barriers to UEM adoption
- Upskill staff to understand how to address the critical functions of CMT with UEM techniques

Hype is moving toward the trough. Interest in UEM remains strong and use-case-driven, yet many organizations revealed the significant processes and technology changes that are required for modernizing management.

User Advice: Clients should stop procuring and consider not renewing licenses for disparate MDM, EMM and CMT tools. They should review existing entitlements to determine the most cost-effective and best fit UEM solution to adopt to replace those tools in the next year. They should investigate the potential to embrace modern OS management using the UEM products in the next two years.

Business Impact: Taking full advantage of UEM disrupts long-standing traditional processes, tools and organizational designs. It will require a new approach, consolidated organization and significant process reengineering, but has several benefits:

- Simplifies management of continuous OS updates.
- Enables management of devices regardless of their connection (on LAN, VPN or internet connected).
- Support a wider range of devices and operating systems.
- Enables internet-based patching, policy, configuration management.
- Reduces the total cost of ownership (TCO) of managing endpoint devices by simplifying device management and support processes.
- Supports tool portfolio rationalization and reduction efforts.
- Establishes a baseline for integrated UES tools to provide continuous, contextual authentication and controls.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: BlackBerry; Citrix; IBM; Ivanti; ManageEngine; Matrix42; Microsoft; MobileIron; Sophos; VMware

Recommended Reading:

“How to Keep End Users Connected to the Digital Workplace During Disruptions”

“Essential Considerations When Choosing Separate PC and Mobile Management Tools”

"Adopt Continuous Endpoint Engineering and Modern Management to Ensure Digital Workplace Success"

"Prepare for Unified Endpoint Management to Displace MDM and CMT"

"Magic Quadrant for Unified Endpoint Management Tools"

"Solution Criteria for Unified Endpoint Management Systems"

Business Process Risk Modeling

Analysis By: Claude Mandy

Definition: Business process risk modeling is the activities and tools used to represent the processes of an organization to provide a foundation for assessing risk by analyzing value chains, bottlenecks, controls, dependencies, critical paths and inefficiencies. Models combine process/workflow, functional, organizational and data/resource views with underlying metrics such as costs, cycle times and responsibilities.

Position and Adoption Speed Justification: Business process risk modeling has been used with limited success in risk analysis for over a decade, mostly within the financial services industry. It allows security and risk management leaders to assess risk by visualizing the logic of critical business process steps and their linkage to IT system dependencies. It is effective in assessing the effectiveness of both business and IT controls within the business context. Detailed business process risk modeling can be a costly and time-consuming process that is susceptible to human interpretation, lack of business knowledge and lack of objective validation techniques.

Effective business process risk modeling requires broad involvement of subject matter experts who understand the business and technical details required for a meaningful analysis. As a result, adoption of business process risk modeling remains limited within less than 5% of the target market and current approaches will fade into obsolescence as existing business processes are digitized into codified business logic. A smaller subset of modeling focused on identifying IT service dependencies will continue to gain adoption with the target audience between 5% and 20% already using it extensively within business continuity management and IT resilience.

User Advice: SRM leaders considering use of business process risk modelling should reduce the effort and cost by:

- Focusing on business processes where detailed understanding of business processes can increase the effectiveness of controls, such as improving logging and monitoring, enforcing segregation of duties and improving IT resilience.
- Understanding existing business process modeling capabilities or integrations in existing IT risk management or IRM solutions.
- Leveraging existing business process models or data, such as relational data from configuration management databases (CMDBs) or IT service dependency mapping (SDM) tools where possible.

- Focus on understanding the business logic behind the process flow rather than describing observed process flow.
- Investing in process mining capabilities that are designed to discover, monitor and improve actual processes (that is, not assumed processes) by extracting knowledge from event logs readily available in today's information systems.
- SRM leaders should be cognizant that business process modelling is not a once-off exercise. Without process mining capabilities to keep all discovered and modeled processes up to date, organizations will need to update models manually for every change or refresh models regularly to keep business process models up to date and consistent. Accuracy is critical to providing the insight needed to assess and improve the effectiveness of controls.

Business Impact: Business process risk modeling can be costly and time-consuming as it often requires input from both technical and business stakeholders across multiple functional areas and systems. It requires ongoing effort to maintain accurate business process models. As a result, business process risk modeling has not been widely adopted. However, the visualization of process flow and linkages between critical business process and IT system dependencies can significantly increase understanding of business logic and the subsequent design and effectiveness of controls. Controls that can be significantly enhanced through understanding of business processes include logging and monitoring, segregation of duties and IT resilience.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: BusinessOptix; Celonis; Minit; QPR Software; Signavio; Software AG

Recommended Reading:

"Enhance GRC With BPM for Improved Enterprise Risk Management"

"Market Guide for Process Mining"

"How Process Mining Can Support Operational Resilience in Times of a Crisis"

Environmental, Social & Governance

Analysis By: Sarah Watt

Definition: Environmental, social and governance (ESG) refers to a collection of corporate performance criteria that assess the robustness of a company's governance and its ability to effectively manage environmental and social impacts. ESG-based analysis aims to link a company's performance in ESG indicators to its overall financial performance. Corporate social responsibility (CSR) is a management concept that leads businesses to account for the short- and long-term environmental, societal and economic implications of their business decisions.

Position and Adoption Speed Justification: Leading companies use CSR to uncover opportunities and manage risks, to achieve sustainable business outcomes. What has changed compared to previous years, is that momentum behind CSR has accelerated. Firstly, investors continue to focus on ESG performance — boards must act now to oversee strategic long-term plans, based on materiality, that are likely to include action on climate change, responsible sourcing and water scarcity among other macro issues. Secondly, consumer concern around issues such as climate change and end-of-life plastics continues to increase.

CSCOs must prepare for increased demands from stakeholders to comprehensively disclose and set ambitious improvement targets for their environmental and social impact. CSR is unlikely to go away as many countries, as a result of COVID-19, consider tying economic stimulus to CSR and carbon reduction activities.

User Advice: Get started now! An effective CSR-based strategy will identify opportunities and risks. Don't wait for negative shareholder votes, customer boycotts or a reputation crisis before initiating and developing a CSR governance infrastructure.

- Become familiar with fundamental CSR concepts, such as stakeholder engagement, materiality and CSR reporting standards, and data collection methods. Ensure actions are aligned with the UN's Sustainable Development Goals.
- Assess the maturity of your organization's governance infrastructure for managing CSR within supply chain and determine strategies to advance to the next level (see "How Supply Chain Leaders Can Start and Advance Their Sustainability Journey").
- Learn more about the complex environmental and social issues affecting your industry or company by talking to peers, customers and stakeholders.
- Collaborate with investors and others to prioritize the material areas of environmental or social risk exposure. Take note that the emphasis on strategies for reducing greenhouse gas emissions has increased in the last 24 months (see "Supply Chain Brief: Set and Invest in Radical Goals for Greenhouse Gas Emissions Reduction").
- Mobilize resources on signature, audacious projects. Although companies initially start these projects within their own organizations, more mature CSR programs bring about change across the ecosystem.
- Advocate that companies promote their CSR strategies when recruiting "millennial" workers who consider companies' environmental and social impact as they consider supply chain management employment options (see "Supply Chain Brief: How to Compete for Millennial and Gen Z Talent").

Business Impact: Businesses using CSR as a platform for strategy, risk management, talent management, innovation and growth must significantly reorient their decision-making frameworks to widen their focus beyond short-term profits, costs and service. Given the complexity, the changes associated with adopting a CSR-based strategy and governance infrastructure involve a transformational and potentially revolutionary journey with changes in processes, roles, performance metrics and trade-off decisions.

Leaders must organize an ecosystem of partners inside and outside the enterprise. For example, CSCOs must work with finance, legal and compliance, as well as suppliers and logistics partners, on effective risk assessment and mitigation strategies. Leading companies engage in precompetitive problem solving with third parties (consultants, nongovernmental organizations) or industry consortia.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Recommended Reading:

"How to Lead Supply Chain in the Big Shift to Sustainable Business: A Gartner Theme Insight Report"

"Supply Chain Brief: Help Stakeholders Adapt to Sustainability by Sharing Fundamental Definitions"

"Supply Chain Brief: Make Strategic Choices for Measuring and Reporting Sustainability Performance"

"Use 3 Change Leadership Strategies to Build Backing for Early-Stage Supply Chain Sustainability Initiatives"

"The Need for Multispeed and Sustainability in Retail's Last Mile"

"A Guide to the Packaging Sustainability Initiatives of the 2019 Gartner Supply Chain Top 25"

"Strategies to Build and Advance Sustainability Programs in Logistics"

IT Vendor Risk Management

Analysis By: Joanne Spencer

Definition: IT vendor risk management (VRM) is the process of ensuring residual risk, associated with vendors and service providers (that access sensitive data or systems or manage critical business processes), is effectively managed. The discipline of VRM addresses the mitigation and remediation of these risks to avoid business disruption and financial and regulatory impacts. VRM technology supports various activities as part of a broader VRM framework for identifying, assessing, analyzing, remediating and monitoring vendor threats and risks.

Position and Adoption Speed Justification: Increased reliance on vendors exposes enterprises to greater risk of business disruption and damage to their brand and reputation. Lack of visibility into the third and fourth parties (e.g., subcontractors), major security breaches, rapid adoption of cloud models, global pandemic, and increasing regulatory requirements heighten the need for VRM technology solutions.

As independent stand-alone solutions arise and the ease of implementation improves, we anticipate the adoption of these solutions will continue to increase, primarily in response to increased risk, data privacy, and cybersecurity regulations. Three issues and trends could affect adoption and extend the slide of VRM through the Trough of Disillusionment:

- Additional resources (both personnel and budget) needed to provide ongoing monitoring and tracking of vendors
- Lack of mature VRM programs, expertise and processes
- Growth and adoption of security and risk rating services (BitSight, SecurityScorecard, RiskRecon, UpGuard, Panorays, FICO, etc.), and vendor risk assessment data in a shared model (Prevalent, CyberGRX, Venminder, OneTrust, TruSight Solutions)

User Advice: IT VRM is a critical element of enterprise and IT risk management. Regulatory guidance (OCC FFIEC, HIPAA) and newer privacy and data breach notification regulations (GDPR, NYDFS, etc.) mean it is an essential requirement for many industries. However, it's not all about risk mitigation. IT VRM can be a catalyst for improved vendor performance, by identifying vendor-related risks early and mitigating them through effective controls and process improvements.

VRM solutions automate part or all of the assessment, analysis and control validation process, provide remediation and mitigation guidance, and facilitate monitoring of risks associated with vendors and other third parties that access, support or control information assets. VRM solutions are stand-alone or exist in broader IRM strategies, procurement, vendor management or third-party management solutions. Some VRM solutions are industry-focused, whereas others are more focused on providing outsourced or an out-tasked model. Implementation and customization vary between tools — while some are delivered on-premises, SaaS-only delivery models are now commonplace.

Gartner recommends:

- Select VRM solutions that provide a common system of record for all parties involved in the VRM program.
- Ensure that processes and methodologies used by the enterprise for IT VRM are supported by the VRM solution. Increasingly, solutions are integrating with risk and security rating services, risk exchanges and content providers to assist with ongoing vendor risk monitoring.
- Develop a roadmap to improve VRM maturity and align your solution decisions with your current and planned maturity levels. Without that, a technology solution will not deliver the expected value.
- Ensure that all relevant stakeholders are engaged in VRM workflows, including risk management, IT security, procurement, vendor management, legal and business continuity management.

Business Impact: Some industries (e.g., banking, financial services and healthcare) have industry-specific regulations that mandate vendor risk monitoring. Others face compliance pressures to improve VRM due to Payment Card Industry (PCI) data, Securities Industry and Financial Markets

Association (SIFMA) requirements for business continuity management (BCM), local and national data breach notification regulations, and other privacy regulations.

VRM can be a catalyst to improve vendor performance by identifying risks early and mitigating them through effective controls and process improvements.

To get the most value from VRM solutions:

- Treat vendor risks as drivers affecting the quality of products and services defined in vendor contracts.
- View vendor risks with overall business unit and/or enterprise risk. Integrate results from the VRM solution with the larger set of risk assessment results from enterprisewide initiatives.
- Prioritize risk weightings based on criticality of solutions and technology, and sensitivity of data or IP that a vendor may access or control.
- Ensure vendors perform their contracted risk obligations, including risk reporting, security incident notifications and business continuity plans.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Allgress; Galvanize; MetricStream; NAVEX Global; OneTrust; Prevalent; ProcessUnity; RSA; ServiceNow; SureCloud

Recommended Reading:

“Critical Capabilities for IT Vendor Risk Management Tools”

“Magic Quadrant for IT Vendor Risk Management Tools”

“Develop Contingency Plans for Your Critical Suppliers, or Risk Business Disruption”

“Navigating the Vendor Risk Management Solution Market”

“Formalize Vendor Risk Management Practices to Lessen the Probability of Business Disruption”

End-to-End Supply Chain Risk Management

Analysis By: Kamala Raman

Definition: End-to-end supply chain risk management (E2E SCRM) aims to make businesses resilient to supply chain risks across the physical and digital ecosystem. It combines strategic design of products and network with tactical flow optimization flow and operational mitigation of

and response to disruptions. It is strengthened by technology used for risk identification and monitoring, holistic risk impact analysis and coordinated operational mitigation/response.

Position and Adoption Speed Justification: Although the risks of supply and operational disruptions have become front and center during the COVID-19 pandemic, risks could be commercial, financial, regulatory, reputational, environmental or digital in nature. Organizations have found that existing risk frameworks have largely not been effective in managing pandemic response and at the same time, the importance of balancing risk against other competing network objectives has shot up.

A SCRM framework should create visibility to the network, identify risks, assess their impact, monitor risks and create a mitigation/response strategy. Risks should be measured on impact and frequency of incidence but also on the ability to detect. Supply chain visibility and response quality can be improved with control tower like capabilities, however the ability of organizations to create a holistic framework that goes beyond simply managing for the most recent threat has to catch up.

Conventional risk mitigation has been focused on operations disruptions. But for most organizations, investments in inventory or capacity buffers for resilience require resources that may directly compete with the goal of operational efficiency. Beyond this, risks that are harder to predict are here to stay in several areas. Intensifying geopolitical competition is threatening unfettered global trade. Data breaches and cyberattacks that severely disrupt operations or impact products are growing. Climate change, extreme weather events and the threat of resource constraints must be managed. As outsourcing expands, the adoption of tools to monitor multiple tiers of suppliers for quality, performance or social responsibility risks is growing. Solutions that integrate products, information, services and corporate islands of risk data are proliferating. But organizational ability to act on this information at a network level is still maturing due to the collaboration required across multiple functions for a true E2E SCRM framework.

Longer term, supply chain risk management should balance the value of resilience for agility and an improved customer experience in ecosystems focused on cost efficiency. The right level of resilience may vary even within an organization based on the nature of product portfolios, market presence and profitability structures.

User Advice: Supply chain strategists responsible for risk management should:

- Define an E2E SCRM framework, which spans all three horizons relevant for risk management, and integrate for data sharing with core business systems.
- Identify product design stage gates, key sites, critical sourcing arrangements, product flow paths and transportation hubs, to track interdependencies, bottlenecks and potential failure points within the business network.
- Identify and prioritize risks by impact, likelihood of occurrence, level of control and financial value at risk to generate a register of the most impactful risks.
- Where individual risk events cannot be predicted, establish measurement criteria, such as maximum recovery time or lead times and set thresholds for monitoring and notification.

- Create risk mitigation strategies focused on risk reduction, avoidance, transfer or acceptance. Simulation and scenario planning by testing alternate network designs can help with risk mitigation. Escalation plans for vendors and customers is a way to manage risk transfer. Business continuity plans or crisis preparedness refines risk response strategies while inventory can help cover recovery time during disruptions.
- Regularly review and test business continuity plans. Network resilience requires quick responses and speedy execution of remedial actions once a risk event has been detected.
- Perform a continuous improvement assessment that assesses the quality of risk responses and update the SCRM framework based on mitigation efforts already in place.
- Organizations must dedicate the funds and resources ongoing risk management, along with the governance to manage performance and risk.
- Users need to invest in technologies to support E2E SCRM, combining two or more solutions as needed. For example, network design tools to design for resilience and supply chain visibility tools for live incident monitoring and intelligent response.

Business Impact: In a global multitier network, complex interdependencies can make detection and impact analysis of key risks challenging. Mitigating these risks also requires action across multiple partners in the network and good tracking of outcomes to bolster accountability. Tactically, in lean supply chains, organizations are exposed to disruptions when inventory time to survive is less than supply time-to-recover. Strategically, they may overemphasize high visibility but low probability events at the expense of a comprehensive approach. Organizations must determine the right balance between cost efficiency and resilience and selectively invest in redundancy measures. E2E SCRM designs supply chains for resilience and manages for and mitigates ongoing risks using scenario analysis to balance between the false certainty of a single forecast and paralysis from overanalysis. The business impact is, therefore, significant.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Achilles; DHL Resilience360; Elementum; m-risk; riskmethods; Resilinc; Sourcemap

Recommended Reading:

“Design Resilience Into Your Supply Chain With Scenario Planning to Weather the Unexpected”

“Get Ahead of the Expanding Risk Frontier: Supply Chain Security”

“How Your Supply Chain Should React to Tariff Uncertainties in the United States and China”

“Weathering the Storm: Supply Chain Resilience in an Age of Disruption”

Operational Technology Security

Analysis By: Ruggero Contu

Definition: Operational technology (OT) security is the practice of protecting critical production and operation systems and services in asset-centric enterprises. OT security addresses industrial automation and control as well as other nonindustrial use cases where physical state changes depending upon secure, safe and reliable function. It also addresses the impact of using IT, IoT and physical security technology and practice when doing so. OT security is part of comprehensive digital security for digital transformation.

Position and Adoption Speed Justification: OT security technologies provide controls to secure OT environments, with the aim to preserve reliability and safety of production and operations environments. Established international standards, such as IEC 62443, European NIS, NIST 800 Series guidance frameworks, among others, provide product and service providers with direction related to function with vertical specific requirements that the OT security market is starting to address.

The OT security market consists of IT security companies that have extended capabilities of existing solutions to address specific OT functional differences and requirements. They also extended capabilities to address specific OT system providers adding security controls to their OT platform offerings and specialist OT security companies that have come to market to address specific OT-related security needs. Recent offerings address industrial IoT (IIoT) requirements as well.

Obstacles in OT security remain in coverage across all verticals and all major OT systems. They also address legacy OT system requirements, keep pace with regulatory requirements and changes to those requirements, provide cultural and organizational challenges in IT/OT integration, and provide scalability and support globally. OT security providers are making progress and expanding market presence (as 2020's Hype Cycle shows) as a result of improved maturity on the buyer side. A selected number of products are entering a phase of significant adoption. IIoT security technologies are leading future evolution with less expensive offerings, more extensive data collection and flexible command functionality.

User Advice: Security and risk managers should:

- Pursue a cyber-physical approach to achieve an IT/OT/IoT alignment and integration strategy for digital security that underscores governance, strategy and planning as a more centralized process reporting, toward an adaptive security approach.
- Accelerate OT security assessments with reputable and specialist consulting firms to assist in finding risks and gaps to be addressed by the security controls and infrastructure, and implement skills training and awareness schemes for converging IT and OT where possible.
- Map OT leading performance indicators against IT/OT leading risk indicators to write security policies consistent with maintaining and improving performance.
- Apply OT security controls based on digital security policies across OT infrastructure where needed.

- Build repeatable processes for service portfolio management to manage the growing security service portfolio supplementing in-house OT security systems.
- Develop coordination in the OT supply chain to assess partner security controls affecting your organization.
- Focus early infrastructure purchasing on asset discovery, monitoring and reporting, anomaly and incident detection and response, vulnerability management, access control, endpoint security and network segmentation.
- Focus on organizational and cultural challenges by restructuring as required and establishing complete communication and awareness programs between IT and OT.
- Apply pressure on equipment vendors to ensure that their (future) systems are secure by design.
- Apply defense-in-depth strategies to OT security.

Business Impact: OT security is of major relevance to asset-centric organizations such as those considered to be part of national critical infrastructure (for example, energy and utilities, transportation, oil and gas, manufacturing, and natural resources) and other general industrial verticals. It is also found in commercial markets in areas such as building automation and facilities management, healthcare, and retail. OT security is also useful in addressing specific engineering needs for protecting real-time, event-driven systems that have high impact on safety of people and environments. As such, adoption rates for OT security solutions have risen year over year as understanding and market availability have provided options for organizations.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Barracuda; Cisco; Claroty; Forescout Technologies; IBM; Kaspersky; Microsoft; Nozomi Networks; PAS; Radiflow

Recommended Reading:

“Competitive Landscape: Operational Technology Security”

“Secure Your OT With Basic Security Hygiene”

“OT Security Best Practices”

“Market Guide for Operational Technology Security”

“How to Develop a Security Vision and Strategy for Cyber-Physical Systems”

“Market Insight: Act Before Convergence Kills Your Stand-Alone OT/IoT Security Product Solution”

“Market Trends: IoT Edge Device Security, 2020”

Climbing the Slope

Crisis/Emergency Management Solutions

Analysis By: Roberta Witty

Definition: Through a common operating picture or single pane of glass, crisis/emergency management (C/EM) solutions provide consistent orchestration and management of a crisis through all its phases. C/EM solutions are used to manage the data, resources, expenditures, communications and tasks associated with the crisis and analyze the changing crisis conditions to enable situational awareness. Also, they ensure crisis/emergency management procedures comply with government, regulatory and industry emergency management standards.

Position and Adoption Speed Justification: The goal of crisis/emergency management is to contain and minimize a crisis or incident. A crisis may take several forms: weather events, natural disasters, public health emergencies, man-made events, accidents, information security breaches, infrastructure failures. Damage can be done to people, assets, an organization's reputation and revenue streams, and public safety compromised. To protect the reputation of the organization in the eyes of all stakeholders — employees, customers, citizens, partners and suppliers, auditors, and regulators — C/EM solutions are used to:

- Improve the organization's ability to protect public and workforce safety, and restore services as quickly as possible
- Codify the roles, responsibilities and decision-making authority involved with a crisis
- Improve the efficiency of crisis/incident command and control through continual progress assessment
- Manage relationships and communications with internal and external stakeholders, including between critical infrastructure service providers and government agencies during regional and nationwide disasters
- Manage response, recovery and restoration phase actions for the event through task and workforce management
- Manage media communications, including national services and social media traffic
- Manage expenses incurred during the crisis to better ensure their repayment from business interruption insurance policies
- Integrate with hazard risk intelligence services to provide pre-event risk management
- Provide postincident reviews for regulatory reporting and overall process improvement

COVID-19 has triggered a dramatic increase in interest in C/EM solutions, which can now consolidate organizational data with public health data to provide an integrated picture of the impacts of the crisis on the organization. Data integration, visualization and artificial intelligence (AI) are key capabilities that have accelerated the benefit of C/EM solutions in pandemic management.

Some business continuity management program solutions have added C/EM and pandemic management capabilities to their solutions to ensure a complete BCM process.

The 2020 Hype Cycle position remains the same as the 2019 Hype Cycle position, moving out of the Trough of Disillusionment. This is because C/EM implementations are still mainly used for government or quasi-government organizations (e.g., airports). However, due to COVID-19, we expect a significant investment, growth and adoption of these solutions as organizations realize the value in using them for crisis management as well as pre-event risk management. Hence, we expect that crisis management capabilities will become part of day-to-day operations solutions so that risks can be anticipated early, and action to mitigate or respond can be better executed.

User Advice: Organizations considering the purchase of a C/EM should:

- Match the C/EM solution selection to the use case of the business. This is especially true for the healthcare provider and utility sectors, which have regulatory prescribed processes that must be performed to ensure the safety of citizens, customers, patients and the workforce.
- To ensure interoperability with public-sector response agencies, choose a platform that adheres to public-sector emergency management protocols relevant to the geographic regions in which the solution is deployed — e.g., National Incident Management System/Incident Command System (NIMS/ICS) in the U.S., and the UAE's National Emergency Crisis and Disaster Management Authority.
- Organizations exposed to environmental, health and safety (EH&S) issues should adopt solutions that are interoperable with regional public-service protocols. This will help ensure timely and efficient responses that minimize damage, and consult with their corporate counsel for jurisdictional issues relating to privacy and rules of evidence.
- Organizations that already have a BCMP solution should evaluate the crisis/emergency management capability of that solution before selecting a pure-play C/EM solution, as it may not be required.

Business Impact: C/EM solutions may be:

- Specific to the operations of one industry (use case) — for example, government, military, electric utilities, transportation, public health, healthcare, or oil and gas
- Generalized for the management of any type of crisis — for instance, crisis/emergency management functionality as found in a BCMP solution
- Part of an EH&S application
- Part of a custom-developed BPM-platform-based case management framework solution
- Specific to the operations of one aspect of business operations — for example, supply chain crisis management
- Specific to a specific crisis event — for example, pandemic management

C/EM solutions help organizations impose a standardized, best-practice model, including uniform managerial controls across the organization. They also reduce staff training time and ensure better integration with the broader internal and external community involved in recovering from a disaster.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: 4C Strategies; Esri; Everbridge; Fusion Risk Management; Grey Wall Software (Veoci); IntraPoint; Juvare; LiveProcess; Swan Island Networks; Tableau

Recommended Reading:

"Market Guide for Crisis/Emergency Management Platforms"

"Magic Quadrant for Business Continuity Management Program Solutions, Worldwide"

"Critical Capabilities for Business Continuity Management Program Solutions, Worldwide"

Hazard/Threat Intelligence

Analysis By: Roberta Witty

Definition: Hazard/threat intelligence services evaluate worldwide incidents that threaten the health and safety of citizens and the workforce, cause damage to critical physical and technology infrastructure, or cause a disruption to normal business operations. These predictive hazard/threat intelligence alerts are delivered to customers in real time for early warnings and in-progress events. In 2020, we renamed "hazard/threat intelligence services" from "hazard risk analysis and communications services," which appeared in prior Hype Cycles.

Position and Adoption Speed Justification: Hazard/threat intelligence services deliver alerts and reports at the facility, neighborhood, regional, national and international levels to clients via email, SMS, phone, and print. To do so, they leverage thousands of information sources — including in situ and remote sources such as news outlets, government agencies, academic, political and business personnel, institutions, and technology resources. Some hazard/threat intelligence solutions provide additional services, which include:

- A centralized communication hub for worldwide personnel, including a 24-hour hotline for access by personnel who may be in harm's way
- Travel risk management services
- Medical, security, kidnapping or evacuation assistance to personnel impacted by an incident

The awareness of incident specifics (aka situational awareness) is improved by such services as GIS for geolocation analysis of people, facilities, suppliers and other resources, and layered data visualization for many risks an organization may face. Therefore, more organizations, especially

those with a multilocation footprint, are adopting these tools. The GIS capability, in particular, provides a significant benefit to business operations, physical security and BCM, because the service can be tailored specifically to an organization's operations. By categorizing the severity of incidents and geocoding their resources/assets in the system, alerts can be prioritized and directed to the right people within the organization in real time for investigation and faster response actions.

Due to the COVID-19 pandemic, some offerings now include intelligence alerts for changes in government directives regarding lockdowns, stay-at-home orders, social distancing and return-to-the-workplace protocols.

The 2020 position remains at the 2019 position, comfortably past the Trough of Disillusionment. Although the number of incidents around the world is increasing, our biannual BCM survey show that adoption of hazard/threat intelligence services remained relatively the same as in 2019, at 36%. However, we expect to see the adoption for these services to grow based on the post-crisis effect of COVID-19. The increased risk awareness after-effect from COVID-19 will encourage adoption for more frequent use cases, such as organizational compliance with duty of care regulations, and integration with emergency/mass notification services (EMNS) and crisis management software. This added adoption will help mature the overall crisis management processes within organizations.

User Advice: Organizations should integrate these services with EMNS and crisis/incident management software tools to gain improved situational awareness before and during an event. Organizations should consider the use of hazard/threat intelligence services when:

- They are maturing their BCM or operational risk management programs to include crisis/incident management and travel risk management
- Their operations are in locations that have a medium to high level of risk of environmental, geopolitical, weather-related and health-related incidents
- They have a medium to high percentage of the workforce that travels on a regular basis (for example, daily or weekly)
- They have personnel regularly traveling to and from medium- to high-risk locations
- Look for a solution that includes:
- Multiple sources of hazard/threat intelligence alerts that cover multiple crisis event types (e.g., weather, natural disasters, law enforcement, medical/public health, government directives, supply chain, traffic, social media, biohazards, accidents, economic crises, cultural events, geopolitical/terrorist attacks, crime, civil unrest, etc.), for all of your operating locations — global and hyperlocal
- GIS capability that can be customized to your operating footprint
- Risk intelligence communication via phone, email and SMS, and customer-customizable reporting
- Mobile device app support for communications and interactive situational awareness activities

Business Impact: Hazard/threat intelligence services are used by government and private enterprise professionals in corporate security, BCM, HR, supply chain management, travel risk management, watch command, fusion centers and more for a number of purposes:

- Risk assessments of all operating locations as part of the due diligence done for business decision making, such as data center or recovery site development, and personnel or operations relocation
- Situational awareness for the impact of disruptions on production operations, traveler and expatriate duty of care, and other corporate-interest impacts
- Preparedness and response management for large-scale scheduled events, such as sporting events (e.g., the Olympics, Super Bowl and World Cup), global government meetings (e.g., the G20 summit) and political conventions.

Incidents that can cause a business disruption can occur 24/7, every day of the year. Without accurate and timely information, knowing which incident will turn into a crisis that requires a directed response can be a daunting task. Monitoring the multitude of news sources from the news networks, the internet, social media outlets and more can result in information paralysis and under- or overreacting to an incident. For this reason, we assign a high benefit rating to this technology service.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Anvil; CountryWatch; Dataminr; Everbridge; International SOS; Kinetic Global; Risk Intelligence; SAP Concur; Willis Towers Watson (Alert:24); WorldAware

Recommended Reading:

“Market Guide for Crisis/Emergency Management Platforms”

IT Risk Management Solutions

Analysis By: Khushbu Pratap; Claude Mandy; Brent Predovich

Definition: ITRM solutions operationalize the risk management life cycle for scenarios originating in or attributed to digital infrastructure, applications, systems, processes and teams. These deliver primarily three ITRM buyer use cases: basic risk and controls self-assessment, advanced risk management and governance, and cybersecurity risk management. ITRM solutions have critical capabilities ranging from workflow design, risk analysis and reporting, to board reporting, digital asset discovery, and basic and advanced integrations.

Position and Adoption Speed Justification: The ITRM market maturity level continues at “early mainstream,” with a market penetration of 20% to 50%. It is not projected to plateau for another three to five years. The pandemic has shined a strong light on IT operational dependencies, even

more so as a result of moving to remote and extended operating environments. Combined with a continuing, heightened focus on cyber-risk exposures, buyers have maintained high levels of interest in ITRM solutions; and interest will persist due to cybersecurity mandates seen worldwide.

Although many organizations are using ITRM solutions to manage security and technology risk exclusively, they have begun adding business context in prioritizing vulnerabilities. This prioritization of business context aligns with a steadily increasing maturity in risk management discipline. Adoption levels for ITRM solutions have been higher in North America and Europe, followed closely by the APAC region. We see slow adoption in the Middle East and Africa.

User Advice: Gartner discourages buyers from trying to use these solutions to create functions and workflows without process clarity in their organizations. The market reality is that not all buyers wait for sufficient maturity of their processes before looking to automate those processes and, by doing so, often cause more confusion and loss of time and investment. There is no single best product for all organizations. However, there are typically several good options to fit a specific set of requirements. Key considerations in planning and procuring ITRM solutions include the following:

- Use Gartner's definition of ITRM solutions as a starting point and tailor to your requirements. Go beyond capabilities, implementation, integration, price and support. Select vendors based on their ability to scale and flex with your risk management journey.
- Organizations looking to deploy ITRM solutions must know that the labor associated with populating asset, process, risk and control repositories is significant. This should be considered prework in operationalizing ITRM as an initiative. The scope of prework varies for organizations and, at minimum, requires one FTE.
- Buyer interest in ITRM solutions is often combined with interest in vendor risk, corporate compliance, operational risk or audit management solutions. The main advantage is integration of risk data, workflow and dashboards served up consistently with context to risk owners, risk management teams, and internal audit respectively. If there is no need for correlated information all in one place, then a best-of-breed vendor in one of these areas may be a better choice.

Business Impact: ITRM solutions can offer tangible, direct cost savings in replacing manual effort of FTEs that are needed to coordinate and evidence risk governance in the digital environment. For heavily regulated organizations, penalties avoided from industry enforcement bodies and regulators are attributed toward indirect savings. For all organizations, operational disruptions avoided by potential incidents traced to digital infrastructure, services and applications can be attributed to the cost of running resilient organizations.

Among intangible benefits, ITRM solutions track deviations against chosen baselines and facilitate monitoring of selected risk indicators. Approximately 30% buyers globally either plan to consolidate information in ITRM solutions or already do so to enable management of cyber-risk initiatives. This facilitates cyber-risk reporting to senior management and board members directly or by way of rolling up risk to enterprise risk dashboards and supporting internal and external audits.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Allgress; Dell Technologies; Galvanize; IBM; LogicManager; MetricStream; NAVEX Global; Resolver; SAI Global; ServiceNow

Recommended Reading:

"Critical Capabilities for IT Risk Management Solutions"

"Critical Capabilities for IT Vendor Risk Management Tools"

"6 Principles for Digital Business Risk Assessment"

Business Continuity Management Program Solutions

Analysis By: David Gregory; Roberta Witty

Definition: BCMP solutions are the primary tools used to manage BCM programs and their artifacts for all phases of the life cycle, from planning to crisis activation. BCMP solutions provide capabilities for availability risk assessment, business impact analysis, business process and resource/asset dependency mapping, recovery plan management, exercise and crisis management, and BCM program management metrics and analysis.

Position and Adoption Speed Justification: Organizations need a consistent, repeatable process for all aspects of the BCMP development process. Also, the growing focus on BCM program metrics has increased BCMP solution sophistication by providing program analysis capabilities, which more mature BCM programs use to promote resilience in day-to-day business operations. The biggest competitors for BCMP solutions are "do-it-yourself" approaches leveraging Microsoft Office tools, with SharePoint as a document repository. Almost all BCMP solutions are available as SaaS solutions, which is extremely beneficial when there is a real disaster, and internal IT services (including potentially on-premises BCMP solution access) and systems are not available.

In the 2020 Hype Cycle, we retained BCMP solutions at its 2019 position. This is because there has been no significant change in the adoption rate during the past 12 months. There is, however, significant evidence that this may change over the coming months.

The COVID-19 pandemic has placed a direct spotlight on organizational resilience, and this is likely to be a significant factor in generating interest in the BCMP market during 2020 and 2021. This is likely to be particularly true in small and midsize businesses (SMBs), where BCM activities are often ad hoc, fragmented and practiced in departmental silos, which has led to a slow and disjointed response. Where this is the case, it is probable that organizations will be interested in BCMP solutions because they provide an easy way to jump-start a BCM program and deliver great benefit due to the standardization and centralization of BCM activities.

The BCMP solution market continues to enter the Plateau of Productivity level for large and extra-large organizations, regulated enterprises, government agencies, as well as for organizations with complex business operations.

We anticipate continued adoption during the next five years, given the increase in preparedness initiatives across all industries, especially due to COVID-19 and continued targeted cyberattacks.

User Advice: Consider a BCMP solution when you are:

- Starting a new BCM program and want to follow standard practices throughout the organization
- Updating or automating your current BCM program and processes, such as risk assessments and business impact analyses
- Maturing your BCM program, thus needing more program management analytics than traditional office management tools can provide
- Expanding your BCM program's automated footprint to gain more control over the execution phase of the BCM program life cycle
- Integrating plans from several departments, business units, divisions and legal entities into a consistent and easily updated set of recovery plans reflecting all elements of the organization
- Developing future pandemic plans and procedures

Do not overbuy; instead, focus on:

- Ease of use for business users, not IT or BCM program office users only
- Ease of configuration (not code customization) and reporting — by you, not the vendor — to your organization's continuity delivery framework, for example
- Ease of integration with other key business applications — such as enterprise directories, HR tools, business process management tools (internally developed or purchased), CMDBs, IT asset management (ITAM) tools, BCM solutions your organization may have purchased (e.g., EMNS or crisis/emergency management platform [C/EMP] solutions), and news feeds to a BCM program dashboard
- Mobile device (smartphone or tablet) support for recovery plan access and execution at the time of a business disruption

If your organization is already using an IRM solution, then evaluate that product's BCMP capability to determine whether its functionality will support your BCM program.

Business Impact: BCMP solutions will benefit every organization wanting to perform a comprehensive analysis of its preparedness level to cope with business or IT interruptions. BCMP solutions also allow businesses to establish up-to-date, accessible plans that will help to facilitate robust response, recovery and restoration actions.

If used to its complete potential, a BCMP solution database becomes a “gold mine” that can be used to enhance business operations and resilience outside of recovery. It can be used in areas such as:

- HR management
- Business and IT reengineering by finding duplication of services or rarely, if ever, used services
- M&As by having a map of business services to other critical assets

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Sample Vendors: Assurance Software; Avalution; Continuity Logic; Dell Technologies (RSA); Fusion Risk Management; Infinite Blue (BC in the Cloud); Premier Continuum; RecoveryPlanner; SAI Global (Strategic BCP); ServiceNow

Recommended Reading:

“Market Guide for Emergency/Mass Notification Services”

“Market Guide for Crisis/Emergency Management Platforms”

“Magic Quadrant for Business Continuity Management Program Solutions, Worldwide”

“Critical Capabilities for Business Continuity Management Program Solutions, Worldwide”

Cloud Access Security Brokers

Analysis By: Steve Riley

Definition: Cloud access security brokers (CASBs) provide crucial cloud governance controls for visibility, data security, threat protection, and compliance assessment in SaaS and IaaS. CASBs consolidate multiple types of security policy enforcement into one place. Examples include authentication, single sign-on, authorization, device profiling, data security, logging, alerting, and malware removal. Most CASB deployments are cloud-based; on-premises deployments are rare.

Position and Adoption Speed Justification: Vendors offer feature-rich products to increase cloud visibility and apply consistent policy across multiple providers. Execution across all vendors is variable: while some have incrementally improved and added new capabilities, the leading vendors continue to make significant investments that have contributed to the rapid maturation of the market. The acquisition phase of the market has ceased. Major incumbent security vendors now offer a CASB, either stand-alone or as part of a product portfolio; integration with other products in portfolios is inconsistent but improving. While the number of independent vendors has stabilized, the most relevant independent vendors demonstrate sustained innovation and broad market reach. Differentiation among vendors is becoming difficult, and several have branched beyond SaaS

governance and protection to include custom application support in IaaS clouds, cloud security posture management (CSPM) capabilities, and user and entity behavior analysis (UEBA) features.

The most relevant independent vendors continue to receive venture capital funding, while funding for the less well-known private vendors remains uncertain. The pace of client inquiry indicates that CASB is a popular choice for cloud-using organizations. Gartner's 4Q19 security spend forecast predicts a significant but slowing growth rate for CASB: 45.3% in 2020, 40.7% in 2021, 36.7% in 2022, and 33.2% in 2023. While the forecast predicts slowing spend for all security markets, CASB's growth remains higher than any other information security market (see "Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 4Q19 Update").

User Advice: Examine vendor capabilities in four functionality areas: visibility, data protection, threat detection and compliance. All relevant CASB vendors interact with SaaS applications via APIs and can be positioned in-line for real-time traffic visibility. CASB proxies may or may not require endpoint agents for traffic steering outside proxied networks; factor this into your evaluation. Increasingly, CASB vendors offer remote browser isolation as an adjunct to in-line deployments.

Common deployment scenarios that deserve special scrutiny include:

- **Cloud discovery and risk assessment.** Evaluate the thoroughness of the CASB's analysis of an organization's cloud security posture. The CASB should discover every cloud service in use and assign each one a risk score (ask vendors for information about how often this is updated), gleaned from attributes whose weights can be modified by customers. Evaluate the CASB's CSPM capabilities for assessing risk in IaaS storage, compute and virtual network configurations.
- **DLP.** Evaluate whether CASB capabilities are sufficient or require augmentation with deployed enterprise DLP product, either via ICAP or RESTful API integration. In-line CASB DLP capabilities should provide a mechanism to control the movement of sensitive information into and out of cloud services in real time. Examine CASB support for data classification features that can link to existing enterprise classification tools.
- **Adaptive access control (AAC).** Examine techniques vendors provide for altering the behavior of governed applications based on signals observed during and after login. AAC allows for shades of access (e.g., read-only access to content on unmanaged devices) that are more useful to the business than blocking access completely.
- **UEBA.** Evaluate how CASBs detect and isolate risky users and devices. Insider threats and compromised accounts are common attack vectors. Seek mechanisms that build baseline behavior profiles (such as typical upload/download amounts and user locations) and alert and mitigate when behavior deviates from baselines. Step-up authentication is an important capability to test with whatever IAM vendor is already deployed.
- **Third-party app discovery and control.** Ensure that the CASB can detect all third-party apps that have been granted access to SaaS applications (almost always via OAuth). Look for more than single yes/no controls for each app and instead favor the ability to group third-party apps into categories based on OAuth scopes.

- **Regulatory compliance.** Determine whether the CASB offers sufficient visibility and control for aspects such as user privacy and data residency. Carefully scrutinize encryption mechanisms. Encrypting data before sending it to a cloud service might negatively affect certain functionality in the service. Evaluate the CASB's CSPM capabilities for comparing IaaS workload configurations to common regulatory baselines.

Business Impact: CASBs are uniquely positioned to enable organizations to achieve consistent security policies and governance across many cloud services. Unlike traditional security products, CASBs are designed to protect data that's stored in someone else's systems. CASBs are suitable for organizations of all sizes in all industries and are uniquely positioned to help demonstrate that cloud use is well-governed. Given the expected continued feature expansion and relative ease of switching, favor one-year contract terms over lengthier ones.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Bitglass; Censornet; CipherCloud; Forcepoint; McAfee; Microsoft; Netskope; Proofpoint; Symantec; Zscaler

Recommended Reading:

"Magic Quadrant for Cloud Access Security Brokers"

"Critical Capabilities for Cloud Access Security Brokers"

"Peer Lessons Learned: Implementing Cloud Access Security Brokers"

"How to Secure Cloud Applications Using Cloud Access Security Brokers"

"Best Practices for Planning, Selecting, Deploying and Operating a CASB"

Enterprise Legal Management

Analysis By: Jim Murphy

Definition: Enterprise legal management (ELM) denotes products sold to in-house legal departments as single solutions, suites or bundles that support legal operations and workflows. Such products include legal e-billing, matter management, contract life cycle management, intellectual property management, e-discovery, legal entity management and risk management. ELM platforms provide common services for document repositories, search and reporting, stakeholder collaboration, workflow, automation, and analytics.

Position and Adoption Speed Justification: Several factors are driving steady ELM adoption:

- The COVID-19 crisis has put a spotlight on the need for a comprehensive ELM strategy. It has also altered ELM's emphasis, from general efficiency and speed to compliance and cost optimization.
- Ongoing digital business initiatives must still support business ventures into new arenas with new ecosystems, while addressing mounting regulatory complexity.
- Most enterprises seek to optimize costs by in-sourcing certain legal work, while applying more rigor to managing spend with outside law firms and alternative legal service providers.
- AI, analytics and automation advancements inspire new opportunities to improving legal workflows.

ELM is a multifaceted market. Although several vendors are attempting to consolidate many applications into unified platforms and suites, the components of ELM are often variable and nuanced. In-house legal departments are adopting ELM widely, but that doesn't mean they're always taking single-vendor, single-product approaches. Rather, most are treating ELM as a framework to help coordinate and prioritize legal- and compliance-related technology investments over a multiyear time frame.

User Advice: We advise:

- Resist the temptation to shop for ELM products without appropriate planning. Application leaders responsible for corporate legal and compliance technology should work with general counsel and chief compliance officers to identify desired business outcomes. Then they should designate use cases and critical legal workflows in need of improvement. Most legal departments focus on overcoming capacity constraints, optimizing costs, managing risks and demonstrating impact to the business through data and analytics.
- Specifically, application leaders should examine workflows for legal request/matter intake, legal services sourcing, document management, legal billing, contract creation and review, and collaboration with external parties such as external counsel.
- Require all external providers (e.g., law firms, cloud vendors and legal service providers) that are part of the legal services value chain to adhere to a set of data and privacy protection standards in information sharing, communication and collaboration.

Business Impact: Legal departments can lower costs, increase efficiency and manage risk by adopting an ELM strategy. Gartner research reveals ample room for improvement in legal workflows through automation. Correctly targeted automation often pays off. AI, advanced process management and analytics all bring innovation that promises additional benefit.

However, Gartner's research also reveals a less-than-stellar success rate with some packaged ELM applications. Therefore, organizations must ensure alignment with business goals and pursue the optimal buy, assemble or build approach to garner the ultimate benefits of ELM.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: doeLEGAL; iManage; Legal Suite; LexisNexis; Mitratech; Onit; Thomson Reuters; Wolters Kluwer

Recommended Reading:

"Market Guide for Enterprise Legal Management Solutions"

"Market Guide for Corporate Legal Matter Management"

"Market Guide for Corporate Legal E-Billing"

"Cool Vendors in Legal and Compliance Automation"

Cybersecurity Maturity Assessments

Analysis By: Claude Mandy; Sam Olyaei

Definition: A cybersecurity maturity assessment is the evaluation of an organization's cybersecurity functions and their underlying people, processes and technologies against a defined maturity model with distinct levels of maturity. The maturity levels are determined based on guidance from industry standards and frameworks and are loosely based on variations of maturity levels defined by the Capability Maturity Model Integration (CMMI). Maturity assessments are used to guide priorities and highlight areas where improvement may be required.

Position and Adoption Speed Justification: Cybersecurity maturity assessments have been adopted by SRM leaders as an essential part of strategic planning and demonstrating improvements in cybersecurity. This adoption is "early mainstream," with a market penetration of close to 50%. A significant number of assessments labelled as maturity assessments only measure the implementation of controls and technology. This includes the usage of "maturity" assessments based on NIST Cybersecurity Framework (CSF) implementation tiers, which explicitly states that the implementation tiers do not necessarily represent maturity. Higher adoption should be achievable over the next two years as the value of maturity models that assess people, process and technology capabilities is recognized by more SRM leaders.

User Advice: SRM leaders involved in strategic planning should use cybersecurity maturity assessments to evaluate their organization's cybersecurity functions on a regular basis to guide priorities and inform strategic plans aimed desired levels of cybersecurity capability. Cybersecurity maturity assessments should not be used in isolation nor misrepresented to senior management to avoid creating a false sense of security based on a maturity score and losing credibility as a result of an incident.

Maturity does not necessarily translate directly into reduction of specific risks or increased value to the organization. In addition, the value of maturity assessments to improving the security program will diminish as organizations achieve higher maturity. Cybersecurity maturity assessments should always be considered in in conjunction with the external threat environment, business objectives, risk appetite and risk profile of the organization to avoid misconceptions about effective

management of risk versus maturity of the function. SRM leaders can maximize the insight offered by maturity assessment by being selective in choosing a maturity model to base the assessment on; and validating with an outcome-driven assurance program. Gartner recommends maturity models that evaluate the broader organizational maturity including people and processes and not only evaluate implementation of controls.

Business Impact: Cybersecurity maturity assessments can help organizations form an understanding of how well the security organization is performing in its current state and guide priorities and investments to achieve desired levels of cybersecurity capability. Increased cybersecurity maturity will not only reduce risk from immature cybersecurity capabilities, but also continue to transform the overall security function to ensure optimum use of investments.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Accenture; EY; KPMG; NTT Security; PwC

Recommended Reading:

"IT Score for Security & Risk Management"

"Frequently Asked Questions on the IT Score for Security and Risk Management"

Emergency/Mass Notification Services

Analysis By: Roberta Witty; Mike Gotta

Definition: EMNS automate the distribution and management of messages to relevant stakeholders for localized events and regional and catastrophic disasters across multiple channels. Use cases include organizational crises, business-critical operations, IT outages, and public and personal safety. EMNS is used when operational communications solutions are not available or suitable for use (for example, during a cyberattack), when the need to communicate is in minutes, and for off-hours communications.

Position and Adoption Speed Justification: Crisis communications best practice is to notify people in as many ways and in as short a time frame as possible. Therefore, EMNS support multiple channels: SMS, voice, email, desktop, digital signage, public alerting systems, social media, operational communications solutions, RSS feeds, big speakers, internal collaboration solutions, personal communications tools, etc. Most EMNS customers use the services for the full crisis life cycle: potential crisis identification, crisis declaration, crisis response and recovery actions, and crisis stand-down.

EMNS innovation includes expanded support for mobile device apps (high administrator adoption; low end-user adoption), situational awareness, group-based crisis communications (e.g., by

location, role, department, project or skills), personal safety, IT services alerting and IoT device integration for alert triggering.

COVID-19 has expanded the use of EMNS in two ways:

- Notifying workers who do not have or don't want to have a corporate identifier — the employee provides the preferred method of contact
- Two-way communications for surveying employees about their health and sentiment for returning to the workplace

EMNS vendors are being challenged by crisis/emergency management (C/EM) vendors leveraging communications platform as a service (CPaaS) offerings to build their own EMNS or to expand their existing EMNS capabilities. (Gartner has yet to see CPaaS vendors entering the EMNS market.) As a result, some EMNS vendors are expanding into the broader C/EM solutions market.

The other challenger is the employee communications applications (ECA) market, which provides an enhanced employee communications experience acting as a portal for all types of communications, including news, organizational notices and collaboration. ECA solutions do not support all the channels that EMNS solutions support.

COVID-19 has made clear that organizations want a single solution for all employee communications — both crisis and operational in nature. Not all organizations use EMNS or ECA, or both. A COVID-19 example is using EMNS to announce an outbreak at a location, and then using ECA for in-depth health and safety communication as well as return-to-the-workplace guidance — all part of the broader response. Gartner will watch the EMNS and ECA markets, as well as other markets, such as workstream collaboration (WSC), to identify overlaps in capabilities and cooperative opportunities.

The 2020 position remains at the 2019 position, beyond the Trough of Disillusionment but still ahead of the Plateau of Productivity. Based on the Gartner 2019 Security and Risk Management Survey, over 60% of participants are using EMNS. We expect EMNS adoption to grow based on the post-COVID-19 effect. End-user awareness and maturity have increased, and more customers are now testing the full functionality of EMNS in use cases such as building access management integration, IT network location and personal safety, potentially pushing the platforms to their limits.

User Advice: Document all notification use cases by location, department, role and contact groups to select the right solution for your needs and make the best use of your investment.

Expand EMNS channels to broaden your crisis communications reach within the organization. Pricing beyond the core of voice, SMS and email channels is usually extra.

Survey your workforce to determine peoples' level of comfort in using a corporate-issued mobile device app on their personal device. Not every worker will; therefore the benefit of using functionality only available through the mobile device app may not be realized.

Choose an EMNS vendor that has:

- Hosting data centers in the geographic regions in which you operate. This will ensure two things: compliance with privacy protection regulations applicable to your organization (for example, keep personal contact information within the EU), and that the same crisis doesn't affect both you and the EMNS vendor.
- Customer support services located in the same or adjacent time zones as your organization, as well as language support for your operating locations.
- Create templates that cover the timeline of the crisis, from identification to stand-down, for your defined use cases.

Business Impact: Stakeholder communication is critical during crises, ranging from localized to global disasters. The business benefits of using an EMNS are:

- Preserving and enhancing organizational reputation during a crisis.
- Key personnel and large numbers of affected personnel receive critical information about the crisis in minutes.
- Human error, misinformation, rumors, emotions and distractions — all common during a crisis — can be better managed and corrected.
- Management can focus on critical decision making and exception handling.
- A documented notification audit log can be provided for real-time and postevent management.
- SaaS EMNS is best when you have a crisis because your own data center may be affected and therefore, not available, slowing your crisis response due to delays in reaching your recovery teams and staff.
- During a cyberattack, you don't want the attackers to know you are aware of their presence, so communicating via offline channels is an important crisis management tactic.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Agility Recovery; AlertMedia; Aurea; BlackBerry; Everbridge; Kinetic Global; OnSolve; Rave Mobile Safety; Singlewire Software; xMatters

Recommended Reading:

"Market Guide for Emergency/Mass Notification Services"

"Market Guide for Crisis/Emergency Management Platforms"

"Magic Quadrant for Business Continuity Management Program Solutions, Worldwide"

"Critical Capabilities for Business Continuity Management Program Solutions, Worldwide"

"Market Guide for Employee Communications Applications"

Ethics and Compliance Management

Analysis By: Elizabeth Kim

Definition: Ethics and compliance management technology supports compliance leaders' roles in managing compliance and ethics risks and improving employee decision making. Ethics and compliance management technology include policy management, ethics and compliance training, hotline and investigative case management, conflicts of interest, gifts and hospitality management, compliance risk assessment, and third-party risk management.

Position and Adoption Speed Justification: The ethics and compliance innovation profile was previously known as Corporate Compliance and Oversight (CCO). The reason behind the change to ethics and compliance management was:

- The broad definition and scope of CCO
- The evolving coverage of IRM (see "Technology Outlook for Integrated Risk Management")

Adoption of broadly defined CCO solutions has proved to be slow and unrealistic for some organizations. Many have found it difficult to align and rationalize their different compliance functions, their varying working methods, and solutions they use to meet isolated needs. Efforts to comply with the Sarbanes-Oxley Act (SOX) and similar financial reporting rules, or to support anti-fraud or anti-bribery, or to support security frameworks often warrant separate solutions.

Meanwhile, ethics and compliance management technologies are established with relatively high-end user adoption, which makes it one of the most mature in the risk management solution marketplace. Buyers of ethics and compliance management solutions often start off with a narrow scope such as policy management or whistleblower capability. As such, the marketplace largely consists of vendors offering a comprehensive ethics and compliance management solution suite and vendors offering more narrowly focused application of ethics and compliance.

User Advice: Compliance leaders should establish a clear understanding of their compliance requirements and evaluate vendors that support the corresponding scope of compliance management. For example, ethics compliance vendors can confuse buying decisions by marketing themselves as risk management solution vendors; however, most cannot effectively support the workflow, analysis and reporting needed for other compliance requirements such as SOX compliance or IT/security compliance.

For users that have implemented IRM solutions, some ethics and compliance management capabilities such as policy management, compliance risk assessment and third-party risk management could be supported from the platform. Regulatory compliance (which includes regulatory change management, regulatory intelligence, and the ability to map regulations to controls, risks and policies) is often a core capability of IRM.

Business Impact: While there is increased level of focus on regulations and the business impact on all levels of organizations, most enterprises business impact overall will be mainly on enabling efficiency and reduced cost of compliance through automation.

The COVID-19 pandemic highlights the opportunity to leverage ethics and compliance management technology. This applies to areas such as policy and procedure management for policy updates made to accommodate the rapid development of COVID-19 and investigative case management to support intake and investigation of workplace misconduct. This relates to xenophobic comments and actions fueled by the spread of COVID-19, or concerns around a sick employee entering the office or facility.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ComplyALIGN; Convercent; ConvergePoint; ETHIX360; FixNix; GAN Integrity; i-Sight; Mitratech; NAVEX Global; SAI Global

Recommended Reading:

“Market Guide for Corporate Compliance and Oversight Solutions”

“Technology Outlook for Integrated Risk Management”

“Managing Regulatory Changes for COVID-19 and Beyond”

Entering the Plateau

Qualitative Risk Matrices

Analysis By: Jie Zhang; Sam Olyaei

Definition: Qualitative risk matrices are a form of tabular output from a qualitative risk analysis exercise. This exercise is usually designed to prioritize relevant risks using a predefined rating scale. Typically, the matrices are represented with two axes — the likelihood of a particular risk being realized in the future and its impact on business objectives.

Position and Adoption Speed Justification: Qualitative risk matrices have been used in risk analysis and decision making for more than a decade. They are a simple but crude way to depict and communicate risks to business stakeholders and leaders. These metrics often appear in numeric ratings (i.e., on the scale of 1 to 5 or 1 to 10) or qualitative measures (i.e., extreme, high, moderate and low). The two dimensions for “calculating” these ratings or measures are the likelihood of a risk realization — ranking from certain, likely, possible, unlikely to rare — against its impact on business objectives — ranging from negligible, marginal, critical and catastrophic. They are easy-to-use and easy-to-understand tools for conveying a complex risk analysis narrative.

Therefore, qualitative risk matrices are widely used by organizations. But, the value of these matrices is limited and can be manipulated because the input values are based on subjective human estimates. Many variances can influence these estimates, such as an expert's inherent outlook on reality as well as the level of experience and understanding of risks by the expert.

Organizations with some level of formal risk assessment and analysis are increasingly using, or preferring to use, qualitative matrices for communicating risks. Due to their simplicity, qualitative risk matrices will likely continue to widespread and mainstream adoptions.

User Advice: Recognize the limitations of qualitative risk matrices. Hence, explore quantitative risk analysis methods in conjunction with qualitative risk matrices. The combination of both methods can improve risk communication and decision making by revealing additional nuances and by offsetting human biases.

If qualitative risk matrices have become the main means to inform decision makers on risk exposure, ensure a good understanding how matrices are typically created and the major input providers' responsibilities and backgrounds.

Ensure that any qualitative discussion is happening within the context of a broader risk appetite level or statement for maximum value.

Business Impact: Risk analysis is a complex undertaking as it often requires input across multiple functional areas and systems. It is also challenging to interpret various inputs and present the results in a timely and meaningful way. A simple communication tool like qualitative matrices for describing the risk landscape and its potential future impact on business goals is powerful. It can simplify a complex narrative in a consistent and comparable style. Furthermore, the investment for creating qualitative matrices is straightforward and much lower than quantitative analysis. Due to their simplicity and low investment, the returned value is justifiably significant. This is why qualitative risk matrices have been widely adopted.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Recommended Reading:

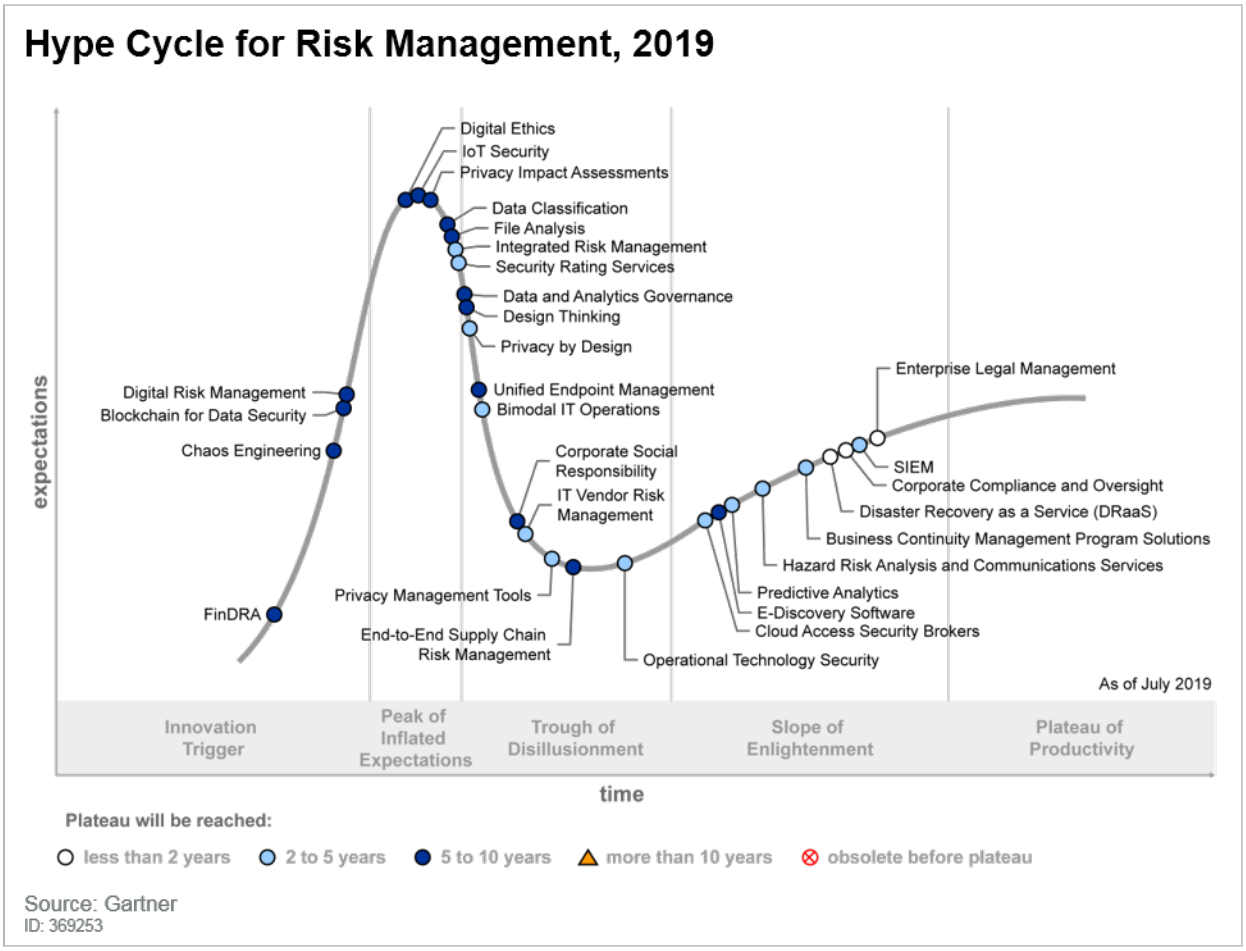
"Action-Oriented Risk Matrix (Power Co.)"

"Risk Responsibility Matrix (Pepco)"

"Toolkit: A Practical Risk Heat Map That Drives Change and Growth"

Appendixes

Figure 3. Hype Cycle for Risk Management, 2019



Source: Gartner
ID: 369253

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough public demonstration, product launch or other event generates significant press and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.
Trough of Disillusionment	Because the technology does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the technology's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the technology to reach the Plateau of Productivity.

Source: Gartner (July 2020)

Table 2. Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2020)

Table 3. Maturity Levels

Maturity Level	Status	Products/Vendors
Embryonic	▪ In labs	▪ None
Emerging	▪ Commercialization by vendors ▪ Pilots and deployments by industry leaders	▪ First generation ▪ High price ▪ Much customization
Adolescent	▪ Maturing technology capabilities and process understanding ▪ Uptake beyond early adopters	▪ Second generation ▪ Less customization
Early mainstream	▪ Proven technology ▪ Vendors, technology and adoption rapidly evolving	▪ Third generation ▪ More out-of-the-box methodologies
Mature mainstream	▪ Robust technology ▪ Not much evolution in vendors or technology	▪ Several dominant vendors
Legacy	▪ Not appropriate for new developments ▪ Cost of migration constrains replacement	▪ Maintenance revenue focus
Obsolete	▪ Rarely used	▪ Used/resale market only

Source: Gartner (July 2020)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

2020 Gartner CEO Survey: The Year of Recession

6 Principles for Digital Business Risk Assessment

How to Engage Your Board of Directors on IRM

2020 Strategic Roadmap for Business Continuity Management

Market Guide for Emergency/Mass Notification Services

Competitive Landscape: Integrated Risk Management

Magic Quadrant for IT Vendor Risk Management Tools

Magic Quadrant for IT Risk Management

Recommended COVID-19 Strategies and Resources for Risk Management Leaders

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp