Performing Risk Assessments of Emerging Technologies

Emerging technologies represent a major source of risk, and their complexities make those risk areas especially difficult to assess. Practitioners must consider the whole system view of the emerging technology, its use, its interplay with other technologies, and the combination of parties that could be involved. The uses of emerging technology often depend on the industry and whether an enterprise will use the technology itself or work with other vendors or enterprises to use it. These factors tend to be poorly understood when it comes to new technology, making it difficult to understand the vulnerabilities and risk, including the extent of the risk and how to define plans to mitigate it. Several existing frameworks can be used to assess risk; however, it is important to understand the complexities involved in considering the risk for successfully implementing new technologies and to understand that relying on a single framework poses its own risk.

Considering the Risk of Emerging Technologies

Technology is crucial to many industries, from those directly linked to it (e.g., telecommunications), to those heavily reliant on it (e.g., banking, medicine), to those just starting to use it more extensively (e.g., agriculture, hospitality services). But new technological developments are reported every day. To reach their full potential, organizations must be able to assess new technologies that could be advantageous to their operations. The key to having a complete picture of the advantages and disadvantages of technology is to understand its risk—and the possible ways to mitigate risk.

MICHAEL KELLY | PH.D., CRISC, CISM

Is an experienced business, IT telecommunications, risk and security professional. For the last five years, he has worked with Standard Chartered Bank helping mitigate risk. As the global head information security risk officer for technology and innovation and SC Ventures, he is responsible for ensuring that the bank's technology base is secured by its risk appetite. He helped develop the governance framework for the use of cloud services (both Infrastructure as a Service [IaaS] and Software as a Service [SaaS]) and is helping to create the security building blocks for effectively using blockchain and distributed ledger technology. Working with the startups in SC Ventures, he is proactive in considering different security standards and risk approaches.

ADELINE CHAN | CISM

Is the head of the information cybersecurity framework and strategy for corporate, commercial and institutional banking at Standard Chartered Bank where she works on the first line of defense. Prior to this role, she spent eight years on the second line of defense as a risk officer responsible for implementing a risk framework and conducting risk assessments. She has worked in operational risk, covering financial crime, and in cybersecurity risk with a focus on identity and access management and data protection domains. She was also responsible for developing the risk framework to support startups in SC Ventures. She volunteers actively for SheLeadsTech and the ISACA® Singapore Chapter.

The Difficulties in Assessing Emerging Technology Risk

Emerging technologies by definition are fairly new. There is a great deal to learn about their implications—both in terms of the requirements for operating them and their potential impact should they fail to operate as expected. Predicting the possibility of such a failure also poses difficulties, since there is little historical use on which to base any assumptions. Potential threats can often be predicted if they are related to use cases, but the controls needed to operate the technology safely and securely may be unknown.

Multiparty Risk

Many emerging technologies involve not just technological complexities, but also factors such as the need for interaction with multiple parties, the ambiguity of regulatory environments, a lack of implementation experience and a lack of internal operational experience. Combined, these factors affect the successful deployment and operation of the technology and, thus, the ability to effectively assess its risk. For example, the technology can involve a platform with many interlinked applications; a combination of parties, with each offering some portion of the overall system (e.g., Software as a Service [SaaS] provided by an enterprise offering a business service); or a private blockchain used by a consortium with multiple nodes and shared responsibility.

A business unit may lack existing policies and processes for the emerging technology and may not understand what roles and controls are required to manage the risk of implementation. Most emerging technologies require significant effort in acquiring new knowledge to understand how the application is relevant to the enterprise. Because emerging technologies often demand new skills, knowledge and capabilities, many organizations rely on external parties for aspects of the technology or its use, leading to increased third-party risk. For example, in the automotive sector, manufacturers look to technology enterprises to supply the hardware and software for connected cars.[1] But this presents a new level of risk since it is not always clear who is ultimately responsible for the breakdown in trust if the technology is compromised. It takes time and effort to understand roles and include them in contracts.

Risk and Adoption Stages

Assessing emerging technology risk can be broken down into different decision points corresponding to the technology's adoption stages (**figure 1**).

FIGURE 1

Assessing Emerging Technology by Adoption Stages

Adoption Stage	Emerging Technology Familiarity in the Organization	Need to Understand	Desired Outcome
General business consideration	Not used before	Possible use case and benefits, general threats with controls and ballpark costs	Potential business value Do possible benefits outweigh costs?
Implementation of the first use case	Not used before	Options for deploying, specific threats for the use cases, specific controls needed and cost	Determining the best option for initial benefit
Implementation of further use cases	Limited use	Options for deploying, specific threats for the use case, specific controls needed and cost Building on initial experience and considering what else is known about the technology and its use	Success for each use case
Integration with a strategy to scale	Disparate, often no cohesive view	Best option for scaling to effect strategy with threats, controls, costs and benefits	Maximize benefits and gain economies of scale

Evaluating and Selecting a Risk Framework

Risk frameworks have been developed to help organizations manage operations and comply with regulations. Some rely on more quantitative data to determine the relative effects of the use of technology and controls. No risk framework has yet been established specifically for assessing emerging technology, but some existing models can be used with varying degrees of success depending on the stage of the technology's adoption and whether a general or specific risk assessment (e.g., cybersecurity) is being performed. Some examples of risk approaches include the Risk and Control Self-Assessment (RCSA) framework,[2] Factor Analysis of Information Risk (FAIR) Basic Risk Assessment Methodology[3] and KPMG's Dynamic Risk Assessment.[4] These three examples can be used as starting points for organizations, and similar considerations can be applied to other methodologies.

RCSA Framework

Many organizations adopt the RCSA framework to analyze their operational risk. The RCSA framework is also often used by financial institutions to meet regulatory requirements for an annual self-review of enterprisewide operational risk. It can also be used as a methodology for evaluating third-party vendor risk.

An RCSA framework typically consists of five key elements shown in **figure 2**.[5]

An RCSA exercise is generally conducted by each business unit in an organization. The assessments are then collected and compiled to illustrate a comprehensive understanding of the risk within the entire organization. RCSA is useful for addressing emerging technology risk if the identified risk is primarily process-based and can be managed operationally. RCSA's main weakness when addressing emerging technology risk is that enterprise stakeholders often do not have enough expertise or knowledge of the emerging technology to be able to identify the processes and controls necessary to address weaknesses.[6]

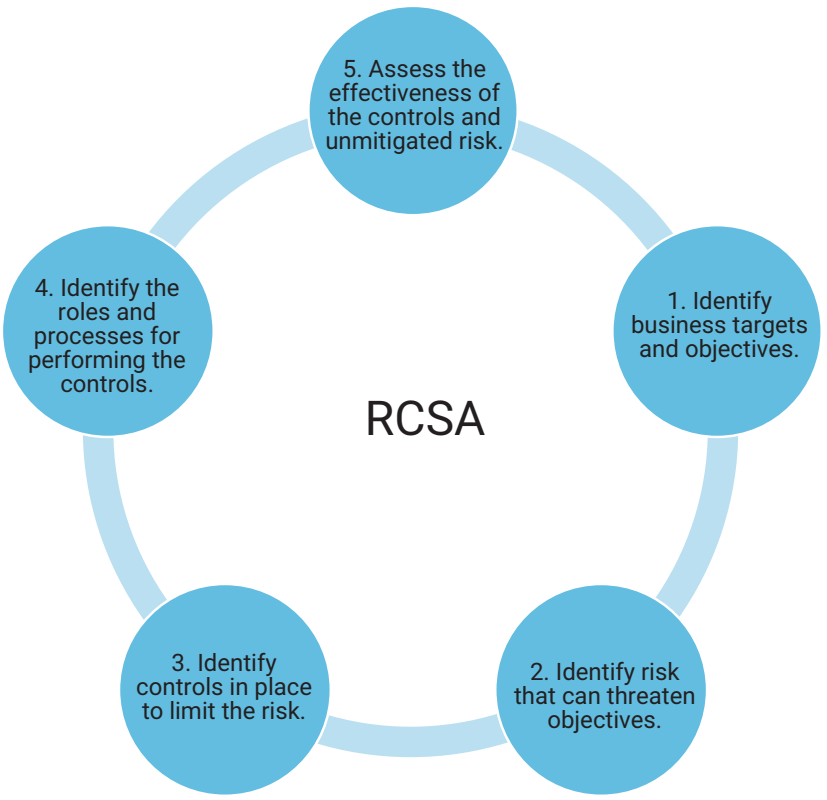
FAIR Methodology

FAIR provides a model for understanding, analyzing and quantifying cyberrisk and operational risk in financial terms. The FAIR Basic Risk Assessment Methodology covers four stages shown in **figure 3**.[7]

No risk framework has yet been established specifically for assessing emerging technology, but some existing models can be used with varying degrees of success depending on the stage of the technology's adoption and whether a general or specific risk assessment…is being performed.

The value of FAIR lies in quantifying cyber and technical risk for information in terms of business impact to assist with enterprise decision-making. FAIR relies on obtaining data from systems and controls combined with data from assessed impact and transforms them into estimates of low, high and most likely impact, sometimes used with Monte Carlo modeling (which predicts the probability of different outcomes when the intervention of random variables is present).[8] FAIR is not intended to be used for assessing the early-stage potential risk of emerging technologies and their

FIGURE 2
RCSA Framework Key Elements

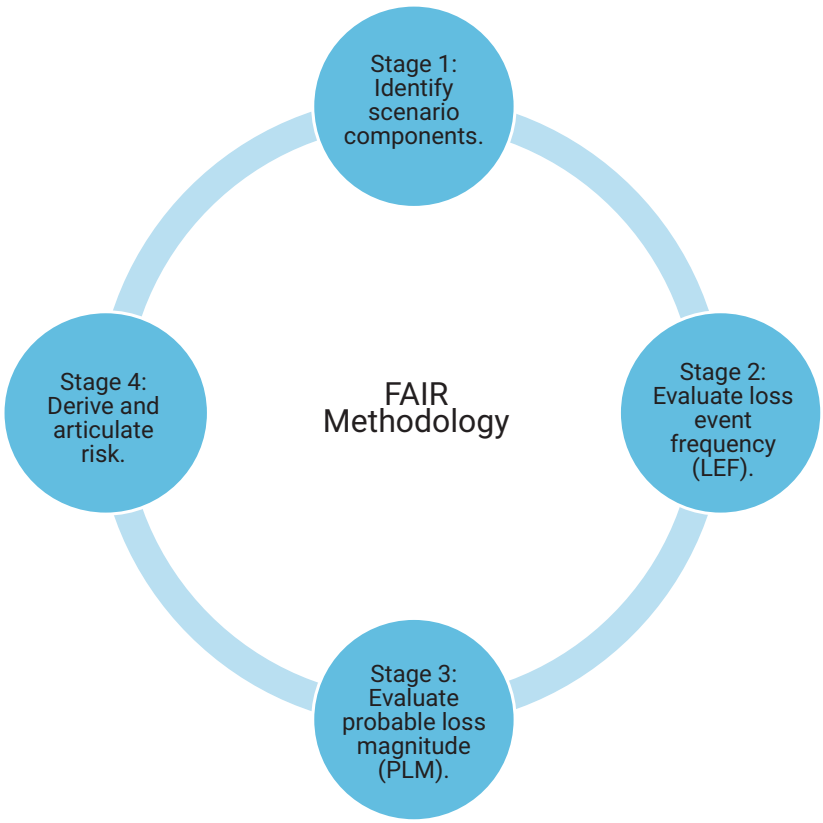


potential adoption as use cases. It offers possibilities where any emerging technology is used as an existing technology, or when similar processes and controls might be employed. Possible use cases could be modeled based on assumptions of how current controls and situations would apply to the risk, which may provide an idea of how the technology would work for the organization. But relying on assumptions rather than considering new approaches could predispose the resulting risk assessment. In addition, the number of assumptions could make the variation for the calculations too broad to be useful. FAIR may be difficult to use in the initial assessment, considering the interrelationships of technology, security and process controls and the effectiveness of those controls for the particular use of the emerging technology.

Dynamic Risk Assessment

Dynamic risk assessments traditionally include continuous assessments to aid in decision-making in changing situations, but they can also help in situations with complex, highly interactive environments and their changing data. There are many dynamic risk assessment methodologies. KPMG's Dynamic Risk Assessment is an example of how sophisticated algorithms and data analytics can be applied to identify, connect and visualize risk in four dimensions. The KPMG Dynamic Risk Assessment framework considers not only likelihood and impact, but also velocity and connectivity. Velocity is the speed at which an incident can develop. It can also be used to describe multiplying and cascading risk. Connectivity involves the way risk can lead to more risk and the degree to which the sources of risk are interrelated. Given the interconnectedness of some of the emerging technologies and the networks with other players in many use cases, a risk practitioner could model different ways that scenarios might develop and players might affect each other. Scenarios could also be used to consider the speed at which incidents can develop and the impact of risk on another risk. By interconnecting risk, practitioners can determine the scenarios in which what appears to be a source of lower risk can be more important and require earlier prioritization (because it could cascade into a risk with greater impact).

FIGURE 3
FAIR Methodology Stages



Assessing risk for emerging technology should start with a framework that addresses the associated business risk.

Employing such a methodology to assess interactions among risk sources and users can be especially useful for emerging technologies that require a networking effect, such as multiple parties deploying a private blockchain in a way that involves interacting with other users. However, one may derive more value from this approach once the technology is better understood and more is known. Understanding and allowing for the factors in different scenarios means stakeholders can take advantage of the methodology's ability to define the specific risk interconnections.[9]

Comparing Risk Approaches

Each of these three methods has its benefits and challenges for assessing emerging technology risk, depending on the organization's stage of consideration and adoption of the technology.

Assessing risk for emerging technology should start with a framework that addresses the associated business risk. Threats should be assessed and a governance framework should be developed to ensure that risk oversight is available. Information collection is key to building a model for managing the implementation of emerging technology and its associated risk. Once information is available, threat analysis using FAIR can be conducted and decisions on controls can be made appropriately through the RCSA. A dynamic risk rating can be applied in situations with more than one risk to be reviewed. **Figure 4** provides a comparison of the possible usefulness of each framework by stage.

Because most organizations have existing risk frameworks, they may select a commonly used framework regardless of the adoption stage. For many organizations, this can mean using the traditional RCSA framework. Given the higher cost of adopting multiple frameworks simultaneously, this could be a reasonable approach; however, the structures of a particular framework could limit its applicability at some stages—or there could be other limitations, such as RCSA not being able to accommodate the complexities of many emerging technologies.

The cloud can be advantageous when using different risk frameworks. When initially adopting cloud computing, it may be better to use an industry analysis approach (similar to RCSA) that allows for more general considerations of the potential impacts and potential value of the cloud, rather than trying to apply the specifics of the existing framework. Once the cloud is used, the threats and controls become more apparent, and the organization can apply a FAIR-like framework to consider how to effectively increase its use of the cloud. RCSA has been adopted for third-party cloud vendor assessments as it is widely understood by risk managers and audit teams. More sophisticated methods, such as FAIR and dynamic risk assessment, can be applied to address threats specific to the organization, which may not only be limited to cloud use but could also address overall weaknesses and linkages to other vulnerabilities in the organization. Complexities in hybrid cloud models may lend themselves well to an approach using some of the features of dynamic risk assessments.

Key Considerations for Assessing the Risk of Emerging Technology

There are three key considerations for implementing emerging technology and assessing risk based on

LOOKING FOR MORE?

- Read *Risk IT Practitioner Guide. www.isaca.org/risk-it-pg2*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 4

Potential Usefulness of Frameworks by Adoption Stage

Adoption Stage	RCSA	FAIR	Dynamic
General business consideration	Frameworks could provide a view of the risk to help with trade-off analysis.	Use is limited since there are no data to support detailed assessment.	Value is added by thinking the interconnected nature of risk.
Implementation of the first use case	Frameworks could be used for assessing operations and their effects on other business and technology risk.	Value is limited at the start, but as the use case develops, data are created to build an assessment.	• Limited value as view on dependencies is still unclear • Has yet to establish interconnectivity
Implementation of further use cases	Gaining insights from the earlier use case, operations support broader business risk analysis.	Data from each use case could help build a broader risk assessment.	Starting to build out a model could give insight for each succeeding case and for the next stage.
Integration with a strategy to scale	Combining the use case assessments into the overall enterprise risk assessment could provide a thorough view into strategy risk and possible options.	Data from existing use cases and business can help build a broader assessment for determining risk with the strategy, and for refining and assessing risk as the strategy unfolds.	Data from existing use cases and business can help drive broader analysis and give insight into layered risk that might be otherwise missed, or help find a better way to invest for scaling.

the selection of the risk frameworks. Managing associated risk should include people, governance process and system design.

People

The first key consideration to implementing emerging technology and assessing its risk is dependent on the business users' level of understanding and their collaboration with IT.

- What is the current level of maturity of the organization—i.e., do the business users understand the complexity and features of the emerging technology?
- What is the level of trust and confidence among the stakeholders impacted by the emerging technology?[10]
- Do different IT groups—such as application (app) development, security, and infrastructure—collaborate well, enable communication across various parts of the organization and help identify risk?[11]

Governance Process

The second key consideration is the process for governing the risk with changing regulations.

- Is the selected emerging technology continuously operating within acceptable risk thresholds?
- Are the organization's business processes mature enough to manage and balance the risk associated with implementing emerging technology?[12]
- Is there continuous monitoring of new regulations and agile development processes to ensure that emerging technology models comply with changing and new regulations?

Systems Design

The third key consideration is whether systems are designed with compliance requirements and policies embedded.

- Is trust built into the design of the emerging technology so that risk is considered ahead of time and managed alongside the design?[13]
- Are discussions about risk and controls initiated early in the technology's implementation to help identify any unaddressed issues and process improvements and ensure that emerging technologies are successfully integrated into the business?

Blockchain Illustration

Given most organizations' relative immaturity in adopting blockchain, it is useful to illustrate the concepts affecting the use of risk frameworks and the risk considerations.

Blockchain is an emerging technology that poses challenges in risk assessment. Uncertainties make it difficult for users to understand the technology and its impact on their enterprises, including:

- Undeveloped standards for blockchain lead to security, privacy and interoperability risk.
- High-energy costs required to support proof of work pose issues for the business case and potential regulatory, environmental, social and governance (ESG) impacts.
- Data privacy, especially with different nation-imposed and regional regulations, adds complexity to the use of blockchain.
- Trust in developers is required as blockchain is a new platform.
- User-oriented risk, such as maintaining private keys used to access a wallet, is a challenge for a decentralized network.
- Scalability and transaction speed may be impacted by congestion.
- Using public blockchain vs. private blockchain or permissioned blockchain vs. permissionless blockchain affects the use case.
- The highly networked quality of most blockchain implementations requires extensive interworking with third parties as partners and providers.

In the initial stage of deciding whether and how to use blockchain, a risk approach that supports broad considerations and risk implications is needed. General matters from an RCSA may be applicable at this early stage to consider the effect of risk on the business case. Details for a risk framework such as FAIR can be obtained only once an organization selects and implements a specific blockchain use. And the complex interrelationships lend themselves to the use of dynamic assessments to determine where most attention should be placed.

Conclusion

Emerging technology adoption has its own life cycle and the adoption stage determines the type

of risk assessment required. This, in turn, affects the types of frameworks that can provide the necessary view of risk at a given stage. The degree to which emerging technology is similar to existing technology and its current mode of use can factor into whether a particular framework should be used. Early in the adoption process, little is known about the technology's possible effects and no data are available to feed into more comprehensive models, such as FAIR. However, as use cases develop and experience with the new technology is gained, standards and operating processes are developed and an understanding of the impact becomes a basis for assessing broader use of the technology. If an organization is already using more quantitative risk assessments, such as FAIR, then data from earlier use cases can feed into the overall assessment and provide support as a strategy to be considered and implemented. In a more mature organization, emerging technology can be risk-assessed using more sophisticated, data-driven models, such as dynamic risk assessment, to gain better insights into the potential interrelated nature of the risk. Whatever framework an organization uses normally, a willingness to use multiple risk methodologies will enable matching an agile risk management approach to the adoption of the technology and the benefit of the business.

The degree to which emerging technology is similar to existing technology and its current mode of use can factor into whether a particular framework should be used.

Endnotes

1 Brachio, A.; "How to Manage the Evolving Risks of Emerging Technology," EY, 15 February 2019, *https://www.ey.com/en_sg/consulting/how-to-manage-the-evolving-risks-of-emerging-technology*

2 Kumar, T.; "The Methods and Tactics Behind Risk and Control Self-Assessment," *The Global Treasurer*, 6 February 2019, *https://www.theglobaltreasurer.com/2019/02/06/the-methods-and-tactics-behind-risk-and-control-self-assessment/*

3 FAIR Institute, "FAIR Risk Management," *https://www.fairinstitute.org/fair-risk-management*

4 KPMG, *Dynamic Risk Assessment*, Netherlands, June 2019, *https://assets.kpmg/content/dam/kpmg/au/pdf/2017/dynamic-risk-assessment-four-dimensional-view.pdf*

5 *Op cit* Kumar

6 Riggins, N.; "The Methods and Tactics Behind Risk and Control Self-Assessment," *The Global Treasurer*, 6 February 2019, *https://www.theglobaltreasurer.com/2019/02/06/the-methods-and-tactics-behind-risk-and-control-self-assessment/*

7 *Op cit* FAIR Institute

8 Kenton, W.; "Monte Carlo Simulation," Investopedia, 4 October 2021, *https://www.investopedia.com/terms/m/montecarlosimulation.asp*

9 *Op cit* KPMG

10 PricewaterhouseCoopers (PwC), "Emerging and Disruptive Technology Risk," *https://www.pwc.co.uk/services/risk/technology/emerging-disruptive-technology-risk-stay-in-control.html*

11 Pariseau, B.; "IT Governance Must Catch Up With DevSecOps, Experts Say," *TechTarget*, 24 November 2020, *https://www.techtarget.com/searchitoperations/news/252492646/IT-governance-must-catch-up-with-DevSecOps-experts-say*

12 Young, J.; "Balancing the Benefits With the Risks of Emerging Technology," *TechTarget*, 19 July 2021, *https://www.techtarget.com/searchsecurity/post/Balancing-the-benefits-with-the-risks-of-emerging-technology*

13 *Op cit* Brachio