The Cyberrisk Quantification Journey

Many organizations suffer from being unaware of their levels of cyberrisk and lack business engagement in cybertechnology in general. Cybersecurity improvements are often capability based and led by IT; however, many cybersecurity practitioners are unable to obtain funding for holistic cybertransformation programs because they do not speak the same language as those operating the business. To resolve these issues, organizations must embark on cyberrisk journeys that include identifying risk scenarios, developing risk profiles (possibly as part of an enterprise risk management [ERM] exercise), using frameworks such as those shown in **figure 1** to assess controls, and using Factor Analysis of Information Risk (FAIR) to assess risk and determine optimal remediation road maps. The final part of the journey is the use of machine learning to reduce subjectivity and increase the cadence of work. **Figure 1** shows the frameworks used in cyberrisk quantification and the purpose of each.

Risk Scenarios

COBIT® is a useful framework for IT processes and IT general controls. The overall COBIT risk management process (Align, Plan and Organize [APO] APO12 *Manage Risk*) consists of collecting data, analyzing risk, maintaining a risk portfolio, articulating or communicating risk, defining a risk management action portfolio and responding to risk.[1] Risk analysis is the process used to estimate the frequency and magnitude of a given risk scenario—identifying and evaluating a risk and its potential impact on the organization. Risk assessment is a broader process that includes ranking risk, grouping like risk areas and documenting existing controls.[2]

FIGURE 1
Relevant Frameworks

Framework	Purpose
COBIT® 2019	How are IT processes managed, including IT risk and cybersecurity?
International Organization for Standardization (ISO) 2700X	How is cybersecurity managed?
NIST Cybersecurity Framework (CSF)	How is the maturity of cybersecurity controls measured?
MITRE ATT&CK	What techniques do attackers use?
FAIR	How much cybersecurity risk exists? Which remediation activities should be prioritized?

DAVID VOHRADSKY | CISA, CRISC, CISM, CGEIT, CDPSE

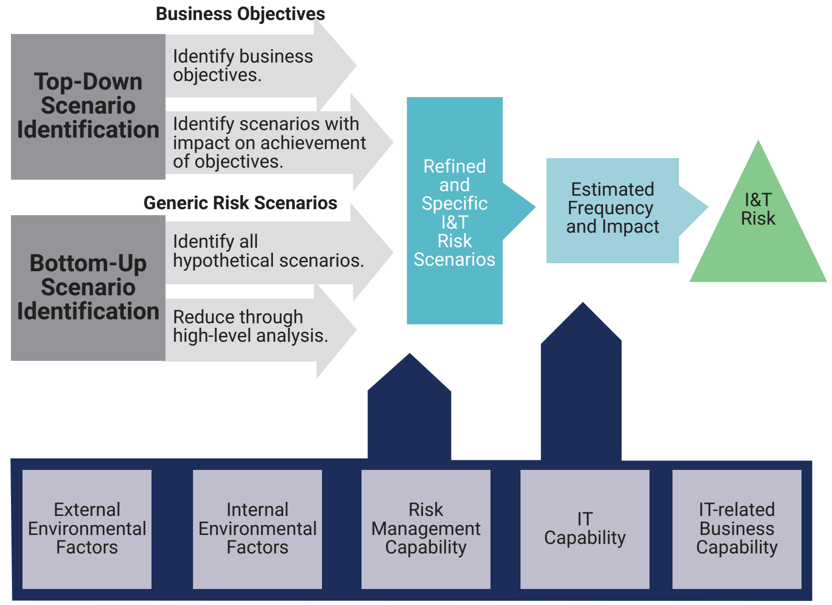
Is the founder of Cyberisk Australia, a boutique cybersecurity consultancy specializing in cybersecurity risk quantification and remediation road maps, digital transformation and third-party risk assessments, and cyberpolicy and risk framework development for Australian Stock Exchange (ASX) mid-capitalization organizations and medium-sized government agencies. Vohradsky has previously held senior-level management and consulting positions with Protiviti, Commonwealth Bank, the New South Wales Government, Macquarie Bank and Tata Consultancy Services. He is also a member of the ISACA® Information and Technology Risk Advisory Group.

As shown in **figure 2**, cyberrisk scenarios can be identified top down from business objectives or bottom up beginning with a list of potential threat actors, event types, target assets and types of impact.[3]

The starting point should be a discussion about what the business does, what data and systems are used, and the risk factors related to the external competitive and cyberthreat environment and internal business and technical environment.

FIGURE 2

Risk Scenario Overview


Business Objectives
Top-Down Scenario Identification
Identify business objectives.
Identify scenarios with impact on achievement of objectives.
Generic Risk Scenarios
Bottom-Up Scenario Identification
Identify all hypothetical scenarios.
Reduce through high-level analysis.
Refined and Specific I&T Risk Scenarios
Estimated Frequency and Impact
I&T Risk
External Environmental Factors
Internal Environmental Factors
Risk Management Capability
IT Capability
IT-related Business Capability

Source: ISACA®, *Risk IT Framework*, 2nd Edition, USA, 2020, *www.isaca.org/risk-it-f2*

Figure 3 shows an example risk scenario for a health services organization.

In this case, the threat actors are cybercriminals, internal staff and third parties, and the threat vectors include phishing, vulnerabilities, ransomware and unauthorized access. For a more granular approach, it is possible to work out attacks based on the MITRE ATT&CK Framework,[4] a framework of adversary tactics, techniques and their possible mitigations based on real-world observations, to validate the reasonableness of the scenarios. The critical data assets are patient, practitioner and employee data, and payments and security credentials, which means that the critical systems are those supporting the critical data assets.

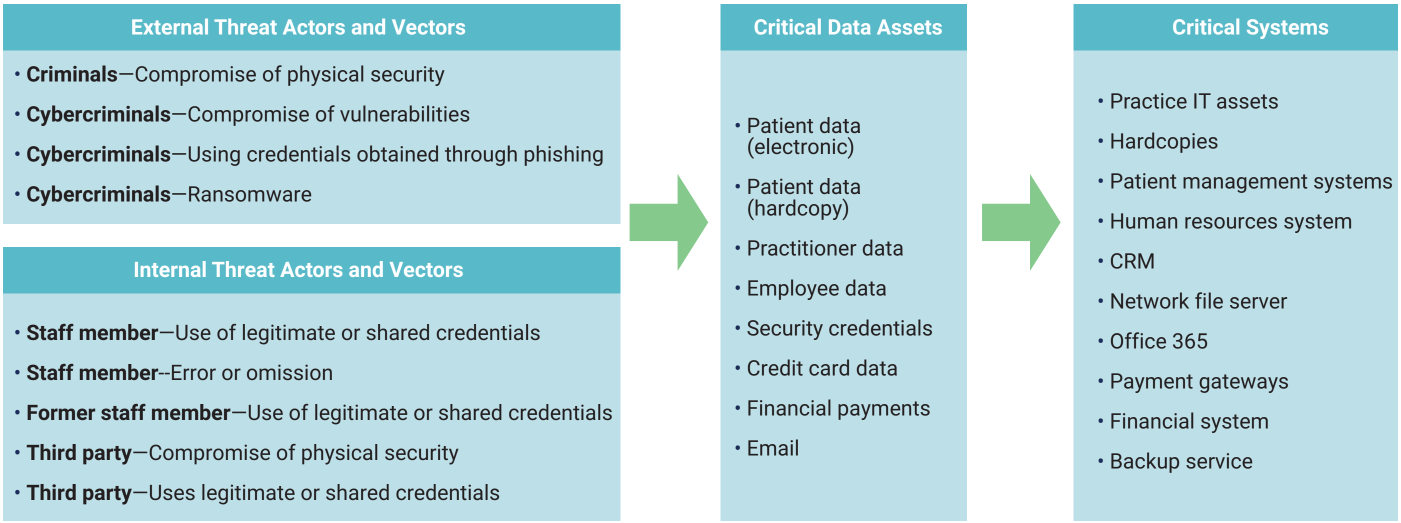
The risk scenarios derived from the material combinations of actors, attack vectors and assets, shown in **figure 4** (for patient data), can be used as examples for this use case.

A Simple Threat and Risk Assessment

Cyberrisk is the combination of the likelihood of an event (risk scenario) and its impact. There are three methods of analyzing this risk: qualitative, quantitative and a hybrid of the two (semiquantitative).

FIGURE 3

Example Health Services Risk Scenario



External Threat Actors and Vectors

- **Criminals**—Compromise of physical security
- **Cybercriminals**—Compromise of vulnerabilities
- **Cybercriminals**—Using credentials obtained through phishing
- **Cybercriminals**—Ransomware

Internal Threat Actors and Vectors

- **Staff member**—Use of legitimate or shared credentials
- **Staff member**--Error or omission
- **Former staff member**—Use of legitimate or shared credentials
- **Third party**—Compromise of physical security
- **Third party**—Uses legitimate or shared credentials

Critical Data Assets

- Patient data (electronic)
- Patient data (hardcopy)
- Practitioner data
- Employee data
- Security credentials
- Credit card data
- Financial payments
- Email

Critical Systems

- Practice IT assets
- Hardcopies
- Patient management systems
- Human resources system
- CRM
- Network file server
- Office 365
- Payment gateways
- Financial system
- Backup service

FIGURE 4

Patient Data-Related Scenarios

Scenario	
P1	Cybercriminal uses phishing to gain access to the patient management system
R1	Cybercriminal performs a ransomware attack against the patient management system
R2	Cybercriminal performs a ransomware attack against another critical cloud service
V1	Cybercriminal compromises vulnerabilities in the patient management system
V2	Cybercriminal compromises vulnerabilities in another critical cloud service
S1	Employee uses legitimate credentials to gain access to the patient management system
S2	Former employee uses legitimate credentials to gain access to the patient management system
S3	Third party uses legitimate credentials to gain access to the patient management system

The simple qualitative approach is to create a table that compares the likelihood and impact of each risk scenario. This is useful for communicating risk to stakeholders and seeking feedback.[5] The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 27005:2011 *Information Technology—Security Techniques–Information Security Risk Management* contains an example risk assessment matrix,[6] or probability impact graph (PIG), for a simple qualitative risk assessment (**figure 5**). Typically, this is used in a mirror reverse, with the highest-rated risk in the top right corner. Many other risk analysis and presentation models can be used for such an assessment.

The example risk scenarios are assessed by assigning a qualitative likelihood and impact through a five-level Likert scale and plotting the results on a risk matrix to allow communication and stakeholder feedback on the high-rated (red) risk (**figures 6** and **7**).

The scales can be linear or logarithmic, using descriptive choices, probabilities, or currency or percentage values, all of which are subjective. **Figure 8** shows a semiquantitative risk matrix with the scales defined using probability (for likelihood) and a number or percentage (for impact).

Issues with qualitative and semiquantitative assessments include subjective scoring, difficulty in comparing risk assessed by different stakeholders, difficulty in prioritizing gaps, the ability to cheat the system and the inability to obtain a holistic value of cybersecurity risk.[7] This qualitative approach assumes a linear difference between ratings and that the subjective nature of the description of choices only connotes accuracy,[8] while influencing stakeholder responses in different ways.

FIGURE 5

Example Risk Matrix

	Likelihood of Incident Scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Source: International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), ISO/IEC 27005:2011 *Information Technology—Security Techniques—Information Security Risk Management,* Switzerland, 2011, *https://www.iso.org/standard/56742.html.* Reprinted with permission.

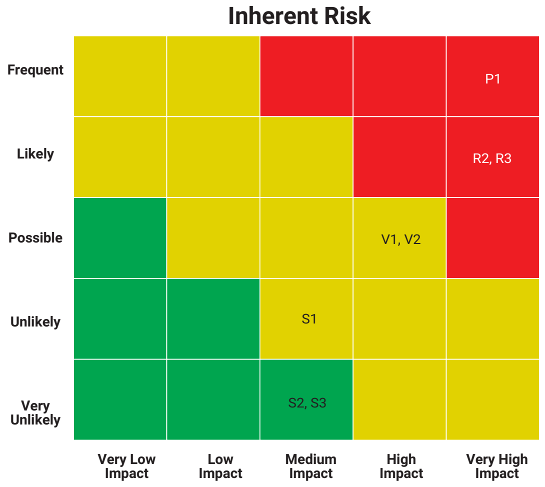
FIGURE 6

Example Qualitative Risk Assessment

#	Scenario	Likelihood	Impact
P1	Cybercriminal uses phishing to gain access to the patient management system	Frequent	Very High
R1	Cybercriminal performs a ransomware attack against the patient management system	Likely	Very High
R2	Cybercriminal performs a ransomware attack against another critical cloud service	Likely	Very High
V1	Cybercriminal compromises vulnerabilities in the patient management system	Possible	High
V2	Cybercriminal compromises vulnerabilities in another critical cloud service	Possible	High
S1	Employee uses legitimate credentials to gain access to the patient management system	Unlikely	Medium
S2	Former employee uses legitimate credentials to gain access to the patient management system	Very Unlikely	Medium
S3	Third party uses legitimate credentials to gain access to the patient management system	Very Unlikely	Medium

FIGURE 7

Example ISO 27005 Risk Matrix

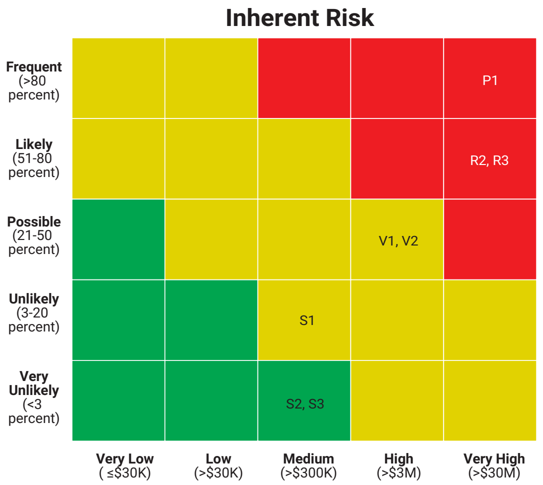


Inherent Risk

	Very Low Impact	Low Impact	Medium Impact	High Impact	Very High Impact
Frequent	🟨	🟨	🟥	🟥	🟥 P1
Likely	🟨	🟨	🟨	🟥	🟥 R2, R3
Possible	🟩	🟨	🟨	🟨 V1, V2	🟥
Unlikely	🟩	🟩	🟨 S1	🟨	🟨
Very Unlikely	🟩	🟩	🟩 S2, S3	🟨	🟨

FIGURE 8

Semiquantitative Risk Matrix (AUD$)



Inherent Risk

	Very Low (≤$30K)	Low (>$30K)	Medium (>$300K)	High (>$3M)	Very High (>$30M)
Frequent (>80 percent)	🟨	🟨	🟥	🟥	🟥 P1
Likely (51-80 percent)	🟨	🟨	🟨	🟥	🟥 R2, R3
Possible (21-50 percent)	🟩	🟨	🟨	🟨 V1, V2	🟥
Unlikely (3-20 percent)	🟩	🟩	🟨 S1	🟨	🟨
Very Unlikely (<3 percent)	🟩	🟩	🟩 S2, S3	🟨	🟨

Control Assessments

The NIST CSF[9] or a similar control framework is useful in determining the maturity and effectiveness ratings for cybersecurity controls (**figure 9**).

Each of the 77 NIST CSF controls can be assessed using a five-level capability maturity scale reflective of the people, processes and technologies that an organization has implemented for the control (**figures 10** and **11**). The maturity scale can be based loosely on capability maturity model integration (CMMI). **Figure 10** shows a maturity 3 user access review control as being fully documented and used in all critical systems.

Effectiveness refers to how well a control is designed and operating (i.e., whether it is weak, marginal or strong).

The effectiveness of NIST CSF controls can be assessed using a control assurance exercise, key control indicators or, in the absence of either, translating from a maturity scale. A smaller set of controls with objectives and effectiveness ratings aggregated from several NIST CSF or NIST Special Publication (SP) SP 800-53 controls can be most useful.

In the example case, a possible subjective conclusion is that maturity 0 and 1 are weak, maturity 2 is marginal, and maturity 3 and 4 are strong.

FIGURE 9

NIST CSF

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identify Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Process and Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Source: National Institute of Standards and Technology (NIST), "An Introduction to the Components of the Framework," *https://www.nist.gov/cyberframework/online-learning/components-framework*. Reprinted with permission.

FIGURE 10

Example NIST CSF Control Maturity Assessment

ID	Objective	Question	Rating	Response
PR.AC-1	Identities and credentials are issued, managed, verified, revoked and audited for authorized devices, users and processes.	What is the process to regularly review access to ensure users are appropriate and revoke it when no longer required?	1	None
			2	*Ad hoc* review by IT or audit
			3	Documented process rolled out to all critical systems
			4	Automated using identity access management (IAM) tools

Figure 12 shows an example subset of NIST control effectiveness ratings for the example health services organization. Subjectively, control ratings from the maturity levels in **Figure 11** can be derived, giving a weak rating for third-party, privileged access management and training because their control maturity levels were less than 2.

Risk Profiles

Following analysis of risk scenarios and assessment of control effectiveness, the next step in the qualitative approach is to subjectively determine current risk for each scenario using a risk profile (**figure 13**).

In this case, the subjective determination is that certain controls are key to mitigating each scenario. This can be worked out more accurately using bow-tie analysis (using cause and consequence diagrams) or through polling (using the Delphi Method[10]).

In this example, the phishing for patient data scenario is still rated high risk because the overall control rating is marginal. Similarly, the vulnerability scenario is still rated medium risk.

A remediation plan for the risk profile could prioritize the weak and marginal key controls related to the high-risk scenario by implementing controls such as privileged access management (PAM) and user awareness training followed by the adoption of a policy framework and incident response plan. But

FIGURE 11

Overall NIST CSF Control Maturity

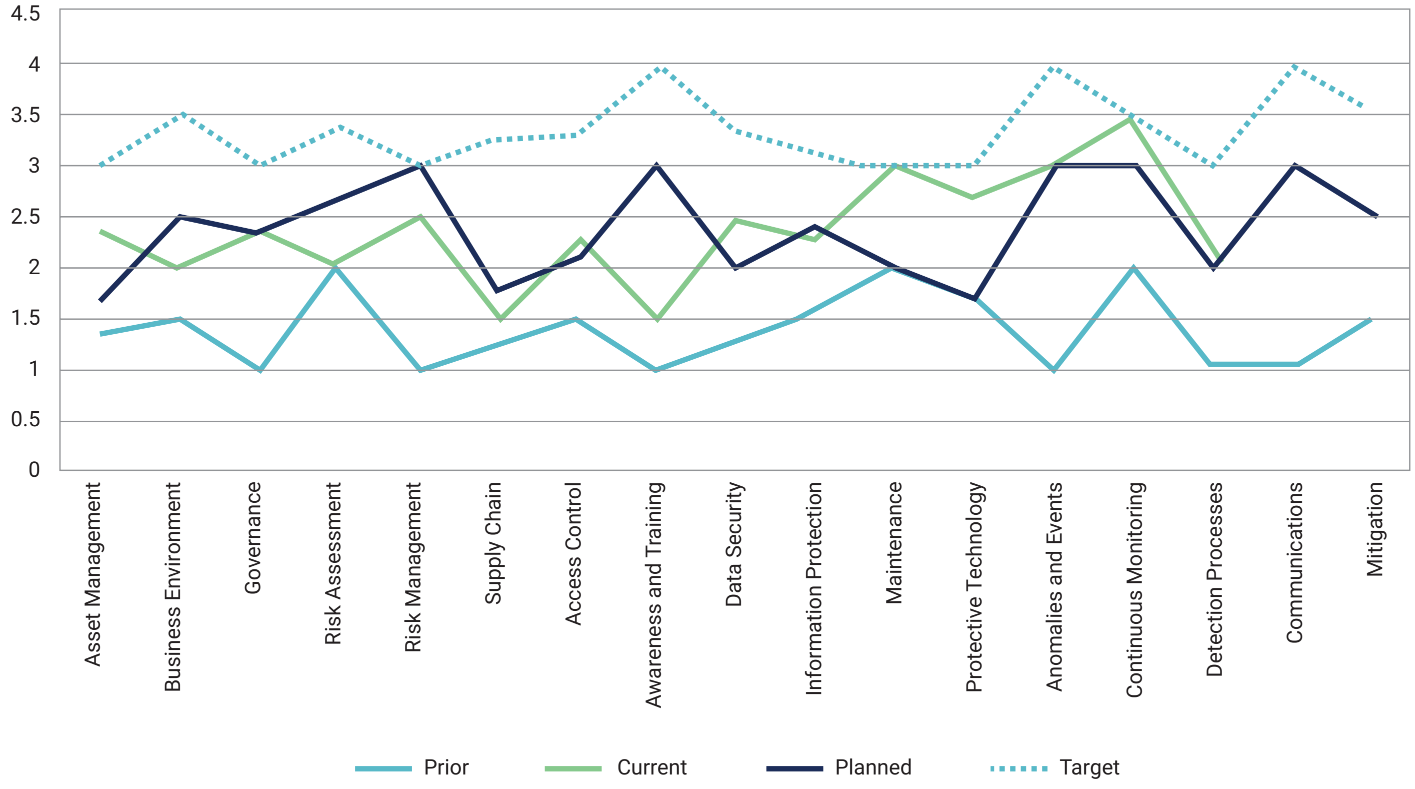


FIGURE 12

NIST CSF Control Effectiveness Ratings

Control	Control Description	Current Rating
DEAE1	Security Logging and Monitoring	Strong
DECM-4	Email and Web Protection	Strong
DECM4-1	Endpoint Protection	Strong
IDAM1/5	Asset Inventory	Marginal
IDGV1	Policy Framework	Marginal
IDRA1-1	Vulnerability and Patch Management	Marginal
IDRA1-3	Penetration Testing	Marginal
IDSC1	Third-Party Management	Weak
PRAC1	Access Management	Marginal
PRAC3	Authentication	Marginal
PRAC4	Privileged Access Management	Weak
PRAC5-1	Secure Network Architecture	Marginal
PRAC5-2	Perimeter Security (Firewall Configuration)	Strong
PRAT1	User Awareness Training	Weak
PRIP1	Secure Baseline Configuration	Marginal
PRIP4	Backup and Recovery	Strong
PRIP9/RS	Security Incident Response	Marginal

there is no ability using this qualitative method of risk profiling to prioritize remediation across all risk scenarios or prioritize within the list of weak or marginal key controls. The resulting cybersecurity road map can only be expressed in terms of a control maturity uplift or a subjective determination of criticality using a framework such as the Essential 8 (an Australian government cybersecurity guideline with eight priority controls).[11]

Cyberrisk Quantification and FAIR

A useful definition of cyberrisk quantification is the process of evaluating cyberrisk scenarios using mathematical modeling techniques in a manner that supports more informed cybersecurity investment decisions.

The benefits of quantifying cyberrisk include the ability to increase the engagement of business decision makers on cyberrisk, understand the business impact of cyberrisk, prioritize controls in monetary terms, make better decisions regarding security trade-offs, determine the level of cyberinsurance required and project the return on investment (ROI) of cybersecurity initiatives.[12, 13]

FAIR is an open international standard risk model that was developed specifically to enable quantified risk measurement. FAIR aims to improve objectivity through the calculation of factors including threat event frequency, primary and secondary loss event frequencies, and primary and secondary loss magnitudes (**figure 14**).

In the FAIR standard, risk is quantified by running a Monte Carlo simulation against each of the risk factors in **figure 14** and adding the factors together to determine the resulting primary and secondary annual loss expectancies (ALEs). Monte Carlo

LOOKING FOR MORE?

- Read *Cyberrisk Quantification.* *www.isaca.org/cyberrisk-quantification*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 13

Qualitative Risk Profile

ID	Scenario	Inherent Risk	Key Controls	Control Rating	Overall Control Rating	Current Risk
P1	Cybercriminal uses phishing to gain access to the patient management system	High	Policy Framework	Marginal	Marginal	High
			Authentication	Strong		
			Access Management	Strong		
			Privileged Access Management	Weak		
			User Awareness Training	Weak		
			Email and Web Protection	Strong		
			Security Logging and Monitoring	Strong		
			Security Incident Response	Marginal		
V1	Cybercriminal compromises vulnerabilities in the patient management system	Medium	Policy Framework	Marginal	Marginal	Medium
			Asset Inventory	Marginal		
			Secure Baseline Configuration	Marginal		
			Perimeter Security (Firewall Configuration)	Strong		
			Secure Network Architecture	Weak		
			Vulnerability and Patch Management	Marginal		
			Penetration Testing	Weak		
			Third-Party Management	Weak		
			Endpoint Protection	Marginal		
			Security Logging and Monitoring	Strong		
			Backup and Recovery	Strong		
			Security Incident Response	Marginal		

simulations are a mathematical way to model the outcomes of a random chain of events, such as each of the factors in the FAIR model.[14]

The example shown in **figure 15** shows click rates, IT-and business-supplied costs of response, and estimates of consequential damage such as fines, lawsuits and loss of business to calculate an ALE of AUD$188 million for the inherent risk of loss of patient data due to phishing.

The vulnerability factor can be semiquantitatively calculated from the subjective control effectiveness. **Figure 16** shows a possible way of doing this. A more accurate calculation can be made by conducting a control assurance exercise using audit grade sampling.

The contribution of an individual control for the overall mitigation of a risk can be semiquantitatively assessed by assigning weightings to control effectiveness based on the type of control. Weightings can be determined semiquantitatively using the analytic hierarchy process (normalized pair-wise comparison of each control using opinions of a small group of small and medium enterprises).[15] **Figure 17** shows an example set of weightings for the example case study.

FIGURE 14

FAIR Risk Factors

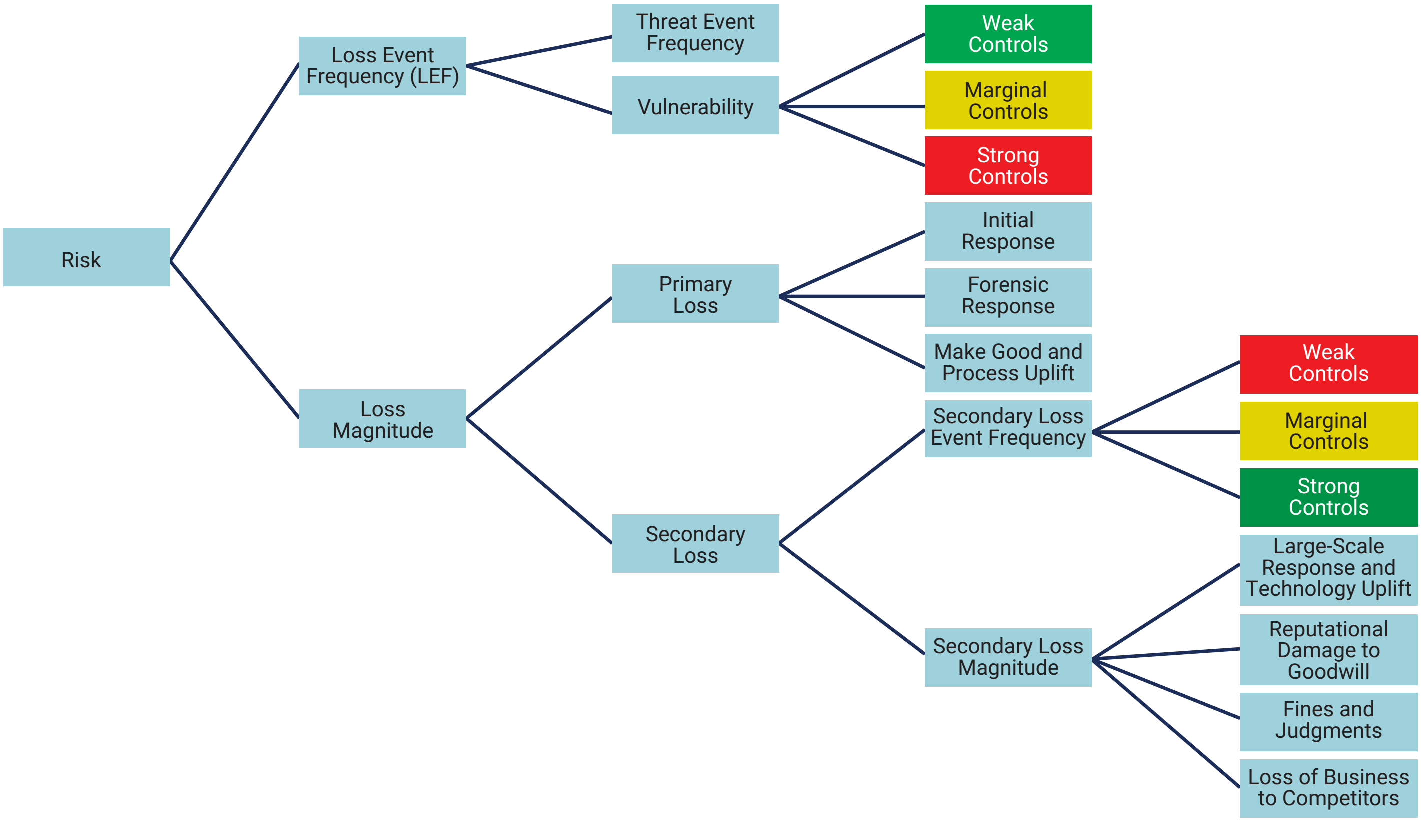


FIGURE 15

Risk Quantification of Scenario P1 Using FAIR

Risk Factor	Value	Example Rationale
Loss Event Frequency (LEF)	13 per annum	Phishing email history, open rates, click rates
Primary Loss—Productivity	AUD$1K–$2K	Diverting staff from routine work to investigate and follow up incident
Primary Loss—Response	AUD$20K	Forensic response specialists
Primary Annual Loss Expectancy (ALE)	AUD$365,000 per annum	
Secondary LEF	10 percent SLEF 13 x 0.1 = 1.7 p.a.	Unlikely, but not rare for a secondary loss
Secondary Response—Replacement	Zero	No reimbursement of payments
Secondary Loss—Response	AUD$310K	Response to the regulatory body, deep dive control assurance, process reengineering, fast-track systems uplift
Secondary Loss—Fines, Judgments, Damages and Compensation	OAIC–AUD$63K Identity–AUD$92M	Office of the Australian Information Commissioner publicly announced fine AUD$63K Identity protection for all customers in case of breach or suspected
Secondary Loss—Competitive	Loss of Business AUD$18.7M	Loss of business due to data breach
Secondary ALE	AUD$188M	

FIGURE 16

Semiquantitative Assessment of Control Effectiveness

Maturity	Effectiveness	Likelihood Control Objective Met	Vulnerability
0-Absent	Weak	0 percent	100 percent
1-*Ad hoc*/Initial		0–20 percent (Unlikely)	80–100 percent
2-Repeatable	Marginal	20–60 percent (Possible)	40–80 percent
3-Defined	Marginal	60–80 percent (Likely)	20–40 percent
	Strong		
4-Managed	Strong	80–100 percent (Almost Certain)	0–20 percent
5-Optimized	Strong		

FIGURE 17

Example Control Type Weighting

Control Type	Weighting
Key	70 percent
Compensating	25 percent
Other	5 percent
Preventive	70 percent
Detective	25 percent
Corrective	5 percent

Again, using a normal loss distribution and 50th percentile, a quantified risk profile can be created using a spreadsheet. **Figure 18** shows a quantified risk profile using the example case study scenarios. In this case, calculations of the relative contribution of each key control are shown. The relative contribution of each key control and the relative risk buydown possible from control remediation can be determined by totaling the weighted contribution of the controls in AUD dollars. However, a true to standard FAIR risk quantification exercise will require more advanced statistical calculations.

For the example risk profile, **figure 19** shows the notional value of remediation of each of the controls across all risk scenarios.

Using a quantified risk profile, the remediation plan of prioritizing PAM and user awareness training followed by policy framework and incident response can be confirmed. Quantification allows the policy framework to be prioritized ahead of weak controls within the medium-rated scenario, even though the need is not obvious within the qualitative risk profile.

A combination of quantified risk assessments using FAIR and semiquantitative control assessments using NIST CSF can also be used to conduct a what-if analysis to develop a point-in-time optimal cybersecurity road map and to calculate a periodic quantified risk buy down. An example is shown in **figure 20**.

Issues with quantitative assessments include lack of threat event data to quantify threat event frequency (TEF), actual likelihood or loss event frequency (LEF), lack of subject matter experts, difficulty of placing a quantitative value on subjective elements of vulnerability (especially weighting controls), and secondary losses, such as reputation. Many events are unpredictable and based on speculation rather than on justifiable facts.[16]

Machine Learning

The final stage of the cybersecurity journey is proactive cybersecurity—where "advanced analytics and machine learning are used for preventive detection, and multilayer security-by-design is embedded in all products and services."[17] In current research literature, quantitative techniques include Bayesian analysis, copula, expert systems, fuzzy logic, game theory and utility theory. These techniques have been researched for loss estimation, insurance premium calculation, vulnerability assessment, threat identification and control selection.[18]

A project at the University of Wollongong, New South Wales, Australia, developed a machine learning cyberquantification platform that will form the basis of a governance, risk and compliance software-as-a-service platform called myRISK. **Figure 21** shows the framework for the underlying machine learning model from the project, which includes a MITRE attack graph, a NIST CSF-aligned MITRE defense graph, and a machine learning computation of the probability

FIGURE 18

Example Quantified Risk Profile

ID	Scenario	Value at Risk (AUD$M)	Control Type	Weight	Key Controls	Contribution (Weight/ Number of Controls)	Control Rating	Vulnerability	Vulnerability Contribution	Overall Vulnerability	Current Risk (AUD$M)	Value of Remediation (AUD$M)
P1	Cybercriminal/ Phishing/Patient System	189.00	Preventive	70 percent	Policy Framework	12 percent	Marginal	50 percent	6 percent	47 percent	88.20	5.15
					Authentication	12 percent	Strong	20 percent	2 percent			2.06
					Access Management	12 percent	Strong	20 percent	2 percent			2.06
					Privileged Access Management	12 percent	Weak	100 percent	12 percent			10.29
					User Awareness Training	12 percent	Weak	100 percent	12 percent			10.29
					Email and Web Protection	12 percent	Strong	20 percent	2 percent			2.06
			Detective/ Corrective	30 percent	Security Logging and Monitoring	15 percent	Strong	20 percent	3 percent			2.65
					Security Incident Response	15 percent	Marginal	50 percent	8 percent			6.62
V1	Cybercriminal/ Vulnerabilities/ Patient System	23.00	Preventive	70 percent	Policy Framework	8 percent	Marginal	50 percent	4 percent	53 percent	12.27	0.48
					Asset Inventory	8 percent	Marginal	50 percent	4 percent			0.48
					Secure Baseline Configuration	8 percent	Marginal	50 percent	4 percent			0.48
					Perimeter Security	8 percent	Strong	20 percent	2 percent			0.19
					Secure Network Architecture	8 percent	Weak	100 percent	8 percent			0.95
					Vulnerability and Patch Management	8 percent	Marginal	50 percent	4 percent			0.48
					Penetration Testing	8 percent	Weak	100 percent	8 percent			0.95
					Third-Party Management	8 percent	Weak	100 percent	8 percent			0.95
					Endpoint Protection	8 percent	Marginal	50 percent	4 percent			0.48
			Detective/ Corrective	30 percent	Security Logging and Monitoring	10 percent	Strong	20 percent	2 percent			0.25
					Backup and Recovery	10 percent	Strong	20 percent	2 percent			0.25
					Security Incident Response	10 percent	Marginal	50 percent	5 percent			0.61

FIGURE 19
Notional Value of Key Control Remediation

Control	Notional Value of Remediation (AUD$M)
Access Management	2.06
Asset Inventory	0.48
Authentication	2.06
Backup and Recovery	0.25
Email and Web Protection	2.06
Endpoint Protection	0.48
Penetration Testing	0.95
Perimeter Security	0.19
Policy Framework	**5.62**
Privileged Access Management	**10.29**
Secure Baseline Configuration	0.48
Secure Network Architecture	0.95
Security Incident Response	**7.23**
Security Logging and Monitoring	2.89
Third-Party Management	0.95
User Awareness Training	**10.29**
Vulnerability and Patch Management	0.48
Access Management	2.06

that a pathway through the MITRE attack framework for a given architecture will be successful for an actor given its relative strength and technique preferences and considering an organization’s NIST CSF control effectiveness.

The objective of this work is to provide a more accurate quantification of LEF for inclusion in FAIR-based assessments and to provide a real-time control prioritization capability.

Conclusion

A qualitative approach to risk assessment, which involves subjective risk scoring, can lead to difficulty in comparing risk assessed by different stakeholders, difficulty in prioritizing gaps, an inability to holistically value cybersecurity risk and a resulting lack of business engagement.

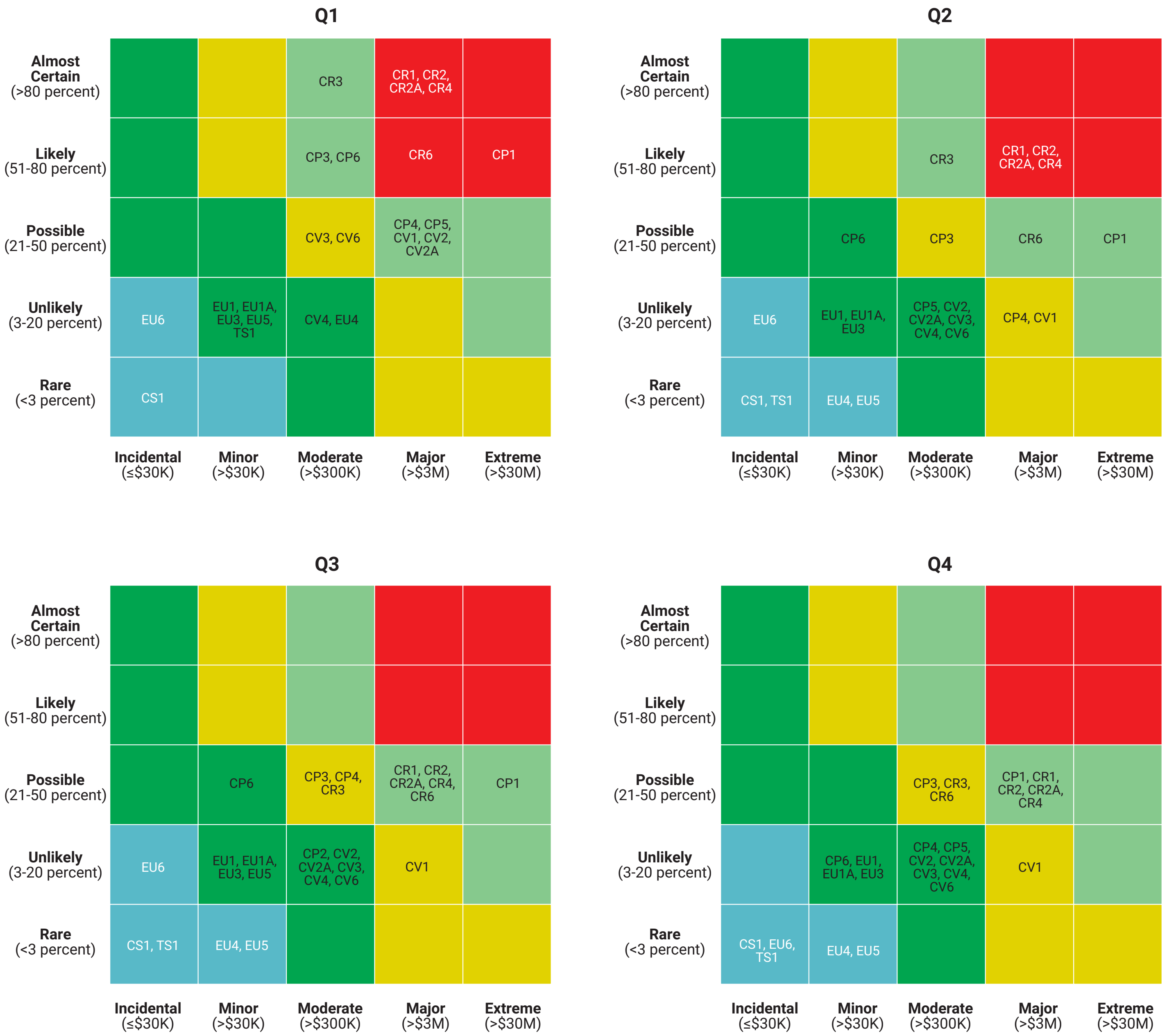
To obtain adequate funding for a holistic cybersecurity transformation program, it is necessary to use a quantitative approach that leverages COBIT, NIST and FAIR frameworks.

Quantification increases business engagement and understanding of cyberrisk and allows better decision-making on control improvements based on return on investment (ROI) trade-offs.

Issues with quantitative assessments such as lack of threat data, lack of subject matter experts, and subjective factors such as control weighting and reputational losses can be addressed through machine learning.

FIGURE 20

Example Periodic Risk Buydown (Illustrative Only) (AUD$)



Q1

	Incidental (≤$30K)	Minor (>$30K)	Moderate (>$300K)	Major (>$3M)	Extreme (>$30M)
Almost Certain (>80 percent)			CR3	CR1, CR2, CR2A, CR4	
Likely (51-80 percent)			CP3, CP6	CR6	CP1
Possible (21-50 percent)			CV3, CV6	CP4, CP5, CV1, CV2, CV2A	
Unlikely (3-20 percent)	EU6	EU1, EU1A, EU3, EU5, TS1	CV4, EU4		
Rare (<3 percent)	CS1				

Q2

	Incidental (≤$30K)	Minor (>$30K)	Moderate (>$300K)	Major (>$3M)	Extreme (>$30M)
Almost Certain (>80 percent)					
Likely (51-80 percent)			CR3	CR1, CR2, CR2A, CR4	
Possible (21-50 percent)		CP6	CP3	CR6	CP1
Unlikely (3-20 percent)	EU6	EU1, EU1A, EU3	CP5, CV2, CV2A, CV3, CV4, CV6	CP4, CV1	
Rare (<3 percent)	CS1, TS1	EU4, EU5			

Q3

	Incidental (≤$30K)	Minor (>$30K)	Moderate (>$300K)	Major (>$3M)	Extreme (>$30M)
Almost Certain (>80 percent)					
Likely (51-80 percent)					
Possible (21-50 percent)		CP6	CP3, CP4, CR3	CR1, CR2, CR2A, CR4, CR6	CP1
Unlikely (3-20 percent)	EU6	EU1, EU1A, EU3, EU5	CP2, CV2, CV2A, CV3, CV4, CV6	CV1	
Rare (<3 percent)	CS1, TS1	EU4, EU5			

Q4

	Incidental (≤$30K)	Minor (>$30K)	Moderate (>$300K)	Major (>$3M)	Extreme (>$30M)
Almost Certain (>80 percent)					
Likely (51-80 percent)					
Possible (21-50 percent)			CP3, CR3, CR6	CP1, CR1, CR2, CR2A, CR4	
Unlikely (3-20 percent)		CP6, EU1, EU1A, EU3	CP4, CP5, CV2, CV2A, CV3, CV4, CV6	CV1	
Rare (<3 percent)	CS1, EU6, TS1	EU4, EU5			

Endnotes

1 ISACA®, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *www.isaca.org/cobit*

2 *Ibid.*

3 *Ibid.*

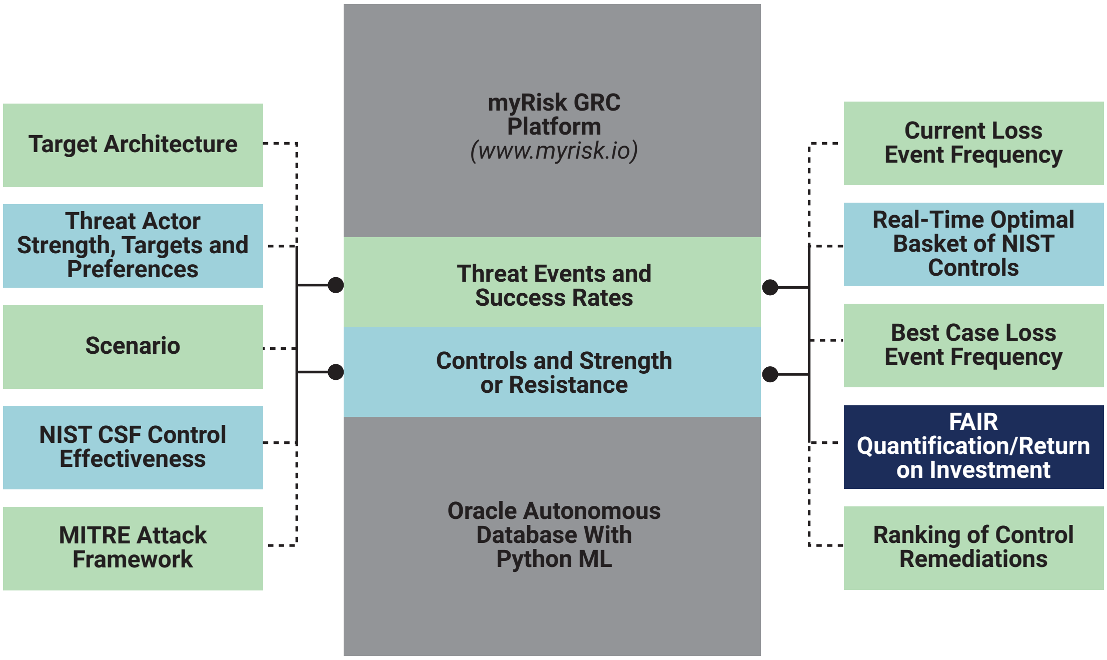
4 MITRE ATT&CK, *http://attack.mitre.org*

5 ISACA, *CRISC Review Manual, 7th Edition*, USA, 2021, *www.isaca.org/crisc-review-manual*

6 International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), ISO/IEC 27005:2011 *Information*

FIGURE 21

myRISK Machine Learning Framework


Target Architecture
Threat Actor Strength, Targets and Preferences
Scenario
NIST CSF Control Effectiveness
MITRE Attack Framework
myRisk GRC Platform (www.myrisk.io)
Threat Events and Success Rates
Controls and Strength or Resistance
Oracle Autonomous Database With Python ML
Current Loss Event Frequency
Real-Time Optimal Basket of NIST Controls
Best Case Loss Event Frequency
FAIR Quantification/Return on Investment
Ranking of Control Remediations

Technology—Security Techniques—Information Security Risk Management, Switzerland, 2011, *https://www.iso.org/standard/56742.html*

7 Protiviti, *Moving Beyond the Heat Map: Making Better Decisions With Cyber Risk Quantification*, USA, 2018, *www.protiviti.com/sites/default/files/united_states/user_generated/pro_1018_pov_107187-quantifycybersecurityrisk_nam_eng_unsec.pdf*

8 ISACA, *Cyberrisk Quantification*, USA, 2021, *www.isaca.org/cyberrisk-quantification*

9 National Institute of Standards and Technology (NIST), Cybersecurity Framework, USA, *www.nist.gov/cyberframework*

10 RAND Corporation, "Delphi Method," *https://www.rand.org/topics/delphi-method.html*

11 Australian Government and Australian Cyber Security Centre, "Essential Eight," *https://www.cyber.gov.au/acsc/view-all-content/essential-eight*

12 RSA Security, *Three Essentials for Cyber Risk Quantification*, USA, *www.scribd.com/document/442421441/3-essentials-for-cyber-risk-quantification*

13 *Op cit* Protiviti

14 Ayres, D.; J. Schmutte; J. Stanfield; "Expect the Unexpected: Risk Assessment Using Monte Carlo Simulations," *Journal of Accountancy*, 1 November 2017, *https://www.journalofaccountancy.com/issues/2017/nov/risk-assessment-using-monte-carlo-simulations.html*

15 Alexander, R.; "Can the Analytical Hierarchy Process Model Be Effectively Applied in the Prioritization of Information Assurance Defense In-Depth Measures?—A Quantitative Study," Capella University, Minneapolis, Minnesota, USA, February 2017

16 *Op cit CRISC Review Manual*

17 Boehm, J.; N. Curcio; P. Merrath; L. Shenton; T. Stahle; "The Risk-Based Approach to Cybersecurity," McKinsey and Company, 8 October 2019, *www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity*

18 Mukhopadhyay, A.; S. Chaterjee; K. Bagchi; K. Kallol; P. Kirs; G. Shukla; "Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance," *Information System Frontiers*, vol. 21, iss. 5, 17 November 2017