SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

BUILDING BEST PRACTICES
BRIEFING PAPER

ROLE OF ERM IN MANAGING RISKS RELATED TO NEW TECHNOLOGIES

TABLE OF CONTENTS

SFG | SHARED ASSESSMENTS

BUILDING BEST PRACTICES BRIEFING PAPER

BUILDING BEST PRACTICES:

Role of ERM in Managing Risks Related to New Technologies

Introduction

The organization's C-suite and board have critical roles to play in order to effectively manage risks associated with new technologies. The following key steps have been identified as helping to establish effective risk monitoring programs that are responsive to potential risks related to new technologies:

- Ensure that board members and appropriate C-suite executives have appropriate knowledge of emerging technology risks and the potential impact of those risks to the organization.
- Establish a board risk committee or group that oversees all risk management activities enterprise-wide and advises the larger board around risk-related decisions. Designate a Chief Risk Officer (CRO) as the primary liaison to inform the risk committee and oversee risk-related issues enterprise-wide.
- Evolve enterprise risk management (ERM) structures in order to better anticipate and prepare for significant technology shifts.
- Develop a strategy to remain aware of and manage emerging challenges as they arise and make sure that the appropriate organizational stakeholders, including the board and risk committee, are aware of technology-related opportunities and potential risks.
- Ensure that risk management teams have an ongoing process that is aligned with the organization's strategy, to better anticipate and mitigate significant emerging technology risks.
- Seek qualified, external assistance to analyze and monitor technology-related opportunities and risks, as needed. Such assistance is especially relevant to smaller organizations that may not have the bandwidth to muster robust emerging technology expertise in-house.
- Ensure that both Outsourcers' and their Third Parties are equipping their ERM structures to anticipate, understand and mitigate technology-related risks stemming and become familiar with the ERM approaches being used.

Issue Landscape

Significant technology advances can fuel heightened productivity, important new product development and an overall enhanced ability to meet business objectives. Yet, along with these important benefits, technology often introduces new risks. An incomplete understanding of those risks, particularly when related to cybersecurity, can lead to material consequences.

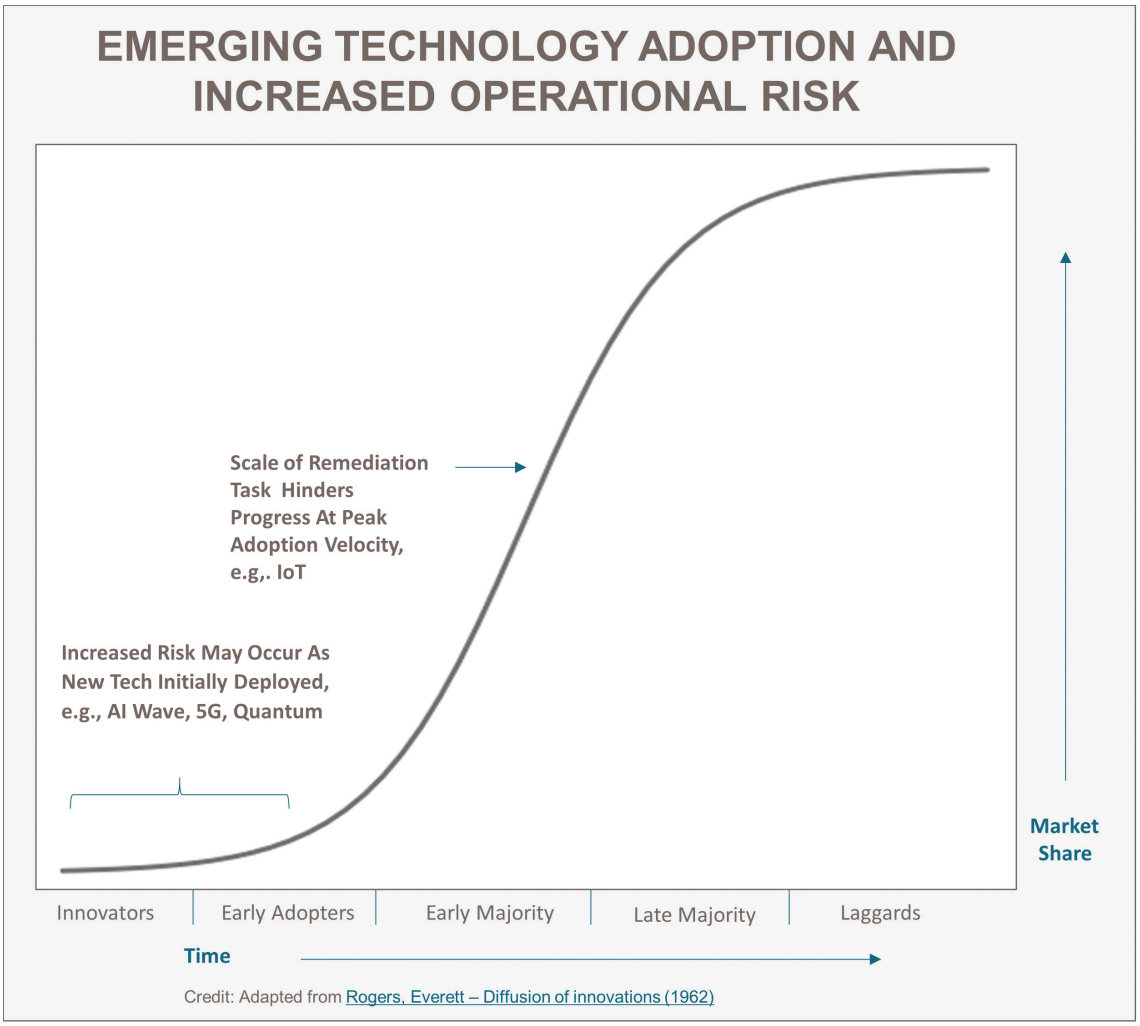

Figure 1: Emerging Technology Adoption and Increased Operational Risk

The board and C-suite can play a valuable role in helping organizations recognize and respond to the fact that they may lack the technology resources to address important risks.

Although Enterprise Risk Management (ERM) structures have grown in number and maturity to better manage and provide a holistic view of risk across organizations, these structures typically lack a systemic means of anticipating and preparing for the challenges that come with significant technology shifts such as Artificial Intelligence (AI), 5G and quantum computing.

Risks and Rewards of Emerging Technology

Emerging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), 5G and Quantum Computing and Encryption have the potential to increase organization efficiency, improve interactions with customers and improve risk management capabilities in the near future. However, a steep learning curve typically accompanies successful adoption of new technology, and organizations need to balance the use of new technology with their ability to mitigate associated risks.

Even technology specifically designed to more quickly detect risks can prove difficult to implement when organizations do not have the right resources or understand nuances of applying the technology in

their unique setting. For example, organizations implementing cybersecurity continuous monitoring and other emerging technologies face common challenges:

- Continuous monitoring technology has the potential to generate an enormous amount of data, often too much information for Outsourcers to manage effectively.
- Outsourcers do not necessarily understand how to optimize continuous monitoring technology to their advantage to obtain relevant and actionable metrics.
- Outsourcers may need to augment staff to better interpret continuous monitoring information and other emerging technologies.

Technology Dependencies

New technologies interact together, creating interdependencies, which while increasing the potential for the development of new products, can potentially magnify risks. For example, 5G has the potential to greatly increase IoT device use. A wider use of IoT devices will enable a new range of services; however, it will also bring increased risk from additional threats including the relative lack of security associated with IoT devices.

Organizations must learn how to anticipate the combined impact of new technologies, rather than assess each technology on a stand-alone basis. In short, there is potential for there to be a lag in the security technology industry when the 5G rollout occurs. Outsourcers will expect their third party providers to be able to adapt quickly and respond to new technology challenges and will hold third parties accountable for inept use of new technologies.

Challenges Related to Technology

This paper explores four emerging technologies (IoT, AI, 5G and quantum computing), highlighting potential risks and opportunities, risk management solutions and key actions that the board and C-suite should take to manage new technology risks.

The Internet of Things (IoT)

IoT is the network of physical objects or "things" embedded with electronics, software, sensors and network connectivity, which enables these objects to collect, monitor and exchange data. The scope of IoT devices is very broad and refers to the connection of devices other than computers (e.g., cars, kitchen appliances, phones). IoT devices in the workplace include network-connected printers and building automation solutions, specialized hospital equipment in the healthcare sector, machines and supplies that have added IoT devices to generate performance data.

IoT devices are attractive to organizations because they provide opportunities to be more efficient, saving time and money. IoT may provide computing functionality, data storage and network connectivity to devices that previously did not have these capabilities, which enables new functionality, such as remote access for monitoring, the ability to better analyze data and better anticipate future events, etc.

IDC estimates that there will be 41.6 billion IoT devices in the field by 2025. These devices and associated data will grow at a compound annual growth rate of more than 28% and generate 79.4 Zettabytes (ZB) of data in 2025. Additionally, companies and consumers will spend nearly $15 trillion on IoT devices, solutions and supporting systems from 2018-2026.[i]

As IoT use continues to grow at a rapid pace and devices become more connected, security and privacy have become an increasing concern. Cyberattacks on IoT devices increased by more than 300% in the first half of 2019.[ii] The U.S. Government Accountability Office has identified the following attacks as primary threats to IoT.[iii]

- **Distributed denial of service attack:** An attack that uses numerous hosts to impair a website/computer by flooding or crashing it with too much traffic. One notable attack garnered national attention in October 2016 by causing a number of major websites to be unavailable.[iv]
- **Malware or malicious code/software:** A program that is inserted into a system with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system. Examples include logic bombs, Trojan Horses, ransomware, viruses and worms.
- **Passive wiretapping:** The monitoring or recording of data, such as passwords, while they are being sent over a communications link.
- **Structured query language injection (SQLI):** The alteration of a database search in a web-based application that can be used to obtain unauthorized access to sensitive information.

- **War driving:** A method of driving through areas with a wireless-equipped computer that searches for unsecured wireless networks.
- **Zero day exploit:** An exploit that takes targets a previously unknown security vulnerability.

Despite all the potential risks that are relevant to IoT, the pace of developing effective IoT risk management strategies has been slow. More than 80% of survey respondents report that the pace of innovation in IoT and varying standards for security makes it hard to catalog and ensure the security of these devices and applications.[v] This results from the serious concerns that all parties face – IoT developers/manufacturers, organizations, third parties and individuals – perceived unmanageable IoT security concerns.

For example:

1) IoT manufacturers have routinely produced devices with easy passwords or other internal vulnerabilities. Although many experts in the field have urged regulatory guidance to hold IoT device manufacturers accountable for vulnerable devices, only recently has there been progress.[vi]
2) Most organizations have been slow to implement an IoT risk management plan.

IoT risks are well-documented and frameworks for managing those risks have emerged in recent years. Yet, research has repeatedly demonstrated that IoT risk management is nascent is most organizations. For example, fewer than 20 % of organizations can even identify the majority of IoT devices connected to their own networks, and are therefore without the complete inventory so essential to robust IoT risk management.

Ongoing Shared Assessments research suggests that:

- 50 percent of organizations do not believe it is possible maintain an inventory of IoT devices.
- 90 percent of those who say it is not possible to maintain an inventory cite the fact that there is no centralized control over IoT devices and associated IoT applications used in the workplace as a primary cause.
- Less than 40 percent of firms have any type of formal approval process before IoT devices are attached to internal networks.
- 70 percent or organizations do not use commercially available tools to collect inventory and monitor the risk of IoT devices used in the workplace.
- Only 45% of organizations conduct any type of an audit of their vendor's IoT security and privacy practices.

IoT risk management solutions: A strong case can be made that lack of focus at the board and C-levels is in part responsible for the slow pace of IoT risk management progress. Governing boards and C-suites should play leading roles in ensuring that IoT risks are addressed both internally and at Third Parties. Governing boards and executive management should make it a priority to ensure that:

- There is clear responsibility for overseeing IoT security both internally and with Third Parties and that key characteristics of the IoT governance framework are widely socialized.
- A record of all IoT devices is maintained in an inventory along with salient characterizes of those devices.
- IoT devices are segregated on their own networks and monitored 24/7 to prevent unauthorized access.
- Known vulnerabilities related to IoT devices are identified and mitigated promptly.

Artificial Intelligence

Artificial Intelligence (AI) is the ability of machines to behave in a way we would consider "smart;" the capability of a machine to imitate intelligent human behavior. AI is the ability to be abstract, creative, deductive — to learn and adapt learnings to new situations. For example, in healthcare, in the future an artificial virtual assistant might hold conversations with patients and provide lab results. AI applies machine learning to solve problems and achieve goals. Machine learning is a subset of AI that enables machines to learn for themselves using the data provided to make predictions.

AI has the potential to revolutionize today's society as a whole. According AI expert Dr. Kai-Fu Lee, the complete AI revolution will take time, however, and will unfold in a series of four waves – Internet AI, Business AI, Perception AI, and Autonomous AI:[vii]

- **Wave 1 – Internet AI:** This wave of AI is largely about using AI algorithms as recommendation engines: systems that learn our personal preferences and then serve up content that is specific to the user. It helps internet companies grab our attention by advertising items of personal preference to buy or suggesting which video the user should watch next.
- **Wave 2 – Business AI:** This form of AI uses company data to develop algorithms that uncover hidden correlations and predict meaningful outcomes, outperforming the most experienced human analysts. Examples of business AI are for gaining insights for trading stocks, diagnosing illnesses and predicting mortgage defaults.
- **Wave 3 – Perception AI:** This wave of AI is learning to recognize faces, understand user requests, and "see" the world. It uses algorithms to group the pixels from a photo or video into clusters and recognize objects, similar to the way the human brain does. This is also applicable to audio data; algorithms can both pick out words and often decipher full sentences. Perception AI will modernize how we interact with the world, using sensors and smart devices to turn the physical world into digital data that can then be analyzed by deep-learning algorithms. Applications using this type of AI include Amazon Echo digitizing the audio environment of peoples' homes, or Apple's iPhone X camera utilizing face digitization to safeguard the phone.
- **Wave 4 – Autonomous AI:** This wave of AI builds off of the three preceding waves, incorporating machine ability to optimize from complex data sets with newfound sensory powers gained from these processes. This form of AI will result in self-driving cars, autonomous drones and intelligent robots and will have the greatest impact on people's lives, with visible impacts ranging across experiences in malls, restaurants, cities, factories and fire departments. Autonomous AI will also occur over time, starting in highly structured environments where it can create immediate economic value (e.g., factories, warehouses and farms).

AI has the potential to revolutionize ERM practices. One example is the challenge in cyber risk management to continuously monitor large blocks of data in order to mitigate risks that rapidly evolve. The potential exists to improve risk management by providing more advanced tools and monitoring systems that use AI. For example, machine learning techniques continue to be deployed in network intrusion detection and prevention, malware detection and secure user authentication.[viii] Countries are also using AI cybersecurity tools.

Thailand is using AI to monitor network traffic and conduct big data analyses to detect suspicious user behavior.[ix] China has positioned itself as a leader in AI development. China's State Council's Artificial Intelligence Development Plan (AIDP) sheds light on China's AI views: "AI has become a new focus of international competition. AI is a strategic technology that will lead in the future; the world's major developed countries are taking the development of AI as a major strategy to enhance national competitiveness and protect national security."[x] China has used AI to fight terrorists, reportedly intercepting 1,200 reportedly terrorist organizations when still planning an attack. It has a facial recognition

system; and for those that the state has identified as terrorists, there is a database.[xi] As recent news reports have made clear, AI has the ability to raise significant privacy and civil liberties concerns.[xii]

China has also addressed AI use within military operations. Zeng Yi, a senior executive at China's third largest defense company, predicted that by 2025 lethal autonomous weapons would be commonplace and said that his company believes ever-increasing military use of AI is inevitable.

Unfortunately, the growth of AI increases the potential for cyberattacks. The same AI techniques (e.g., machine learning, deep learning and neural networks) that enable computers to find and interpret patterns can also be exploited in ways that effect business resilience. Intelligent malware and ransomware that learns as it spreads, machine intelligence coordinating global cyberattacks, advanced data analytics to customize attacks—will soon have the ability to hinder organizations.[xiii] Some risk management professionals predict that AI attacks will be autonomous and self-propagating, learning the organization's network environment rather than relying on known or common vulnerabilities.[xiv]

Ethical considerations: Since AI includes machine learning to perform tasks that require human intelligence, organizations should also make sure their use of AI is ethical. One example of an ethical setback is that Amazon's internal AI test recruiting program was found to be biased against women.[xv] In this case, computer models were trained by exposing the model to resumes submitted to Amazon over the previous ten years that resulted from hirings, and most of these résumés came from men. The computer models "learned" that men were superior job candidates and became biased against women. Organizations need to recognize that potential biases may occur as they implement AI, and should monitor for these biases and respond accordingly.

Strikingly, a recent Deloitte poll indicates that nearly half (48.5%) of C-suite and other executives at organizations that use AI expect to increase AI use for risk management and compliance efforts in the year ahead. Yet only 21.1% of respondents report that their organizations have an ethical framework in place for AI use within risk management and compliance programs. The report continues that "to better scale AI governance over time and to better reduce algorithm bias, leading organizations are approaching AI ethics proactively by embedding ethical frameworks into all AI efforts as a matter of practice."[xvi]

Diversity in the technology workforce is beneficial to the organization, as women and underrepresented minorities can add new insight (different perspectives to add to programming) and make organizations more profitable.[xvii] Finally, ethical issues are also raised by employee anxiety around potential job loss due to AI. According to a 2018 Workforce Institute survey of 3,000 workers across eight industrialized nations, three out of every five organizations globally (58%) have yet to discuss the potential impact of AI on their workforce with employees, and U.S. companies are the most secretive: 67% of U.S. workers surveyed say they have no knowledge whatsoever about their organization's plans for AI.[xviii]

AI risk management solutions: AI is a relatively new field and its role within the risk management processes are not yet well defined. The board and C-suite should realize that the organization's employees may need to learn how to use AI tools. AI requires collaboration between people and machines and some organizations may need to upskill employees or hire data scientists to ensure that AI users are able to interpret AI results correctly.

Effective development of AI requires multidisciplinary teams, including ERM, to come together to solve a problem during development and implementation. The board and appropriate C-suite executives should ensure that their organizations determine how they can use their current ERM process to help identify and manage AI risks.

ERM processes will likely need to be updated to take into account AI technologies used by the organization. Organizational risk appetite frameworks will have to be updated to include potentials risks around AI, including a review policies and management structures to support effective management and risk monitoring.

The board and C-suite should formalize a risk management process around their use of AI, including:

1. Identify risks associated with the adoption of AI.

2. Establish a risk assessment process to take into account AI risk, recognizing that existing risk appetite and assessment frameworks may not sufficiently address AI risks.
3. Develop a process to manage and monitor AI risk, which may require frequent testing and monitoring of the AI technology that the organization uses.
4. Determine and implement a method to measure effectiveness of the AI risk monitoring process and report findings.

AI technology will help risk managers on the ground to make more informed, faster decisions. AI can improve risk management by:

- **Fostering collaboration between product developers and risk managers:** Collaboration is especially useful when firms are just beginning to consider and incorporate use of AI.
- **Allowing for better data management:** Machine learning models can analyze large amounts of data - both structured and unstructured.
- **Improving analytical capabilities in risk management:** AI applications can analyze data to identify patterns and make decisions based on them. Additionally, AI applications are programmed to learn from the data received to refine the way decisions are made over time.
- **Providing greater risk visibility and predictive insight:** Using historical data, AI tools can bring into sharper focus the potential consequences of business related incidents.
- **Improving efficiency:** The learning capabilities of AI can inform streamlining daily risk management processes. One example is financial institutions that use AI to prevent fraud. Fraud prevention systems can examine years and sometimes, decades of transaction data in a 250-millisecond response rate to calculate risk scores using AI. AI also makes it possible to detect fraud attacks in real-time versus having to wait six or eight weeks. Taking this integrative, real-time approach to AI across a digital business yields scores that are 200% more predictive according to internal research completed by Kount, a fraud prevention solutions company.[xix]
- **Providing risk mitigation recommendations:** This includes recommending controls or suggesting actions to mitigate for a specific risk based on similar actions that have been applied to similar risks in the past.
- **Helping to categorize risk:** AI can group incidents by matching the words used in an incident description against incidents that have already been identified in the database.
- **Improving breach identification:** Identifying potential breaches of policies based on data analysis and incident reporting.

5G Effects

5G is the fifth generation of wireless technology that will combine new and existing technology and infrastructure to improve the bandwidth capacity and reliability of wireless broadband services. 5G networks are expected to help meet increasing data and communication requirements, including improved capacity support for IoT devices, facilitate near-real time communications and provide faster speeds to support emerging technologies, particularly AI. 5G is expected to power economies and societies by facilitating connections that will support critical services within healthcare, energy, transport, banking, other critical infrastructure and other verticals. 5G was introduced in the United States in 2018, but widespread usage of a standalone 5G network is not expected until at least 2020.[xx]

The U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency outlines four points of vulnerability in the 5G network:[xxi]

1. **Supply chain:** The supply chain is susceptible to the inadvertent introduction of vulnerabilities such as malicious software and hardware; counterfeit components; and poor designs, manufacturing processes and maintenance procedures. 5G hardware, software and services provided by entities deemed to be untrusted could increase the risk of network asset compromise and affect data confidentiality, integrity and availability.

2. **Deployment:** 5G will use more information and communication technology (ICT) components than previous generations of wireless networks, and organizations may build their own local 5G networks, potentially increasing the attack surface for malicious actors. Therefore, 5G networks will need to be properly configured and implemented for security enhancements related to 5G networks to be effective.
3. **Network security:** 5G will build upon previous generations of wireless networks and will initially be integrated with 4G networks that contain some existing vulnerabilities. 5G networks will also likely generate new vulnerabilities that are not yet known.
4. **Loss of competition and choice:** Although there are standards designed to encourage interoperability, some companies build proprietary interfaces into their technologies. This limits customers' abilities to use other equipment. Organizations that are locked into one technology or service provider may have to choose between continuing to use an untrusted supplier or removing and replacing existing equipment.

The importance of competition and choice is further demonstrated by the case of the Chinese-run telecom company Huawei, which has been blacklisted by the US government because of perceived vulnerabilities in their products. Robert Strayer, deputy assistant secretary for Cyber and International Communications Policy at the State Department's Bureau of Economic and Business Affairs, recently provided statements around this risk: "We are taking a risk-based approach to understanding the implications of the growing global presence of Chinese telecom equipment throughout the 5G technology stack. The potential for Chinese intelligence and security services to use Chinese firms as routine and systemic espionage platforms against the United States and our allies is concerning and a potential direct threat to our mandate to ensure national security and emergency preparedness communications."[xxii]

5G Risk management solutions: The board and C-suite can ensure that their organizations:

- **Limit risk around using new technologies:** Utilize only trusted 5G technologies and limit the adoption of 5G equipment with suspected vulnerabilities.
- **Provide continuous, real-time monitoring with autonomy:** A continuous monitoring approach will be necessary to monitor risk within the 5G network and take deflective/protective action automatically based on pre-defined parameters.
- **Ensure that all IoT devices are approved and certified:** Since 5G will increase capacity for billions of connected IoT devices, it is important to advance the adoption of trusted IoT devices.
- **Set and meet appropriate supply chain standards:** Promote the adoption of 5G hardware, software and services by trusted entities.

Quantum Computing and Encryption

Quantum computing uses quantum mechanics to perform computations. For example, in today's classic computers "bits" are used and these can either be located in the state of zero or one; quantum computers use "qubits" that can exist in multiple states, as opposed to the zero or one that binary can achieve. Quantum computers are significantly more powerful than any of the current computers/supercomputers and, if successfully developed, could lead to breakthroughs in science, life-saving medical advances, and financial modeling strategies; running more complex AI programs; and advancing computations and modeling in chemistry and physics. In short, Quantum computing could dramatically reduce the time needed to solve the mathematical problems on which encryption techniques currently rely—from months to minutes and seconds.[xxiii]

But the successful development of quantum computing could also have a considerable negative impact on cybersecurity. It risks rendering useless most of our existing data security and critical infrastructure systems, including military networks, email and power grids.[xxiv] Our digital security often relies on cryptographic calculations. Quantum computing uses new technology that is able to break cryptosystems and allow access to data that was previously secure.

This is especially worrisome for public-key cryptography, which is used for: (1) Authorization of counter-party in a connection; (2) Developing shared keys; (3) Digital signatures; and (4) Encryption. This makes public key cryptography critical for everything from normal web-browsing to transferring huge sums of money.

Quantum computing and encryption risk solutions: Quantum computers are extremely difficult to build and operate, requiring almost absolute zero (-273˚C). Quantum technology may be commercialized within 5-15 years. Once functional, quantum computing will radically derail contemporary cryptographic protections.

The U.S. National Institute of Standards and Technology (NIST) has launched a program that aims to find algorithms resistant to quantum computing attacks. The goal of NIST's Post-Quantum Cryptography (PQC) work is "to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks." This work is expected to be complete in the 2022-24 timeframe.[xxv]

Some engineers predict that within the next twenty or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. "Post-quantum cryptography is the study of cryptosystems which can be run on a classical computer, but are secure even if an adversary possesses a quantum computer."[xxvi] Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we should begin now to prepare our information security systems to be able to resist quantum computing.[xxvii]

Accordingly, organizations should consider how they are going to transition to post-quantum computing.

Organizations should:

- Educate boards and executive management about the risks quantum computing may pose.
- Stay close to the risk mitigation strategies that are being developed, especially the NIST PQC standardization effort.
- Be prepared to upgrade to PQC encryption techniques.
- Prioritize data that will be moved to post-quantum encryption once standards are available.
- If lacking the right human resources to engage with PQC, recruit appropriate talent or identify outside resources to advise your organization about the development of PQC standards.

Establishing Best Practices for New Technologies

In order to manage emerging technology risks, organizations must establish a systemic, effective process that identifies new technology risks, reports risks to the appropriate organization staff and implements successful strategies to mitigate these risks. The UK Risk Coalition recently published guidance that provides good background around operating an effective board risk committee.[xxviii] The recommended strategies within this guidance provide insight into how to identify and manage emerging risks that the board and C-suite can also apply to new technology risks.

Best practice key takeaways:

- Regularly review cycles of technology evaluation to ensure the frequency is adequate, including whether cycles provide sufficient time for ad hoc or deep-dive exploration of key and emerging risk-related topics and themes.
- Assess and advise the board on the organization's principal emerging risks and the continued viability of its business model.
- Periodically assess the effectiveness of the organization's emerging risk identification and horizon scanning processes. Horizon scanning is a process that organizations use to identify, assess and analyze new or emerging risks and opportunities.
- Seek assurance on the completeness, accuracy and fairness of first line

management's reporting of the organization's principal and emerging risks and their impact on achievement of the organization's strategic objectives. In turn the Chief Risk Officer (CRO) should provide a report to the risk committee on key risk management concerns, including around emerging risks and their potential impacts on achievement of the organization's strategic objectives.

- Ensure that the organization's risk function helps to identify and adapt to developments in the external environment. This includes the development of an enterprise-wide risk identification and horizon scanning process that involves the use of scenario planning techniques and that encourages and incorporates contributions from each of the lines of defense, executive management and the board risk committee.

Conclusions and Recommendations

The board and C-suite must ensure that their organization is positioned to use new technology to its advantage, in a way that both minimizes risk and improves their organizational efficiency. Best practices include:

- Ensuring an effective, systemic process to identify risk management challenges associated with emerging technologies in the planning phase and developing appropriate approaches to meet those challenges.
- Making sure the organization's risk management team has the right talent and skillset to adopt an emerging technology and to manage associated risks. Organizations may need to upskill or hire new employees if there are not people with required skills on staff.
- Recognizing that, even with qualified analysts, there will be differing interpretations of risk data results and bias. Organizations should establish procedures (e.g., designate a model or risk group) that address individualized biases and interpretations.
- Monitoring and assessing the organization's new technology risk management activities (e.g., IoT, 5G, AI) and ensuring that the appropriate groups/individuals are collaboratively working to implement these activities on the ground.
- The organization's ERM structure should be configured to facilitate risk mitigation as new technologies are adopted.

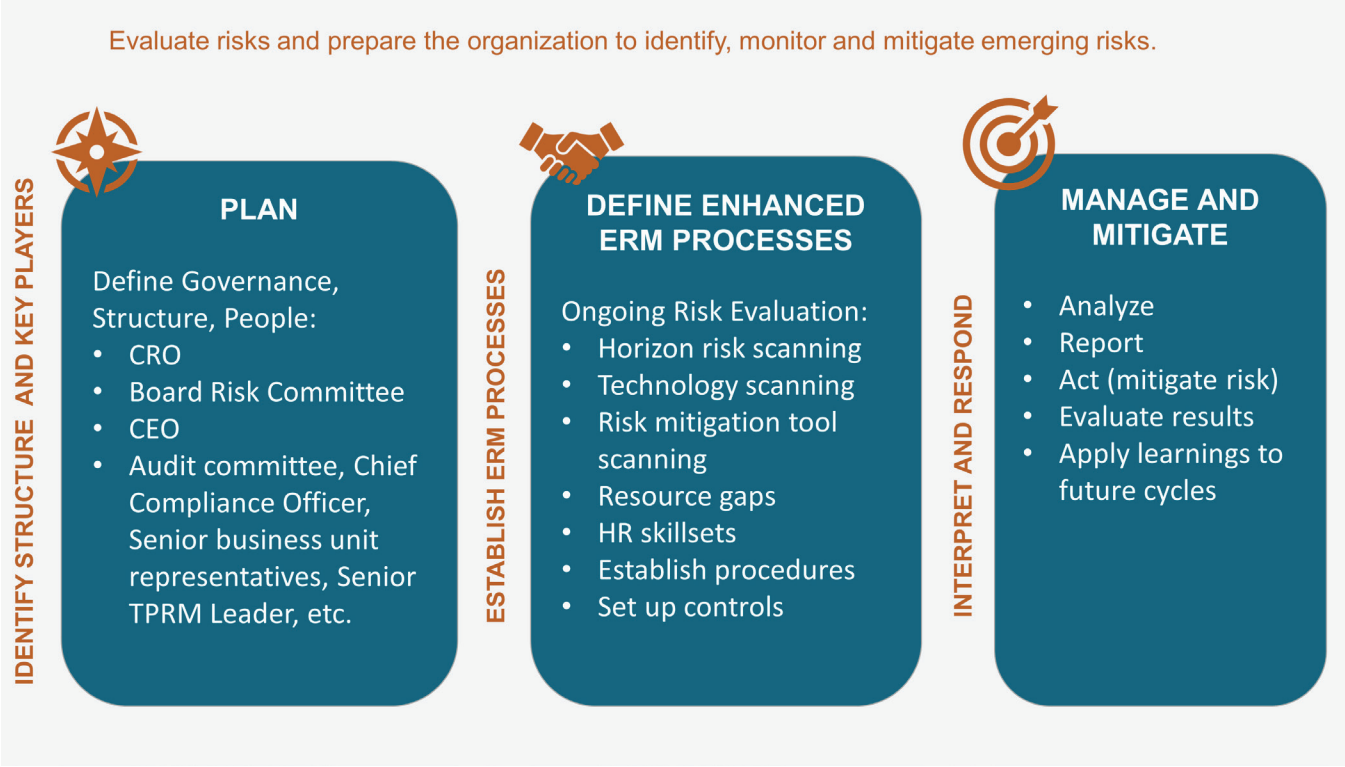

Figure 2: Addressing Emerging Technology Risks with ERM

Acknowledgments

This paper reviews key steps that boards should take to ensure that their organizations are conducting effective risk management programs. We would like to thank the Shared Assessments' Risk Committee volunteer members who conducted this effort:

- **Angela Dogan**, Founder & CEO, Davis Dogan Advisory Services, LLC
- **Mark Holladay**, Executive Vice President and Chief Risk Officer, Synovus Financial Corporation
- **Shawn Malone**, Founder & Chief Executive Officer, Security Diligence, LLC
- **Adam Stone**, Vice President Consulting Services and Chief Privacy Officer, Secure Digital Solutions, Inc.

We would also like to acknowledge The Santa Fe Group, Shared Assessments Program subject matter experts and other staff who supported this project:

- **Catherine A. Allen**, Chairman and Chief Executive Officer
- **Gary Roboff**, Senior Advisor
- **Wendy McCoy**, Technical Writer
- **Charlie Miller**, Senior Advisor
- **Sylvie Obledo**, Senior Project Manager
- **Marya Roddis**, Vice President, Technical Writing
- **Robin Slade**, Executive Vice President & Chief Operating Officer

About the Shared Assessments Program

The Shared Assessments Program has been setting the standard in Third Party Risk Management since 2005. Member-driven development of program resources helps organizations to effectively manage the critical components of the Third Party risk management lifecycle by creating efficiencies and lowering costs for conducting rigorous assessments of controls for cybersecurity, IT, privacy, data security and business resiliency. Program Tools are kept current with regulations, industry standards and guidelines and the current threat environment; and are adopted globally across a broad range of industries both by service providers and their customers. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company based in Santa Fe, New Mexico. For more information on Shared Assessments, please visit https://www.sharedassessments.org.

Join the dialog with peer companies and learn how you can optimize your compliance program. For more information on Shared Assessments, please visit http://www.sharedassessments.org.

Endnotes

i What is the Internet of Things? What IoT means and how it works. Business Insider. May 10, 2018. Accessed at: https://www.businessinsider.com/internet-of-things-definition.

ii Cyberattacks on IoT Devices Surge 300% in 2019, 'Measured in Billions', Report Claims. Forbes. September 14, 2019. Accessed at: https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattackson-iot-devices-up-300-in-2019-now-rampant-report-claims/#45642d105892

iii GAO, Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems (GAO-15-573T). U.S. Government Accountability Office (Washington D.C. April 22, 2015. Accessed at: https://www.gao.gov/products/GAO-15-573T.

iv Major websites affected by the attack include: Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times, among others. Nicole Perlroth. Hackers Used New Weapons to Disrupt Major Websites Across U.S. The New York Times, October 21st, 2016. Accessed at: http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0.

v The Third Annual Study on Third Party IoT Risk: Companies Don't Know What They Don't Know. Ponemon Institute and The Santa Fe Group, Shared Assessments Program. May 3, 2019. Accessed at: https://sharedassessments.org/2019-iotstudy/

vi Connect the Dots: IoT Security Risks in an Increasingly Connected World. SecurityIntelligence. May 11, 2018. Accessed at: https://securityintelligence.com/connect-the-dots-iot-security-risks-in-an-increasingly-connected-world/; California Law SB 327 regulating all IoT devices sold in the state be equipped with security measures effective January 1, 2020; Oregon Bill 2395, May 2019, requires specific safeguards effective January 1, 2020.

vii Lee, K. 2018. The Four Waves of AI - A White Paper Adopted from AI Superpowers China, Silicon Valley, and the New World Order. Accessed at: https://aisuperpowers.com/blog/the-four-waves-of-ai

viii Risk in Focus 2020: Hot topics for internal auditors. European Confederation of Institutes of Internal Auditing. September 2019.

ix How Thailand is using AI for cybersecurity. GovInsider. November 27, 2018. Accessed at: https://govinsider.asia/digital-gov/how-thailand-is-using-ai-for-cybersecurity/.

x Understanding China's AI Strategy. Center for a New American Security. February 6, 2019. Accessed at: https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy

xi General Wang Ning. October 25, 2018. Global Terrorism: Threats and Countermeasures (8th Beijing Xiangshan Forum, Beijing).

xii Diamond, L. and Mitchell, A. China's Surveillance State Should Scare Everyone - The country is perfecting a vast network of digital espionage as a means of social control—with implications for democracies worldwide. February 2, 2018. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/

xiii 2018 AI Predictions. PWC. 2018. Accessed at: https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions.html.

xiv Risk in Focus 2020: Hot topics for internal auditors. European Confederation of Institutes of Internal Auditing. September 2019.

xv Is Artificial Intelligence The Key to Recruiting a Diverse Workforce? Forbes. August 13, 2019. Accessed at: https://www.forbes.com/sites/kimelsesser/2019/08/13/is-artificial-intelligence-the-key-to-recruiting-a-diverse-workforce/#5c292c8f5f8b

xvi AI Use expected to Increase in Risk and Compliance Efforts, But Few Have Ethics Frameworks in Place, news provided by Deloitte. October 28, 2019. CISION PR Newswire. Accessed at: https://www.prnewswire.com/news-releases/ai-use-expected-to-increase-in-risk-and-compliance-efforts-but-few-have-ethics-frameworks-in-place-300945891.html

xvii Tech Experts Share the Importance of Diversity and How to Foster Inclusion. Cornell Tech. October 12, 2017. Accessed at: https://tech.cornell.edu/news/tech-experts-share-the-importance-of-diversity-and-how-to-foster-inclusion/

xviii AI anxiety: An Ethical Challenge for Business. Forbes. March 27, 2019. Accessed at: https://www.forbes.com/sites/insights-intelai/2019/03/27/ai-anxiety-an-ethical-challenge-for-business/#28bc8a057880

xix Top 9 Ways Artificial Intelligence Prevents Fraud. Forbes. July 9, 2019. Accessed at: https://www.forbes.com/sites/louiscolumbus/2019/07/09/top-9-ways-artificial-intelligence-prevents-fraud/#7a91f40814b4

xx Overview of Risks Introduced by 5G Adoption in the United States. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. July 31, 2019. Accessed at: https://www.dhs.gov/cisa/5g.

xxi Overview of Risks Introduced by 5G Adoption in the United States. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. July 31, 2019. Accessed at: https://www.dhs.gov/cisa/5g

xxii Federal agencies stress supply chain safety for incoming 5G technology. Federal News Network. May 21, 2019. Accessed at: https://federalnewsnetwork.com/insight-of-the-month/2019/05/federal-agencies-stress-supply-chain-safety-for-incoming-5g-technology/.

xxiii Quantum computing could dramatically reduce the time needed to solve the mathematical problems on which encryption techniques currently rely—from months to minutes and seconds. Hello Quantum World! Google Publishes Landmark Quantum Supremacy Claim. Nature. October, 23 2019. Accessed at: https://www.nature.com/articles/d41586-019-03213-z

xxiv Herman, A. and I. Friedson. 2018. Quantum Computing: How to Address the National Security Risk. Washington, DC: Hudson Institute. April 2018. Accessible at: https://s3.amazonaws.com/media.hudson.org/files/publications/Quantum18FINAL4.pdf

xxv PQC Standardization Process: Second Round Candidate Announcement. U.S.'s National Institute of Standards and Technology. January 30, 2019. Retrieved from: https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

xxvi A Guide to Post-Quantum Cryptography; https://blog.trailofbits.com/2018/10/22/a-guide-to-post-quantum-cryptography/

xxvii NISTIR 8105, Report on Post Quantum Cryptography. April 2016. NIST. Retrieved from: https://csrc.nist.gov/publications/detail/nistir/8105/final; Post-Quantum Cryptography Standardization Call for Proposals Announcement. November 30, 2017. NIST. Retrieved from: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

xxviii UK Risk Coalition. Raising the Bar-Principles-based guidance for board risk committees and risk functions in the UK Financial Services Sector. December, 2019. Accessed at: https://riskcoalition.org.uk/the-guidance.