In collaboration with Accenture

WORLD ECONOMIC FORUM

The Cyber Resilience Index: Advancing Organizational Cyber Resilience

WHITE PAPER

JULY 2022

Cover: @gonin/Gettyimages

Contents

Foreword

Jeremy Jurgens
Managing Director, World Economic Forum

Jim Guinn
Senior Managing Director, Security, Accenture

The World Economic Forum is committed to elevating cyber resilience and preparedness across the entire digital ecosystem. Published in January 2022, our inaugural *Global Cybersecurity Outlook* report identified a wide perception gap between business executives and cyber leaders on the cyber-resilience posture of their organizations. While 92% of surveyed business executives felt that cyber resilience is integrated into enterprise risk-management strategies, only 55% of cyber leaders agreed.

Understanding the impact of cyber risks on an organization is a complex but critical element of strengthening cyber resilience. There is a need for frameworks and tools to equip cyber leaders to understand and communicate prevailing cyber risks, and their impact, to senior leadership.

Developed in collaboration with the diverse community of the Centre for Cybersecurity and supported by Accenture, the Cyber Resilience Index seeks to serve as a reference framework to provide visibility and transparency on cyber-resilience practices across industries, peers and the supply chain.

Cyber resilience and its benefits should be clear to Boards and leadership. It is therefore important to translate the impact of the state of cyber resilience on business operations, strategy and continuity. We hope the Cyber Resilience Index will help cyber leaders engage better with senior leadership within their organizations to position cyber resilience as a strategic imperative.

Executive summary

> Cyber resilience is the ability of an organization to transcend any stresses, failures, hazards and threats to its cyber resources within the organization and its ecosystem, such that the organization can confidently pursue its mission, enable its culture and maintain its desired way of operating.

> The reward for making cyber resilience part of our ethos is greater opportunity to take healthy risks, innovate and responsibly capture the value of tomorrow's digital economy.

The World Economic Forum Centre for Cybersecurity – in collaboration with the Cyber Resilience Index working group and in partnership with Accenture – developed the global Cyber Resilience Index (CRI). The CRI provides public- and private-sector cyber leaders with a common framework of best practice for true cyber resilience, a mechanism to measure organizational performance, and clear language to communicate value. The CRI is also a universal, impartial medium through which organizations in every sector around the globe can evaluate and engage with their ecosystem partners to create a more cyber-resilient digital network.

The World Economic Forum anticipates that digital transformation as part of the Fourth Industrial Revolution will create an estimated $100 trillion of additional value for the world economy by 2025.[1] The global pandemic only accelerated that revolution when it disrupted and then redesigned the fabric of our digital lives; it also offered a prudent pause to renew focus on the essential principles for responsible development and the use of a digital environment for the future. Given the power of this opportunity, digital creation that is unsustainable, exclusive or untrustworthy – no matter how valuable – is unacceptable. It is time to re-architect our approach to creating systemic cyber resilience for the future.

To succeed, it is imperative to design, build and manage for cyber resilience, and then to get the fundamentals right. Fundamental cyber resilience must be integral not only to technical systems but also in teams, the organizational culture and the daily way of working. These topics have long been underrepresented and conflated with other principles in cyber programmes. Within organizations and among their ecosystems, cyber resilience must be a pervasive mindset upheld by a holistic approach. The approach to cyber resilience must also be free from the fear-driven limitations caused by merely preserving the status quo, which are so often then followed by attempts to return to a demonstrably fragile state when disruption predictably happens. The reward for making cyber-resilience part of the ethos is greater opportunity to take healthy risks, innovate and responsibly capture the value of tomorrow's digital economy.

Yet today, the numbers and current events indicate that much work is needed to close the capability and performance gap in cyber-resilience among industry ecosystems and within individual organizations. The World Economic Forum's *Global Cybersecurity Outlook 2022* report found that only 19% of cyber leaders feel confident that their organizations are cyber-resilient, indicating that a large majority knows their organizations lack the cyber resilience they need to be commensurate with their risk.[2] Further, the report found that 58% of respondents feel their partners and suppliers are less resilient than their own organization, and 88% are concerned about the cyber resilience of small and medium-sized enterprises in their ecosystem. In another report, 81% of respondents said that "staying ahead of attackers is a constant battle and the cost is unsustainable", compared with 69% in 2020.[3]

This indicates that as organizations, ecosystems, supply chains and relationships become more connected and interdependent and the pace of change accelerates, not only is resilience lagging, but a cohesive approach for how to architect for resilience is lacking. It has become increasingly clear that despite this interconnection, no alignment to transcend disruptive cyber events exists.

The four primary reasons cyber resilience is limited in ecosystems today are that many organizations:

- Have a narrow perspective of cyber resilience, focused mainly on security response and recovery
- Lack a common understanding as to what a complete cyber-resilience capability should include
- Find it challenging to accurately measure organizational cyber-resilience performance or communicate its true value to business leadership
- Struggle to be transparent within their organization and with ecosystem partners about shortcomings in their cyber-resilience posture and their experiences with disruptive events.

The CRI addresses these limitations. Further, the CRI gives the world's cyber leaders – who are both drivers and beneficiaries of the digital economy – a blueprint to better build a more sustainable, inclusive and resilient digital environment of the future for everyone.

Introduction

This White Paper details two components, the Cyber Resilience Framework (CRF) and the Cyber Resilience Index (CRI), which guide organizations on their cyber-resilience journey. The CRF (and subsequently the CRI) was developed as a forward-looking solution to promote more effective practices across digital ecosystems. The CRF provides a clear and malleable foundation from which an organization can clearly define and understand what it means to have robust organizational cyber resilience. This will amplify the awareness of cyber-resilience best practices across industries and serve as a guidebook for those designing or strengthening their cyber-resilience approaches. Together, the CRF and CRI deliver a unique cyber-resilience blueprint to improve transparency and visibility and enable global trust across digital ecosystems and diverse industries.

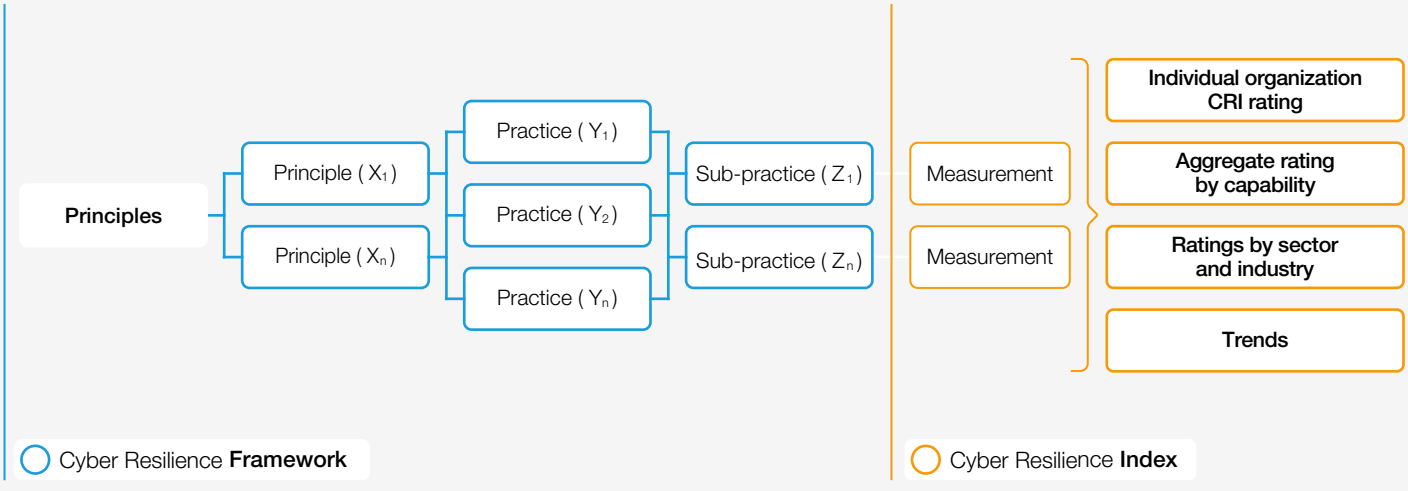
Establishing the Cyber Resilience Framework and Index

The CRF is a guide to best practice for building holistic cyber resilience in an organization. It consists of six key principles, associated practices and their sub-practices with which cyber leaders can clearly define healthy organizational cyber resilience. It serves as a standard, industry-agnostic framework with defined outcomes that can serve as a baseline to all organizations, regardless of geography or size.

Subsequently, the CRI is a tool to help organizations quantitatively measure their cyber resilience using measures of performance against best practices as laid out in the CRF. The CRI provides insights on organizational cyber-resilience maturity to participating organizations, increases general situational awareness within each industry and provides insights to public- and private-sector stakeholders. The CRI also identifies trends within and across industries that can enable organizations to benchmark their cyber resilience against their own industry as well as cross-industry within their entire ecosystem. Establishing a cyber-resilience benchmark is key to helping organizations assess and adjust their cyber resilience in a constantly evolving landscape.

Together, the CRF and CRI bring transparency to the current state of cyber resilience within an organization, and subsequently to its relationship to the broader ecosystem. The CRF is the foundation for the CRI. Using the CRF's principles and practices, the CRI is comprised of measurements of an organization's cyber resilience based on weighted indicators per principle, practice and sub-practice, which are calculated collectively to produce ratings for an organization at an individual level, ratings by sector and industry, and an aggregate rating by capability (Figure 1). When anonymized and taken together, measurements of cyber-resilience performance by capability at the organizational level further reveal trends within and across industries.

FIGURE 1 **How the Cyber Resilience Framework and Cyber Resilience Index relate to each other**

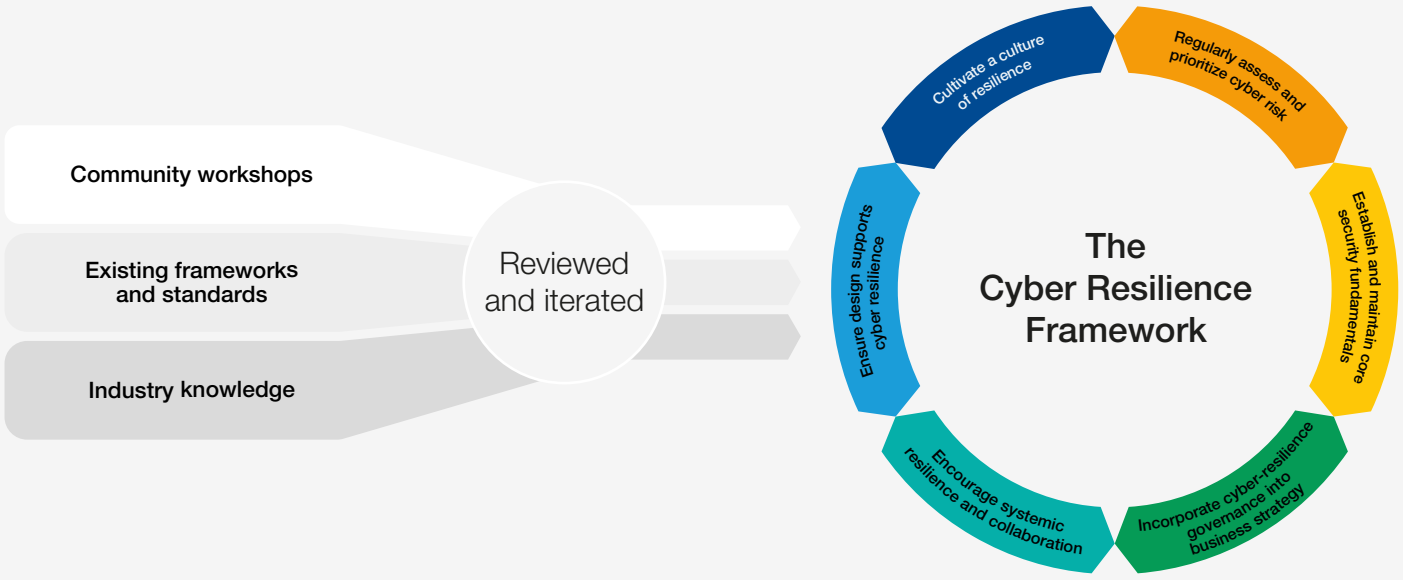


Source: World Economic Forum and Accenture

Methodology

To create a globally trusted source of strategic cyber-resilience insights entailed a highly collaborative and innovation-led approach, assembling a community of cyber leaders and experts in various industries, academia, civil society and international organizations. Through this approach (Figure 2), multiple workshops were conducted, questionnaires distributed and one-on-one interviews held with Cyber Resilience Index working group members. Internationally recognized cybersecurity and cyber-resilience frameworks were evaluated for common practices and elements required for a comprehensive cyber-resilience specific framework (see Figure 5). The goal is for the CRF to complement these existing frameworks rather than reinvent them. The community validated the CRF's principles and practices, considered strategies for data collection and ultimately arrived at the current iteration of the CRF and CRI.

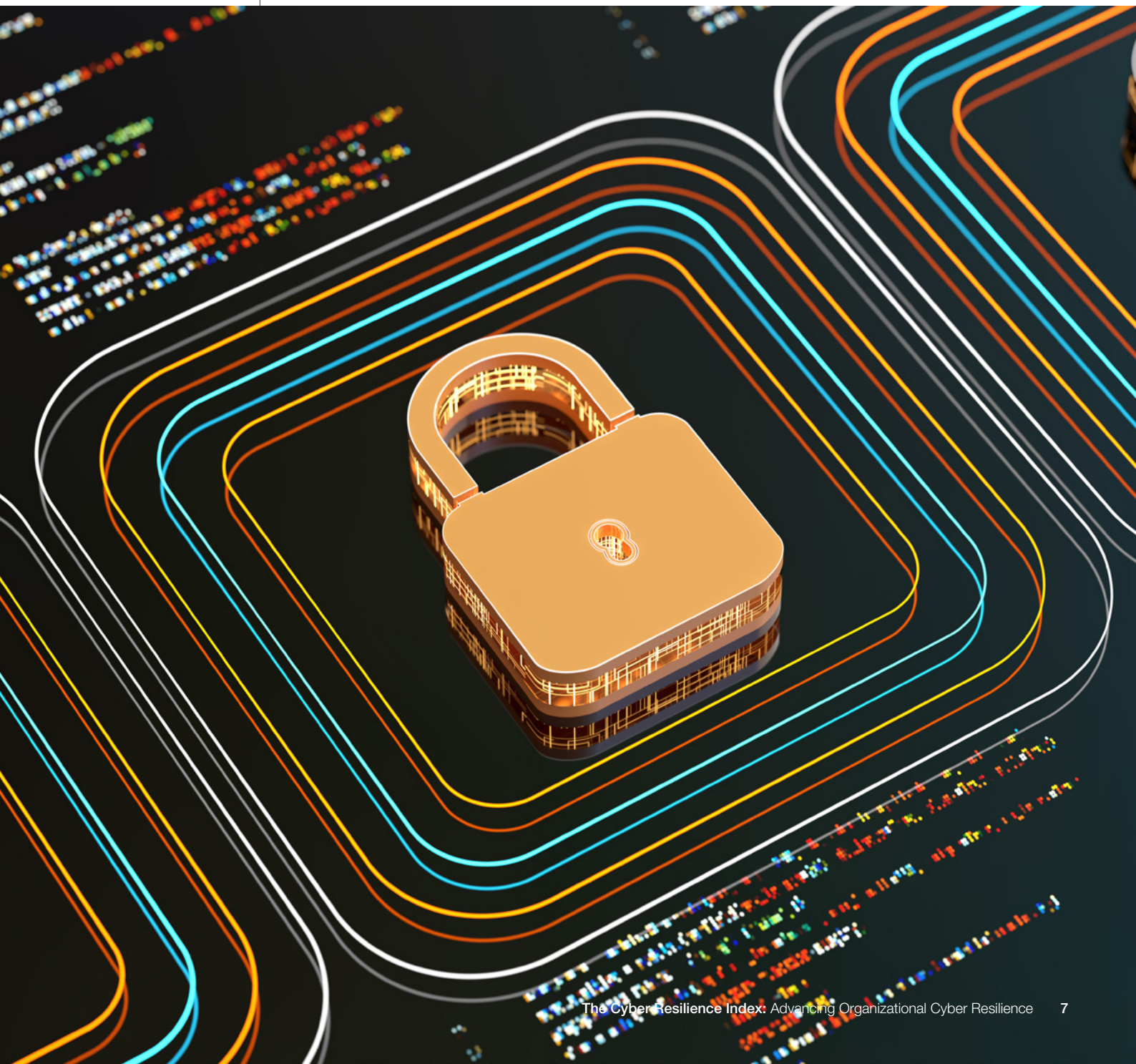
FIGURE 2 **The process for creating the Cyber Resilience Framework and Cyber Resilience Index with the community**



Source: World Economic Forum and Accenture

Below: @kupicoo/
Gettyimages

1 Establishing a framework for cyber resilience

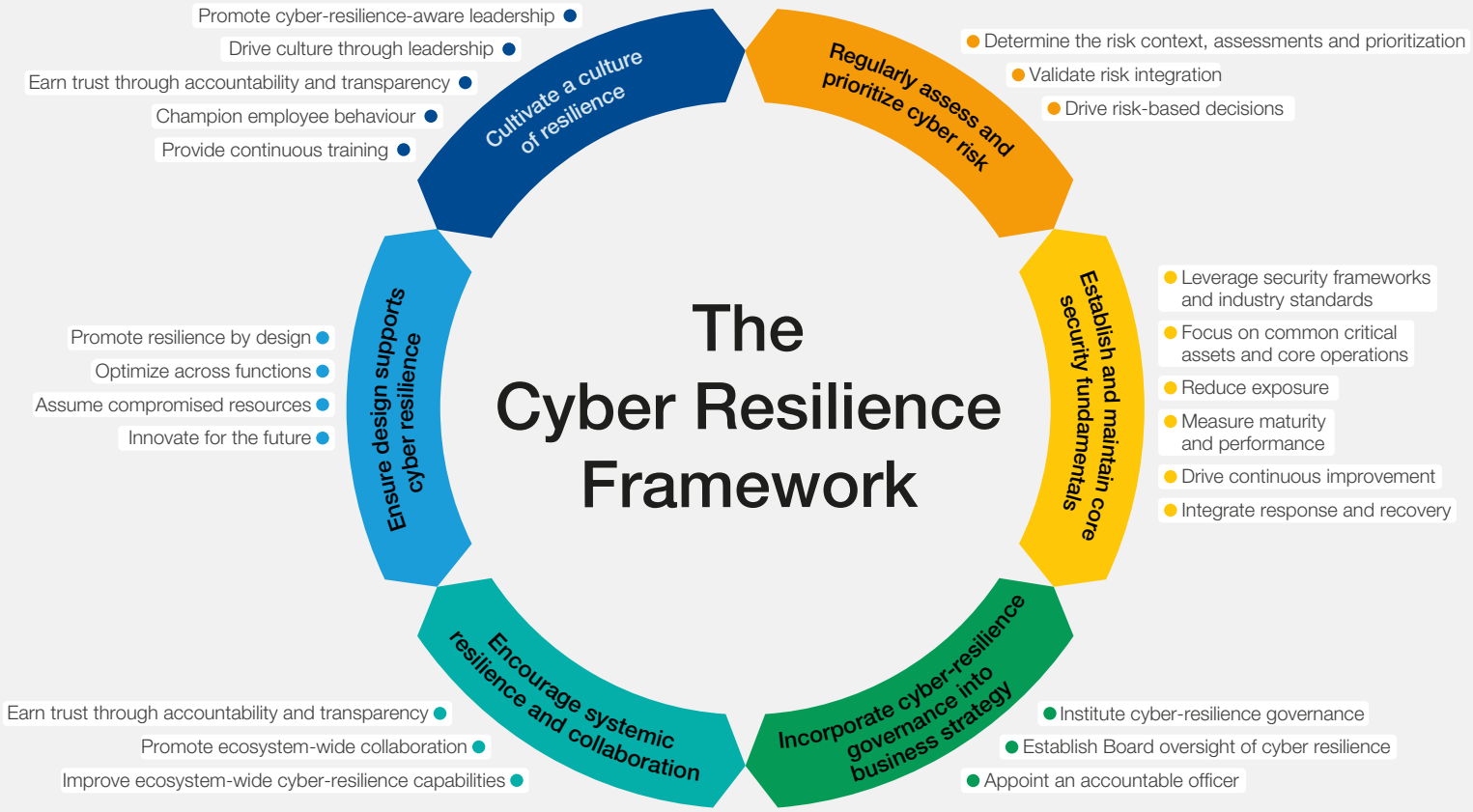


The CRF is the foundation and theory that drives the CRI. The CRF's principles, subsequent practices and sub-practices outline healthy organizational cyber resilience. This section details the entirety of the CRF.

Cyber Resilience Framework Principles

Each of the CRF principles is accompanied by a set of practices and sub-practices to further enable cyber leaders to develop and assess their cyber resilience (Figure 3).

FIGURE 3 **The Cyber Resilience Framework**



Source: World Economic Forum and Accenture

Principle: Regularly assess and prioritize cyber risk

Cyber-resilience management is driven directly by risk.

Practice	Sub-practice
Determine the risk context, assessments and prioritization: The organization is held accountable for understanding its role and interdependencies within the ecosystem, reporting on the systemic cyber risks posed itself and by the ecosystem upstream and downstream, and managing its cyber-resilience efforts accordingly.	– The organization maintains a map of its major ecosystem and supply chain interdependencies, including a value chain analysis, use cases/scenarios and associated systemic impact assessments. – At least annually, the organization reports externally on the state of its analysis on cyber-resilience interdependency in its ecosystem and its associated management efforts.
Validate risk integration: The organization's business risk tolerance, cyber value-at-risk and cyber exposure are integrated into the overall business strategy, enterprise-wide risk management and associated governance structure, which then drive budgeting and resource allocation.	– At least annually, and when material change occurs, the organization conducts a quantifiable assessment of its risk, including cyber value-at-risk and cyber exposure, as compared to its risk tolerance. – The organization formally feeds its cyber-risk assessment results into its budgeting and resourcing decisions at least annually and as necessary when events cause the cyber-risk calculus to change, allocating the appropriate resources to the highest priority cyber-resilience areas.
Drive risk-based decisions: Those responsible for managing the organization's cyber resilience are empowered and have clear channels to communicate to decision-makers circumstances that could exceed the organization's tolerance thresholds. Management is accountable for taking risk-based decisions accordingly.	– All employees have a recognized reporting mechanism and clear escalation channels to management to report situations in a timely manner that are potentially high risk for the organization's cyber resilience. – Management conducts after-action reviews on notable cyber-resilience decisions from incidents and major breaches, or tabletop exercises to ensure they were consistent with risk-based resilience principles and criteria and the situational context. Corrections are made to improve future decision-making.

Principle: Establish and maintain core security fundamentals

Core organizational mission functions and supporting systems are secure in the face of unexpected attacks.

Practice	Sub-practice
Leverage security frameworks and industry standards: The organization uses recognized security frameworks, industry standards and compliance regulations, and is objectively measured against them annually.	– Annually, the organization is objectively measured against a recognized national or international security framework (e.g. National Institute of Standards and Technology [NIST] Cybersecurity Framework, International Organization for Standardization [ISO] 27001 on how to manage information security, NIST Special Publication 800-53 on security and privacy controls, UK Cyber Assessment Framework, etc.). – Annually, the organization is objectively measured against all industry regulatory standards for security, resilience and privacy which it is subject to (e.g. the Health Insurance Portability and Accountability Act, New York Department of Financial Services Cybersecurity Regulation, Cybersecurity Capability Maturity Model [C2M2], North American Electric Reliability Corporation Critical Infrastructure Protection, etc.).
Focus on common critical assets and core operations: The organization applies its security capabilities to prioritize its critical assets and core operations by defining a criticality rubric, grading each asset or operation against it, and applying or adding security capabilities accordingly.	– Assets and operations are classified as common, critical and/or core to essential cyber resilience according to formal criteria for which cyber-resilience capabilities are accordingly applied differentially. – The organization maintains a register – in a central enterprise asset management platform – of all assets and operations rated as common, critical and/or core to essential cyber resilience.
Reduce exposure: The organization ensures that threats can only target a small set of assets that can more effectively be monitored and defended by reducing the attack surfaces, configuring resources to isolate issues, and limiting cascading or compounding effects.	– The organization is committed to principles (e.g. least privilege, network segmentation, footprint reduction) that reduce its unnecessary exposure to intentional and unintentional threats and hazards. – Architecture and configuration for information technology, operational technology and business unit assets and/or processes reduce unnecessary exposure and limit cascading or compounding impacts.

Measure maturity and performance: The organization tracks security maturity and performance through metrics and the continuous improvement of baselines.	– Management formally defines and centrally tracks a set of maturity and performance metrics for meeting minimum security standards as they relate to the organization's overall cyber resilience. – At least quarterly, management formally reports to the accountable executive leadership on defined security metrics and trends over time in relation to cyber resilience.
Drive continuous improvement: Operations include mechanisms to continuously improve based directly on capability gaps against applicable frameworks, standards of practice, regulatory requirements and the organization's evolving risk landscape.	– Personnel with responsibility for managing cyber resilience execute a formally documented action plan of improvement initiatives, updated at least annually. – Management reports quarterly on performance against success criteria for accomplishing improvement initiatives on the action plan.
Integrate response and recovery: Organizational response and recovery operations for security issues are integrated into business as usual, do not disrupt normal unaffected operations and continuously improve as part of optimizing resilience.	– The organization tracks economic and performance progress for its response and recovery actions through metrics, and continuously updates its baselines. – The organization reviews its response and recovery metrics on a predefined cadence and develops action plans accordingly, which are managed to completion.

Principle: Incorporate cyber-resilience governance into business strategy

Cyber resilience is governed holistically across the enterprise from the top-down according to a cohesive strategy aligned to the organization's enterprise goals.

Practice	Sub-practice
Institute cyber-resilience governance: Management implements comprehensive cyber-resilience governance, which ensures the alignment and interoperability of cyber resilience across information technology, operational technology, digital transformation, business continuity and physical security.	– The organization has an established cyber-resilience governance structure, organization chart, operating model and clearly defined roles with accountability and responsibility. – The organization has a cohesive cyber-resilience strategy, including defined resilience principles; codified cross-disciplinary collaboration, interactions and practices; and enforceable policies.
Establish Board oversight of cyber resilience: The Board takes ultimate accountability for the oversight of cyber resilience, although it may delegate primary oversight activity to a committee (e.g. risk committee, cyber-resilience committee).	– The Board of Directors' mandate to take accountability for cyber-resilience oversight and any subsequent delegation is officially documented, including accountability for setting resilience risk tolerances, managing impact and adding organizational value through resilience. – The Board of Directors receives regular briefings on the state of cyber resilience as compared to its goals, and provides clear direction and knowledgeable guidance to management accordingly.
Appoint an accountable officer: One corporate officer is accountable for the organization's ability to manage cyber resilience and for implementing cyber-resilience goals. The accountable officer has regular Board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.	– The role of the accountable officer is formally defined and documented with clearly understood expectations and obligations. The designated officer is appointed in writing and understands the responsibilities. – The organization has clear mechanisms for providing the accountable officer ready access to each of the following: communication with the Board of Directors; empowerment over cyber-resilience strategy, management and enforcement actions; cyber-resilience expertise and executive training; the acquisition of personnel, financial and technology resources.

Principle: Encourage systemic resilience and collaboration

The organization understands the interdependencies within its ecosystem, engages with the other organizations and fulfils its role in maintaining ecosystem resilience.

Practice	Sub-practice
Earn trust through accountability and transparency: The organization maintains transparency in its practices, operations and failings with its ecosystem partners and shares best practices to promote a more resilient collective.	– Responsibility and accountability for aggregating and communicating the organization's cyber-resilience practices to third parties has been assigned to an individual role or group. – Within the boundaries of information-sharing and non-disclosure agreements, the organization participates in cyber-resilience benchmarking activities and best-practice reviews with key ecosystem partners.
Promote ecosystem-wide collaboration: Management creates a culture of collaboration, sets strategic objectives for information-sharing, and understands and mitigates cyber risks in the ecosystem. The organization also actively collaborates with industry peers and policy-makers.	– The organization has established information-sharing agreements with key ecosystem partners to facilitate ecosystem resilience collaboration. – Collaboration governance and cadence are established to provide clear expectations of what can and cannot be shared, including roles and responsibilities for collaboration, the data release approval process and data protection requirements.
Improve ecosystem-wide cyber-resilience capabilities: The organization continuously improves collective cyber-resilience capabilities together with other members of the ecosystem to raise the overall standard of practice. These capabilities appropriately balance innovation, preparedness, protection, response and recovery capabilities.	– The organization has mapped its cyber-resilience value chain and understands the role, criticality and dependencies of itself and each entity in its ecosystem to best engage with developed and implemented mechanisms to assess the cyber resilience of ecosystem partners/vendors/third parties based on their criticality to the organization's essential business needs. – The organization participates in working groups, standards development committees, industry associations and other collaboration forums with its ecosystem partners focused on improving collective maturity and practice.

Principle: Ensure design supports cyber resilience

Agility and adaptability are integral to the organization's cyber-resilience strategy, design and execution, which improve continuously to optimize resilience.

Practice	Sub-practice
Promote resilience by design: Leadership commits to resilience by design in its cyber teams, processes and technologies, then requires management to implement such designs and document progress.	– The organization has clearly defined and documented principles and objectives for the resilient architecture of teams, processes and technology assets, including these assets' interrelated systems, and ensures they follow the principle of least exposure to reduce attack surfaces. – Existing teams, processes, technologies and interrelated systems are reviewed against resilience principles and objectives at least annually. New assets are evaluated against resilience principles and objectives at each stage of establishment, start-up and/or development.
Optimize across functions: Operations are optimized for resilience in coordination with the security, information technology, engineering, site operation and business units.	– Operations under existing people, processes and technology assets for managing cyber resilience are reviewed and rationalized between the security, information technology, engineering, site operation and business units at least annually to optimize effectiveness and efficiency. New assets are developed and implemented with the same optimization in mind. – Resilience scenarios are developed through cross-organization collaboration with all relevant stakeholders. Resilience drills and stress tests are performed annually with cross-organization stakeholder participation. Opportunities for improvement are documented and incorporated back into resilience strategy and operating procedures.
Assume compromised resources: The organization enables its cyber resources to absorb adverse events as part of normal operations and continue to meet performance and quality requirements.	– Performance expectations, quality standards and resource allocation for teams, processes and technology factor in irregular input and disruptive events by design so they do not interrupt the normal operational tempo. – The organization tracks metrics on irregular input and disruptive events to determine their effect on performance and quality over time as the threat, hazard and business landscape changes.

Innovate for the future: Cyber R&D and innovation efforts are holistic across people, process and technology and are designed to be scalable, flexible and systemic – directly tied to enabling the organization's resilience strategy, funded appropriately.	– The organization allocates resources for research, development and innovation initiatives focused on future resilience against horizon threats and hazards, and to add value to forward-looking business priorities. – Resilience research, development and innovation initiatives are consistently funded and resourced, and actively managed as part of the regular budgeting process, commensurate with the organization's projected cyber risk and value creation.

Principle: Cultivate a culture of resilience

Employees are empowered to understand and embody cyber-resilient behaviours.

Practice	Sub-practice
Promote cyber-resilience-aware leadership: Cyber-resilience leadership has the expertise to manage the organization's cyber resilience according to best practice and is incentivized to advance its expertise with changes in the landscape.	– Leadership has job performance goals related to the effectiveness of the organization's cyber resilience. – The organization hires leadership taking into consideration their cyber-resilience experience and background, in addition to their cybersecurity experience.
Drive culture through leadership: Leadership sets the tone and puts the organizational mechanisms in place to drive a culture of accountability for cyber resilience at every level of the organization.	– The organization has clearly defined, documented and communicated rewards, criteria for success, penalties, consequences and corrective action measures for all employees associated with cyber-resilient behaviour, which are reinforced through regular training. – Leadership clearly demonstrates to the workforce living a culture of cyber resilience through their own words and personal actions, including the adherence to policies and procedures, daily interactions and a commitment to partake in learning opportunities to understand the evolving cyberthreat landscape, and submitting to consequences and corrective action when warranted.
Earn trust through accountability and transparency: Management regularly and clearly communicates to its workforce about its cyber-resilience strategy, practices, operations, successes and failings. This helps to build and maintain trust, foster openness and engender pride of ownership in organizational success through cyber resilience.	– The organization measures and tracks metrics for assessing the culture of resilience, transparency and accountability (e.g. conducting employee engagement surveys and collecting violation statistics over time). The organization follows through on delivering its stated rewards and consequences. – Leadership regularly communicates to the workforce about the health of the culture of cyber resilience, transparency and accountability, including positive and negative statistics, organizational case studies of rewards and consequences, and human-interest stories.

Champion employee behaviour: Employees clearly understand expected cyber-resilient objectives, feel a sense of ownership for the organization's cyber resilience, and are empowered to exercise cyber resilient behaviours in their daily interactions without fear of retaliation.	– Employees have access to cyber-resilience training that defines company expectations and empowers the employees to identify and communicate threats. – The organization has job performance goals related to promoting positive cyber-resilient behaviours in employees.
Provide continuous training: Employees are taught cyber-resilience concepts, the importance of cyber resilience and its role in their daily responsibilities, and continuously exercise these lessons, which evolve with the cyber-resilience landscape.	– Staff in roles that are deemed critical to core business functions should be given opportunities to further enhance cyber-resilience concepts through additional training, or through performing tabletop exercises. – The training should be presented in a format that allows an employee to be an actively engaged participant.

Below: @gilaxia/
Gettyimages

2

The path forward for the Cyber Resilience Index

The World Economic Forum encourages all community members worldwide to use the CRI, live its principles and adopt its practices in their organizations. The CRI is developed with agility in mind and is designed to improve as more cyber leaders and their organizations use it. It is industry and geography agnostic, and its application can be achieved swiftly. Each executive and practitioner can introduce constructive improvements to customize the CRI to fit their specific needs.

The main goal of the CRI is to provide cyber leaders with a tool and the visibility to understand their organization's and their ecosystem's cyber-resilience level. In doing so, leaders and executives will learn where their organization needs to improve to reach the next level of resilience. Much like knotted ropes, healthy and diverse organizations can become the strongest, best-performing versions of themselves when they are put under pressure. That is the power of real resilience by design. Similarly, as organizational cyber leaders and other champions of cyber-resilience exercise the CRI and its components, it will gain from the experience and expertise of the community and provide opportunities to continuously improve.

Conclusion

The CRI is but one of the Centre for Cybersecurity's endeavours to address systemic cyber challenges and improve digital trust. By ensuring that the CRI is informed by and builds upon the Centre's previous work[4] and is linked to other efforts, it is possible to help the whole body of practice become greater than the sum of these individual initiatives.

For example, through the Forum's leadership on the Cyber Resilience Pledge, as described in an article in *Modern Diplomacy*, "leading oil and gas stakeholders are calling for industry to come together to stop harmful cyberattacks. The action is in response to major security breaches in the past two years that have highlighted the vulnerability of critical infrastructure. At the World Economic Forum Annual Meeting 2022, 18 companies came together to take a Cyber Resilience Pledge, in recognition of the fact that much more collective preparedness is needed. The pledge aims to mobilize global commitment towards strengthening cyber resilience across industry ecosystems. Organizations endorsing the pledge commit to collaborating and taking collective action on cyber resilience. Launched with the support of organizations engaged in the World Economic Forum's Cyber Resilience in Oil and Gas initiative, the pledge seeks to empower organizations to take concrete steps to enhance cyber resilience across their industry."[5]

Notable examples like this notwithstanding, much still needs to be done. As the CRI continues to scale and improve, much work is also needed to measure cyber resilience at the ecosystem level.

Among other factors, future work should:

– Establish common indicators of eco-systemic cyber-resilience performance

– Measure the causation and correlation of resilience among multiple members of an ecosystem, as well as between ecosystems across geographies and sectors

– Calculate centrality to determine if and how members of an ecosystem carry greater weight and subsequently have more power than others to influence the resilience of the whole ecosystem positively and negatively.

To responsibly capture and sustain the value of the future digital economy, each and every organization must transcend cyber disruption. The Fourth Industrial Revolution means that systemic interdependence is both the risk and the reward of the opportunity, because value and impact on the future are exponential rather than cumulative, and every day counts.

Appendices

1 CRI methodology

The CRI linear aggregator combines measures relating to each CRF sub-practice to create the CRI score. The CRI score for an organization is aggregated from 64 measures of performance, collected for each organization with a self-assessment, with all measurements matched to their respective CRF sub-practices (Figure 4). The selection of measures is determined by the relevance to the sub-practice, the likelihood of an organization having the ability to provide a response, and the direct relevance to cyber-resilience performance.

To allow for the aggregation of measurements with different scales and magnitudes, the CRI adopts a min-max method to transform a score. Scores are transformed to scale between 0 and 100 and then aggregated equally across each sub-practice, practice and principle.

Each indicator is rescaled according to the following formula:

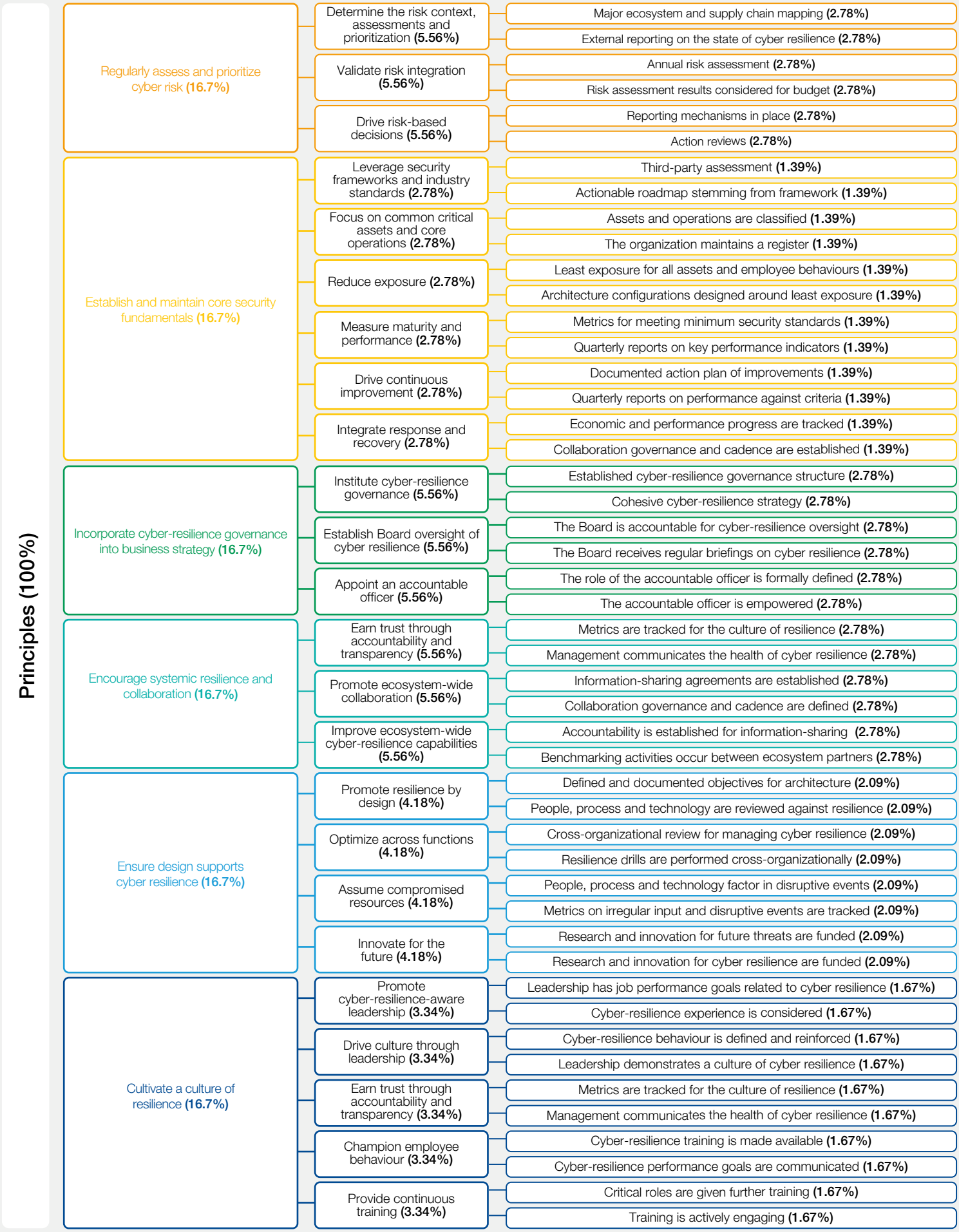
$$Measurement\ score_c = \left(\frac{value_c - min_c}{max_c - min_c} \text{ X } 100 \right)$$

where value c is the measure of organization c, min is the lowest value for the measure and max corresponds to the best possible outcome. Each measurement score is equally weighted when aggregated to the practice it represents, as with the practice to principle, and the principle to organizational CRI score. The organizational scores of an industry are averaged to create the industry CRI score. Figure 4 shows the full list of the weights.

As an example, if an organization were assessing itself against a sub-practice with five possible responses, with the first response having a score of zero (0) and the last having a score of four (4), and the organization determines that the response that best characterizes it corresponds with a score of two (2), its score for that sub-practice would be calculated as follows:

$$Example\ measurement\ score_c = \left(\frac{2 - 0}{4 - 0} \text{ X } 100 \right) = 50$$

FIGURE 4 | **The taxonomy of the Cyber Resilience Index**



Source: World Economic Forum and Accenture

Figure 5 shows the internationally recognized cybersecurity and cyber-resilience frameworks evaluated for common practices and elements required for a comprehensive cyber-resilience specific framework.

FIGURE 5 **Mapping of the Cyber Resilience Framework against other international frameworks**

	Principles					
	Regularly assess and prioritize cyber risk	Establish and maintain core security fundamentals	Incorporate cyber-resilience governance into business strategy	Encourage systemic resilience and collaboration	Ensure design supports cyber resilience	Cultivate a culture of resilience
MITRE Cyber Resiliency Design Principles	✓	✓	✗	✓	✓	✗
Forum Board Principles	✓	✓	✓	✓	✗	✓
Forum Board Principles - Oil and Gas	✓	✗	✓	✓	✓	✗
US Cyber-security & Infrastructure Security Agenda (CISA) Cyber Resilience Review	✓	✓	✗	✓	✗	✓
Scotland Cyber-Resilience Framework (Annex A)	✓	✓	✓	✗	✓	✓
National Institute of Standards and Technology (NIST) SP 800-160 V2 Rev.1	✗	✓	✗	✗	✓	✗
NIST SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations	✓	✓	✗	✓	✓	✓
International Organization for Standardization (ISO) 27001 Information Security Management	✓	✓	✓	✗	✓	✓
UK National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)	✓	✓	✓	✗	✓	✓
Center for Internet Security (CIS) Critical Security Controls (CIS Controls)	✗	✓	✗	✓	✓	✓

Source: World Economic Forum and Accenture

Figure 6 shows the Cyber Resilience Framework's key principles, associated practices and sub-practices in greater detail.

FIGURE 6 **The fully expanded Cyber Resilience Framework**

	Principles					
	Regularly assess and prioritize cyber risk	**Establish and maintain core security fundamentals**	**Incorporate cyber-resilience governance into business strategy**	**Encourage systemic resilience and collaboration**	**Ensure design supports cyber resilience**	**Cultivate a culture of resilience**
Practices	**Validate risk integration**	**Leverage security frameworks and industry standards**	**Institute cyber-resilience governance**	**Improve ecosystem-wide cyber-resilience capabilities**	**Promote resilience by design**	**Provide continuous training**
Sub-Practices	Annual risk assessment	Measured against recognized security frameworks	Established cyber-resilience governance structure	Cyber-resilience value chain is mapped	Defined and documented objectives for architecture	Critical roles receive further training
Sub-Practices	Risk assessment results considered for budget	Measured against industry regulatory standards	Cohesive cyber-resilience strategy	Participation in working groups and collaborative forums	People, process and technology are reviewed against resilience	Training is actively engaging
Practices	**Drive risk-based decisions**	**Reduce exposure**	**Establish Board oversight of cyber resilience**	**Promote ecosystem-wide collaboration**	**Optimize across functions**	**Drive culture through leadership**
Sub-Practices	Reporting mechanisms in place	Least exposure for all assets and employee behaviours	The Board is accountable for cyber-resilience oversight	Information-sharing agreements are established	Cross-organizational review for managing cyber resilience	Cyber-resilience behaviour is defined and reinforced
Sub-Practices	Action reviews	Architecture configurations designed around least exposure	The Board receives regular briefings on cyber resilience	Collaboration governance and cadence is defined	Resilience drills are performed cross-organizationally	Leadership demonstrates a culture of cyber resilience
Practices	**Determine the risk context, assessments and prioritization**	**Drive continuous improvement**	**Appoint an accountable officer**	**Earn trust through accountability and transparency**	**Innovate for the future**	**Champion employee behaviour**
Sub-Practices	Major ecosystem and supply chain mapping	Documented action plan of improvements	The role of the accountable officer is formally defined	Accountability is established for information-sharing	Research and innovation for future threats are funded	Cyber-resilience training is made available
Sub-Practices	External reporting on the state of cyber resilience	Quarterly reports on performance against criteria	The accountable officer is empowered	Benchmarking activities occur between ecosystem partners	Research and innovation for cyber resilience are funded	Cyber-resilience performance goals are communicated
Practices		**Focus on common critical assets and core operations**			**Assume compromised resources**	**Earn trust through accountability and transparency**
Sub-Practices		Assets and operations are classified			People, process and technology factor in disruptive events	Metrics are tracked for the culture of resilience
Sub-Practices		The organization maintains a register			Metrics on irregular input and disruptive events are tracked	Management communicates the health of cyber resilience
Practices		**Measure maturity and performance**				**Promote cyber-resilience-aware leadership**
Sub-Practices		Metrics for meeting minimum security standards				Leadership has job performance goals related to cyber resilience
Sub-Practices		Quarterly reports on key performance indicators				Cyber-resilience experience is considered
Practices		**Integrate response and recovery**				
Sub-Practices		Economic and performance progress are tracked				
Sub-Practices		Metrics are reviewed and action plans are established				

Source: World Economic Forum and Accenture

2 Glossary of key terms

Cyber exposure
An organization's hazard and threat landscape, prominence in the industry, criticality in the ecosystem, reliance on supply chain/ecosystem, and whether the organization is or is not a critical infrastructure provider.

Cyber resilience
An organization's ability "to transcend (anticipate, withstand, recover from and adapt to) any stresses, failures, hazards and threats to its cyber resources within the organization and its ecosystem, such that the organization can confidently pursue its mission, enable its culture and maintain its desired way of operating".[6]

Cyber risk
The value that an organization's cyber resources have to its mission, objectives, culture and operations and that of its ecosystem, as compared to the exposure and likelihood of those cyber resources being negatively impacted.

Cybersecurity
An organization's ability to maintain the confidentiality, integrity, availability and non repudiation of its cyber resources under normal and adverse conditions.

Cyber value-at-risk
An organization's business objectives, ways of working, critical functions, key assets and measurement of their concentration and/or diversity.

Ecosystem
A group of organizations that consistently interact with each other to provide goods or services as part of each organization's operations to fulfil its core mission; ecosystems can be made up of any combination of third parties, service providers, supply chain partners, consumers and other organization-to-organization relationships, including within the same sector and across sectors.

Fourth Industrial Revolution
On par with the three previous revolutions, a "fundamental change in the way we live, work and relate to one another"; "a new chapter in human development, enabled by extraordinary technology advances".[7]

Organization
A cohesive entity with a defined mission and structure regardless of industry and size, and inclusive of government agencies.

3 Acknowledgements

Carlos Aguirre
Security Manager, Accenture

Noura Alajmi
Head, Cybersecurity Awareness and Behaviour Management, Saudi Aramco

Sara Alghunaim
Staff Engineer, Research and Innovation, Saudi Information Technology Company

Alanood Alshehry
Head, Cybersecurity Strategy Realization Office, Saudi Aramco

Mick Ankrom
Chief Resiliency Officer, Bank of America

Darren Argyle
Group Chief Information Security Risk Officer, Standard Chartered Bank

Jatin Arora
Global Head of Governance, Risk and Compliance, HCL Technologies

Neelakarun Asari
Director, Security of Things, HCL Technologies

Giacomo Assenza
Cybersecurity Research Officer, International Telecommunication Union (ITU)

Andrea Barrios Villarreal
External Relations Manager, International Organization for Standardization (ISO)

Marwan Ben Rached
Cybersecurity Coordinator, International Telecommunication Union (ITU)

Christophe Blassiau
Senior Vice-President, Cybersecurity, and Global Chief Information Security Officer, Schneider-Electric

Maya Bundt
Head, Cyber and Digital Solutions, Swiss Reinsurance Company

Jose Manuel Cabrera Pozuelos
Head, Cyber Risk and Governance, Repsol

Perry Carpenter
Chief Evangelist and Strategy Officer, KnowBe4

Pedro Caruso
Managing Director, and Head, Oil and Gas Downstream, Accenture

Francesco Chiarini
Global Lead, Cyber Resilience, Standard Chartered Bank

Sadie Creese
Professor of Cybersecurity, University of Oxford

Henry Cuschieri
Technical Group Director, International Organization for Standardization (ISO)

Jacky Fox
Managing Director, Security, Accenture

Craig Froelich
Chief Information Security Officer, Bank of America

Javier Garcia Quintela
Chief Information Security Officer, Repsol

Jim Guinn
Senior Managing Director, Global Cyber Security Lead, Accenture

Randy Herold
Chief Information Security Officer, ManpowerGroup

Mark Hughes
President, Security, DXC Technology

Jacqueline Jayn
Security Awareness Advocate, APAC Region, KnowBe4

Jack Jones
Chairman, Fair Institute

Lydia Kostopoulos
Senior Vice-President, Emerging Tech Insights, KnowBe4

Sigmund Kristiansen
Chief Information Security Officer, Aker BP

Javvad Malik
Lead Security Awareness Advocate, KnowBe4

Heather Moye
Lead International Affairs Advisor, Europe Portfolio, Cybersecurity and Infrastructure Security Agency (CISA)

Mark Orsi
President, Global Resilience Federation

Haider Pasha
Regional Chief Security Officer, Emerging Markets, Palo Alto Networks

Mahesh Periasamy
Director, Identify Governance and Administration, Baker Hughes Energy Services

Adeline Piotrowski
International Affairs Advisor, Cybersecurity and Infrastructure Security Agency (CISA)

Jim Pruitt
Principal Director, Accenture

Rahul Rathore
Deputy Manager, IT, Vedanta

Ronald Ross
Fellow, National Institute of Standards and Technology (NIST)

Hart Rossman
Director, Global Security and Infrastructure Practice, Amazon Web Services

Basim Al-Ruwaii
Chief Information Security Officer, Saudi Aramco

Anna Sarnek
Director, Risk Solutions, SecurityScorecard

Anina Schwarzenbach
Fellow, Belfer Center for Science and International Affairs, Harvard University

Scott Stransky
Head, Cyber Risk Analytics Center, Marsh McLennan

Veronica Tan
Director, Safer Cyberspace, Cyber Security Agency of Singapore

Kevin Thacker
Head, Support to Cyber Regulation, National Cyber Security Centre (NCSC)

Darren Thomson
Vice-President and Head, Cyber Security Strategy, CyberCube

Rigo Van den Broeck
Executive Vice-President, Cyber Security Product Innovation, Mastercard

Kevin Watkins
Global Head, Cyber Resilience and Strategy, Standard Chartered Bank

Mike Wilkes
Chief Information Security Officer, SecurityScorecard

Andreas Wolf
Chairman, ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy, International Organization for Standardization (ISO)

Contributors

World Economic Forum

Gretchen Bueermann
Research and Analysis Specialist, Centre for Cybersecurity

Algirde Pipikaite
Lead, Centre for Cybersecurity

Accenture

Taylor Browder
Security Consultant

Michael Rohrs
Security Senior Manager

Lauren Stockton
Security Senior Analyst

Endnotes

1. World Economic Forum, “Accelerating Digital Transformation for Long-Term Growth”, 2022, https://initiatives.weforum.org/digital-transformation/home (accessed 8 June 2022).
2. World Economic Forum in collaboration with Accenture, *Global Cybersecurity Outlook 2022,* Insight Report, January 2022, www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (accessed 23 May 2022).
3. Bissell, Kelly, et al., *State of Cybersecurity Resilience 2021: How aligning security and the business creates cyber resilience*, Accenture, 2021, https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf (accessed 23 May 2022).
4. World Economic Forum, “Cybersecurity”, 2022, https://www.weforum.org/topics/cyber-security (accessed 9 June 2022).
5. Modern Diplomacy, “Global CEOs Commit to Collective Action on Cyber Resilience”, Tech News, 26 May 2022, https://moderndiplomacy.eu/2022/05/26/global-ceos-commit-to-collective-action-on-cyber-resilience (accessed 10 June 2022).
6. Ross, Ron, et al., *Developing Cyber-Resilient Systems*, NIST Special Publication 800-160, Vol. 2, Revision 1, US National Institute of Standards and Technology (NIST), 2021, https://csrc.nist.gov/glossary/term/cyber_resiliency#:~:text=Definition(s)%3A,NIST%20 (accessed 10 June 2022).
7. World Economic Forum, “Fourth Industrial Revolution”, https://www.weforum.org/focus/fourth-industrial-revolution?page=10 (accessed 14 June 2022).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org