ISACA®

DIGITAL TRUST

BOARD BRIEFING

Contents

3 Executive Summary

4 The Digital Trust Imperative

6 Benefits and Expectations of a Digital Trust Ecosystem

7 Consequences of Deficiencies in Digital Trust

7 The Digital Trust Ecosystem Supply Chain

7 GRC and Digital Trust

- 9 Governance
- 11 Governance Perspectives
- 13 Risk
- 13 Compliance

13 Digital Trust Oversight

- 14 Digital Trust Committee
- 15 Integrating Digital Trust Into Applicable Committees

16 Fostering Digital Trust

16 Digital Trust Principles for Boards and Governing Bodies

- 19 Principle 1—Systems Thinking
- 19 Principle 2—Risk Governance
- 20 Principle 3—Awareness
- 20 Principle 4—Appropriate Framework
- 21 Principle 5—Risk Management

21 Understanding ISACA’s Digital Trust Ecosystem Framework (DTEF)

- 22 DTEF Structure

26 Conclusion

Executive Summary

An enterprise can improve its relationship with consumers, enhance its reputation and increase brand loyalty by building digital trust. Focusing on digital trust is a natural progression of the digital transformation journey as more and more interactions happen online. Digital trust should be a consideration in all areas of an enterprise—the people, technology, processes and organization—and all products and initiatives should be built with digital trust in mind from the start.

ISACA's Digital Trust Ecosystem Framework (DTEF) can be leveraged to create a digitally trustworthy ecosystem that considers the accountabilities and responsibilities of all enterprise stakeholders and ensures that all digital interactions and transactions are legitimate, trusted and reflect integrity, security, privacy, resilience, quality, reliability and confidence.

Digital trust requires significant iterative work, but enterprises that can demonstrate their digital trustworthiness can boost their reputation and gain an edge over less trustworthy competitors.

The Digital Trust Imperative

The word "digital" is ubiquitous in today's business environment. Everything is becoming digital: product and service development, supply chain management, talent management, sales and marketing efforts, customer interactions. Nearly every aspect of business has some digital component. All industry types and sizes can benefit from going digital, but what exactly does that mean?

Digital transformation integrates digital technology into all business areas, changing how organizations deliver products and services to customers and consumers. Technology has become an everyday part of people's lives, and organizations must understand how to stay ahead of trends and disruption in today's fast-paced and rapidly changing environment. Organizations also need to be vigilant in protecting the data related to their customers and consumers, and maintaining the confidentiality, integrity and availability of the systems upon which their stakeholders rely.

Digital trust centers on the relationship between parties and is broader than just a financial relationship. The key to this concept is trust. This trust is not simply about cybersecurity or privacy protection; it is about faith in the relationships between entities.

ISACA defines digital trust as the confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organizations, processes, information and technology to create and maintain a trustworthy digital world.[1] This definition differs from others because it focuses on how confidence is dependent on—and manifests in—people, processes, the organization itself and modern and emerging technologies. Of course, information is also a critical component of trust because it underpins every other component in a digital trust ecosystem.

[1] ISACA, *Digital Trust Ecosystem Framework*, USA, 2022, www.isaca.org/dtef-ebook

To remain competitive and provide value in today's connected world, organizations need to strive to keep pace with, or stay ahead of, the latest trends in the digital space. Doing this requires an ongoing understanding of the following:

- The integrity of relationships refers to values rather than the traditional definition of integrity associated with information security and privacy.
- Digital trust reflects the entire organizational ecosystem, not siloed parts (i.e., IT, compliance, operations, marketing or sales).
- Digital trust requires engagement across the entire enterprise, as well as with external stakeholders.
- Traditional IT-related disciplines such as security, privacy, risk, assurance and governance form the basis of digital trust, but in themselves are not sufficient.
- Ethics, transparency and accountability play an essential role that can be easily overlooked.
- Digital trust is highly dependent on the less tangible aspects of an organization, such as culture, brand, product quality, data ethics and reliability.

Consumers not only need to feel good about the products and services they receive, but they also need to feel satisfied about an organization's response to negative events. Digital trust efforts are fluid. One major negative newsworthy event, significant outage or improper transaction can affect stakeholders' trust in an organization. Cyberincidents and data breaches are good examples. Actions taken after these events often draw more scrutiny and evaluation than actions taken before. Stakeholders should be assured that organizations will act in their best interest before and after negative events.

Positive events can significantly enhance digital trust, resulting in benefits such as improved reputation, increased revenues, loyal consumers and more reliable data for decision making.[2] Future success can be directly attributed to customers' perceptions of an organization's digital trustworthiness[3] and the adoption of a trust framework to help facilitate trusted digital relationships with stakeholders.

[2] ISACA, "State of Digital Trust 2023," 2023, https://www.isaca.org/resources/reports/state-of-digital-trust-2023

[3] McKinsey, "Why digital trust truly matters," 2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

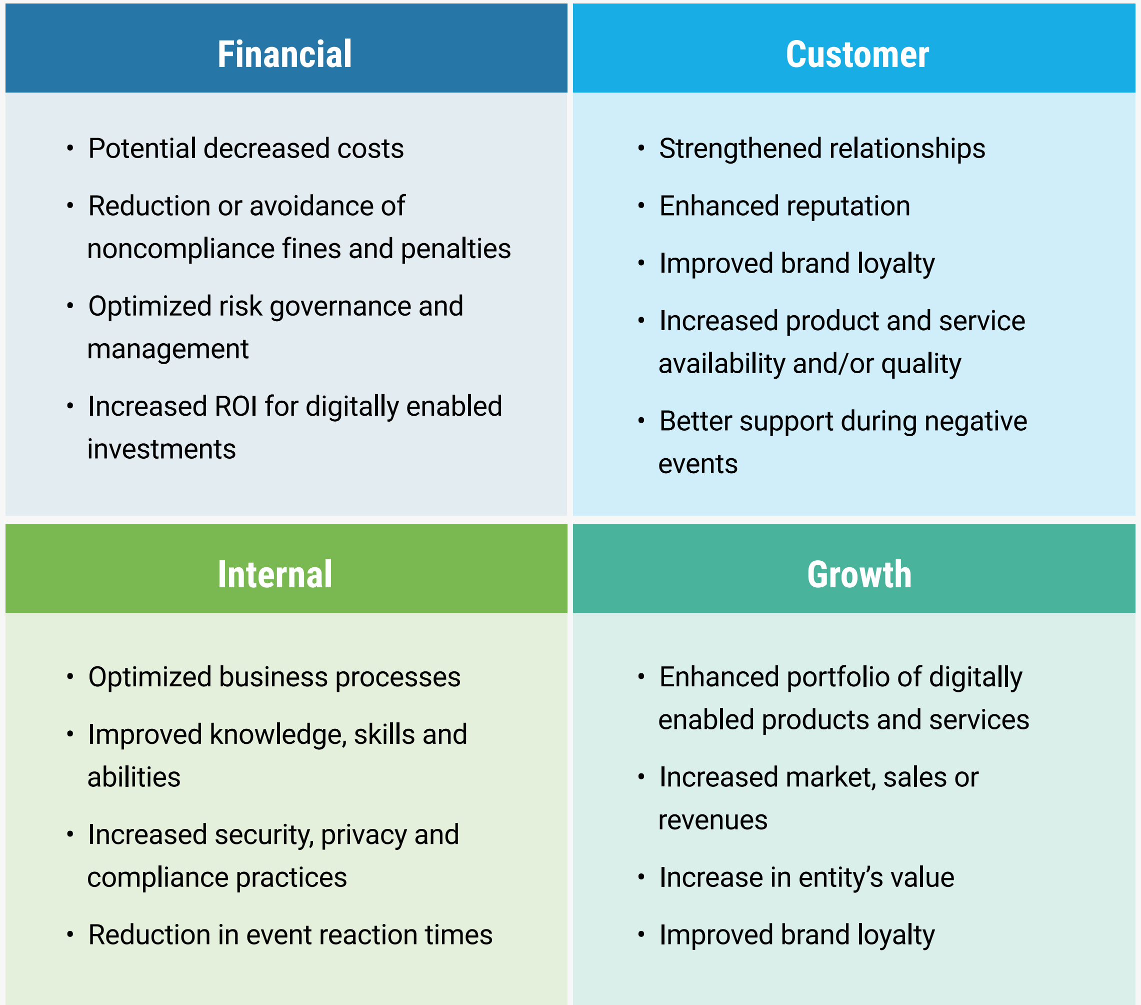
Benefits and Expectations of a Digital Trust Ecosystem

Digital evolution is driven by the business needs and requirements that enable an enterprise to remain competitive and meet customers' changing expectations in a fast-paced and high-velocity environment. For example, the "always connected" customer and consumer market relies heavily on mobile and connected devices and expects companies to adapt business practices to the ever-changing technology landscape.

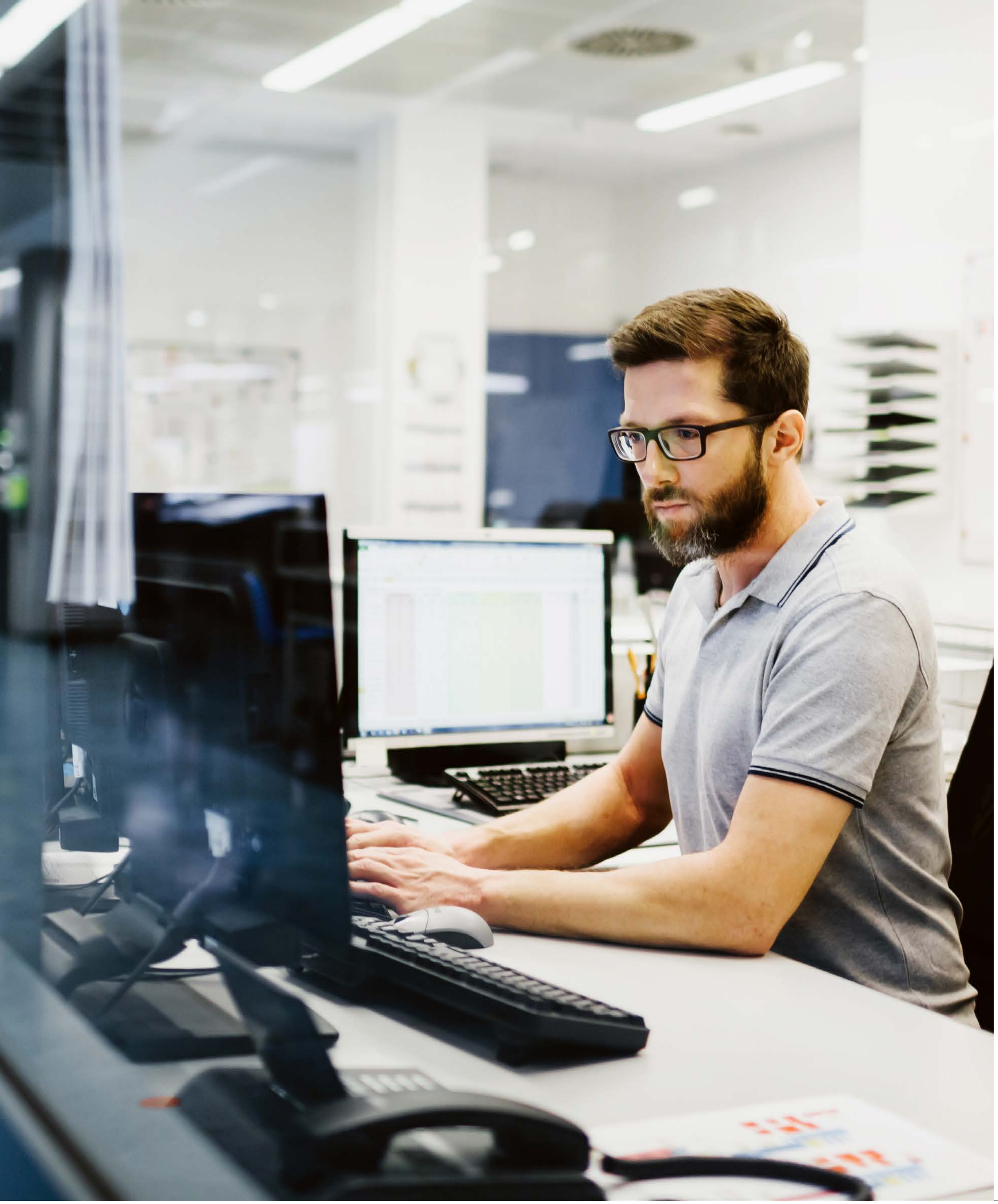
Digital trust is a significant factor that influences consumers' decisions on whether to do business with—or continue doing business with—a company. As a result, companies should understand the interdependencies and inter-relationships of the digital ecosystem where their products and services operate and the consequences of breaking trust (and the factors that could violate it).

Digitally trustworthy enterprises can enjoy many significant competitive advantages over less trusted companies. Consider a balanced scorecard approach: most organizations use a balanced scorecard to organize and manage goals, objectives and performance indicators. **Figure 1** uses the balanced scorecard dimensions to outline some potential benefits of a healthy digital trust posture.

FIGURE 1: Balanced Scorecard Approach to Digital Trust



Financial	Customer
• Potential decreased costs • Reduction or avoidance of noncompliance fines and penalties • Optimized risk governance and management • Increased ROI for digitally enabled investments	• Strengthened relationships • Enhanced reputation • Improved brand loyalty • Increased product and service availability and/or quality • Better support during negative events
Internal	**Growth**
• Optimized business processes • Improved knowledge, skills and abilities • Increased security, privacy and compliance practices • Reduction in event reaction times	• Enhanced portfolio of digitally enabled products and services • Increased market, sales or revenues • Increase in entity's value • Improved brand loyalty



Consequences of Deficiencies in Digital Trust

Rapid advances in—and the accessibility of—emerging technologies have led society to increasingly rely on digitalization, resulting in more inherently complex relationships. A lack of digital trust can have negative consequences for these relationships. **Figure 2** provides examples of how an organization can lose consumer trust and the potential stakeholder responses and outcomes for each scenario.

The Digital Trust Ecosystem Supply Chain

Trust relationships exist not only within an enterprise's ecosystem but also across the supply chain between the consumer and provider and even between the provider and third parties (**figure 3**). Organizations need to understand and address the trust relationships within their ecosystem, and across the supply chain.

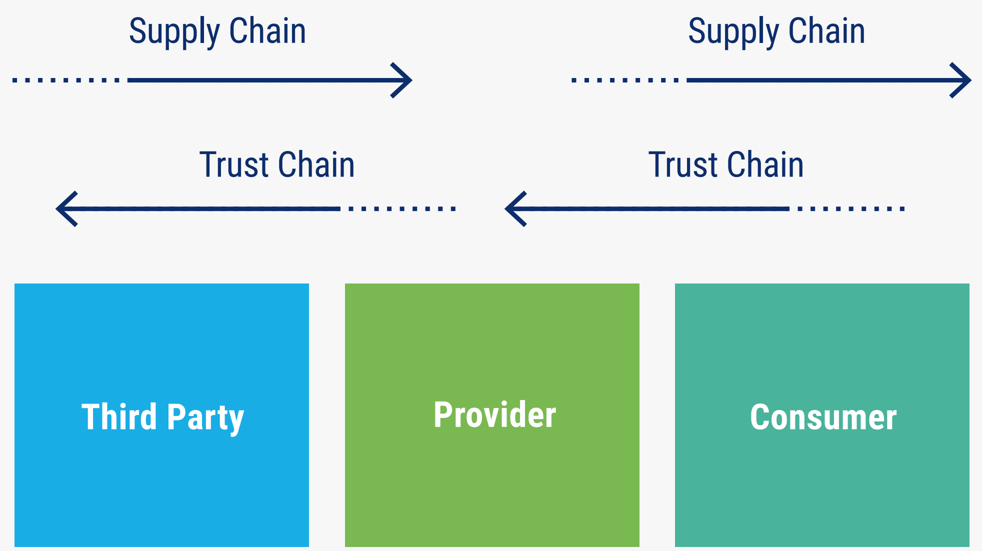
GRC and Digital Trust

Governance, risk and compliance, or GRC, is a structure for aligning organizational practices and activities with business goals and strategies, while managing risk and meeting applicable legal and regulatory requirements. GRC provides a mechanism for enterprises to balance performance (meeting the organization's needs) and

FIGURE 2: Consequences of Deficiencies in Digital Trust

Organizational Actions	A managed services provider experiences a major data breach that exposes thousands of customer records, including personally identifiable information. The company fails to communicate this breach for six months, only after the breach is exposed in the media.	A food manufacturer outsources several key business processes to a third-party software as a service (SaaS) provider. The contract does not require the third party to disclose its continuity documentation or participate in any disaster recovery testing. The SaaS provider experiences a major operational incident where all services are unavailable for 72 hours, leaving the manufacturer without its core customer-facing services.	The social media manager for a popular online clothing company accidentally posts politically sensitive and offensive content using the company account, thinking it is their personal account. Management does not notice the post until the chief marketing officer is notified, and it is removed four hours after publication.
Stakeholder Responses	• Immediate decline in customer accounts • Several individual and class-action lawsuits • Significant negative press on popular social media platforms	• Multiple calls to the helpdesk that overwhelm the call backlog and create a lengthy queue time • Multiple customer requests for "damage reports" resulting from the event • Media coverage on a national news outlet highlighting the outage	• Social media outcry to replace the social media manager, as well as members of the leadership team • A significant drop in social media followers for multiple weeks following the incident • Notification that the company is potentially facing defamation legal actions as a result of the post
Outcomes	• Immediate loss of revenue • Multiple fines for noncompliance and failure to report the incident • Immediate loss of several organizational certifications • Regulator fines and penalties	• Shareholder activists demand a change to the board structure. • The SaaS provider declares bankruptcy, leaving the food manufacturer with compromised business processes. • The CEO and CIO immediately and unexpectedly resign, leaving a critical gap in the leadership team and diminished shareholder confidence.	• The social media manager is terminated, begins a harsh social media campaign against the company and sues for wrongful termination. • The company incurs legal fees and settlement payments. • There is a significant decline in online orders.

FIGURE 3: Digital Trust Ecosystem and the Supply Chain



Digital trust should be embedded into any organization’s GRC model, as connecting digital actions to the governing structure can positively affect the trust between the organization and its stakeholders.

conformance (following the rules) with respect to information, technology and digital investments and initiatives. Digital trust should be embedded into any organization’s GRC model, as connecting digital actions to the governing structure can positively affect the trust between the organization and its stakeholders.

Governance

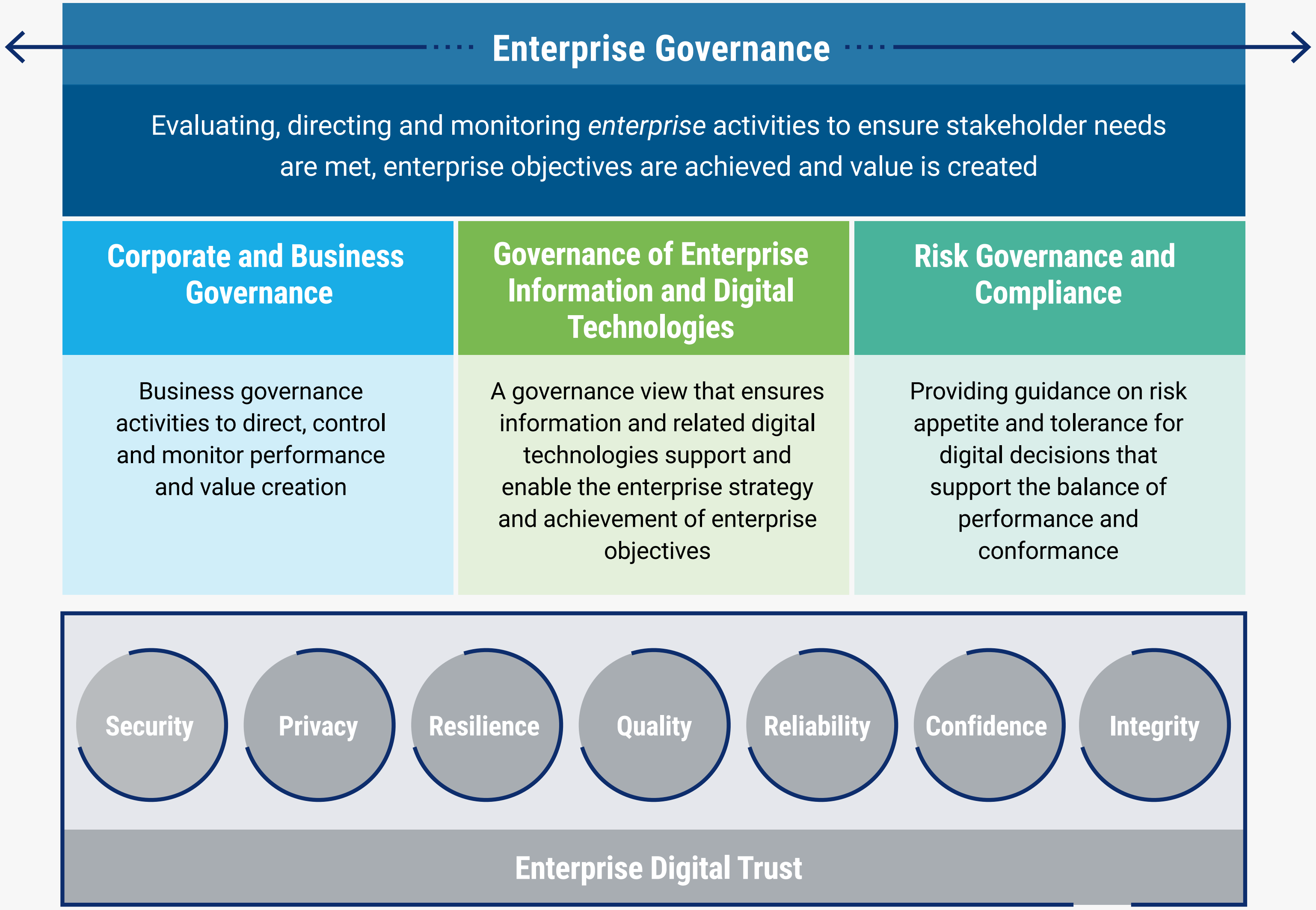
Governance is the means of directing and controlling an organization. Without a governance system in place, organizations lack the proper guidance to meet stakeholder needs. There is a distinction between governance and management. Where governance provides the direction, management executes that direction in compliance with internal and external requirements.

How does this relate to digital trust? Digital trust is not a single process, practice, activity or control but rather a system of all of these that collectively embodies the trust between providers and consumers in a digitally enabled relationship. Further, digital trust is not just cybersecurity and privacy—these are components of the complete trust ecosystem. And all of these elements are components of a governance system.

Until recently, cybersecurity was often not clearly connected to enterprise objectives and was essentially treated as the technical team who manages the network. Breaches, ransomware, data privacy violations and operational outages have vaulted cybersecurity into sharp focus, which requires an enterprise-wide approach. The concept of digital trust arose from the realization that cybersecurity is not enough, and all aspects of an organization must be considered. Digital trust is not limited to a single team, event, investment or program. It is pervasive throughout an organization and requires holistic governance. It should be part of every procedure and activity directly or indirectly connected to the digital ecosystem.

Executives and boards should embed digital trust in all business spheres and activities. This is best executed by professionals who understand technology and can render technology concerns into operational and strategic matters. A way to put this into perspective is by looking at governance in layers, or altitudes. The bridge between the layers of governance enhances the synergy between the highest governing body and operational and tactical management teams, ensuring digital trust is embedded into all facets of governance. **Figure 4** identifies these perspectives: enterprise governance, corporate and business governance, governance of enterprise information and digital technologies, and risk governance and compliance.

FIGURE 4: Governance of Enterprise Digital Trust



Enterprise Governance

Evaluating, directing and monitoring *enterprise* activities to ensure stakeholder needs are met, enterprise objectives are achieved and value is created

Corporate and Business Governance	Governance of Enterprise Information and Digital Technologies	Risk Governance and Compliance
Business governance activities to direct, control and monitor performance and value creation	A governance view that ensures information and related digital technologies support and enable the enterprise strategy and achievement of enterprise objectives	Providing guidance on risk appetite and tolerance for digital decisions that support the balance of performance and conformance

Governance Perspectives

Enterprise governance involves evaluating, directing and monitoring enterprise activities to ensure enterprise objectives and stakeholder needs are achieved and value is created.[4] Enterprise governance is supported by corporate and business governance, which includes activities that direct, control and monitor performance and value creation. Governance of enterprise information and digital technologies is a governance view that ensures information and related digital technologies support and enable the enterprise strategy and achievement of enterprise objectives. Finally, risk governance and compliance can provide guidance on risk appetite and tolerance for digital decisions that support the balance of performance and conformance.

From a governing body perspective, there are many factors that should be considered relative to digital trust:

- **CONFIDENCE**—The faith or belief that one will act in a right, proper or effective way.
- **INTEGRITY**—The guarding against improper information modification or destruction of systems or data; includes ensuring information nonrepudiation and authenticity.
- **SECURITY, CONFIDENTIALITY AND AVAILABILITY**—The extent to which information is accessible when needed and secured (i.e., access is restricted to individuals and systems with proper clearance and valid business need).
- **PRIVACY**—The right of an individual to trust that others will appropriately and respectfully use, store, share and dispose of associated personal and sensitive information according to the context and business purposes for which it was collected or derived.
- **RESILIENCE**—The ability of a system or network to resist failure or recover quickly from a disruption, usually with minimal recognizable effect. This requires organizations to have a common understanding of their priorities and objectives and the ability to anticipate, prepare, respond and adapt to changes or disruptions.
- **QUALITY**—The organization's information pertaining to digital trust meets certain quality criteria. This is supported by intrinsic quality (the extent to which the information provides accurate, objective and reputable information) and contextual quality (the extent to which the information outcomes are relevant, complete, current, appropriate, consistent, understandable, agile and easy to interpret).
- **RELIABILITY**—The ability of a company to perform its required functions accurately and reproducibly under stated conditions for a specified period of time.

[4] ISACA, *COBIT 2019 Framework: Introduction and Methodology*, USA, 2018, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9cEAC

FIGURE 5: Sample Digital Trust Goals and Strategies

Organization Type	Example Digital Trust Goals	Sample Strategy Key Points
Local government agency that offers social services programs to its residents	• Provide complete digital solutions for all services offered to our residents in one year. • Reduce service interruptions due to digital technology by 40%. • Increase resident use of our digital interactions by 60% in the next three years.	• Optimize online user experience with streamlined, frictionless services that are intuitive and understandable. • Increase investments in digital technologies that focus on user interactions through the portal while increasing resiliency to unplanned downtime. • Actively advertise and promote online services to existing and new users, focusing on the quality of the interaction outcomes.
International banking system that focuses on on business accounts for large enterprises	• Increase online business loan services by 40% to address the increase in new service features. • Experience no business banking service outages or unplanned maintenance downtime.	• Establish strategic partnerships with reputable, secure and transparent third parties to support digital services. • Leverage current client testimonials and satisfaction scores in an aggressive marketing campaign to positively affect growth. • Focus infrastructure and architecture investments on service, infrastructure and application resilience to enable high availability.
Online networking platform that focuses on busy business professionals	• Increase Net Promoter Score (NPS) to 80. • Double positive online reviews in the next six months. • Increase customer retention rate by 50%.	• Redesign the customer-facing website to yield top search engine rankings. • Integrate a customer feedback mechanism that continually improves the full customer life cycle. • Develop a customer recognition and reward system to retain customers for future revenue.

Another aspect of governance is developing and supporting the enterprise digital trust strategy, which should be aligned with and incorporated into the overall strategy. A strategy is a high-level plan to achieve the organization's digital goals and objectives, ultimately delivering value to stakeholders. It can also be described as the direction set for the organization and its various units to achieve a desired state. A digital trust strategy is required for an enterprise to maintain a competitive edge in an increasingly digital world.

A digital trust strategy is based on goals; therefore, the strategy will be different depending on the type and size of the enterprise. Digital trust goals should cascade down to all affected internal stakeholders, including business management, IT management, human resources (HR), internal audit, marketing and risk and compliance teams. Each plays a vital role in meeting stakeholder and customer needs by translating business goals into digital trust goals and establishing a trustworthy digital footprint. Examples of digital trust goals and supporting strategies for different organization types are found in **figure 5**.

Risk

A risk is a potential event that, if it materializes, can have an effect on the organization meeting its objectives. From a digital trust perspective, integrating risk into the enterprise risk register is key, as addressing risk is vital to organizational survival. Depending on the industry, this may include product security and privacy. Developing a full view of risk that connects digital technology to business strategy requires the identification of scenarios that can cause negative outcomes.

At the enterprise level, there are several digital trust-related risk scenarios that could be appropriate, including:

- Inability to meet business goals, objectives and strategies
- Degradation or failure of a digitally enabled product or service
- Inadequate availability of knowledge, skills, abilities and desired behaviors
- Loss of enterprise reputation or brand strength
- Failure to meet compliance requirements
- Insufficient controls for cybersecurity or privacy vulnerabilities and scenarios
- Negative internal or external events that affect digital trust
- Core customer, user or consumer loss
- Third-party failures causing disruption in the digital supply chain
- Deficient technologies supporting the digital environment

Compliance

Often synonymous with conformance, compliance refers to an organization's adherence to applicable rules, laws and regulations. These can be country-specific laws, industry regulations or internal policies and directives. Enterprises are charged with adhering to these specifications, or striving to do so, as noncompliance can lead to financial, reputational, legal, operational or strategic risk events.

Today, there are no specific laws or regulatory requirements directly related to digital trust; however, many relate to the technologies, practices, information, privacy and safety aspects that support digital trust outcomes. It is well known that organizations often cannot be 100 percent compliant with every law, rule or regulation in their compliance environment. Organizations must weigh the option of compliance with a legal or regulatory requirement with the penalties and reputational risk associated with noncompliance.

Digital Trust Oversight

For a governing body to do its work effectively, members need to understand their individual accountabilities and responsibilities, and the board must organize itself to perform necessary tasks effectively. Boards should have expertise in legal, marketing, finance, HR, IT, strategic planning, cybersecurity, digital and other areas. These needs can change over time, so it is important for boards to review them regularly and adjust their composition accordingly. Best practices and regulations also play a part in shaping board composition. An example of this is the evolution of best practices related to diversification of board compositions in age, gender, ethnicity and race, as well as the evolution of cybersecurity, privacy, digital transformation and now digital trust. Committees or working groups can enhance the board's effectiveness in these areas.

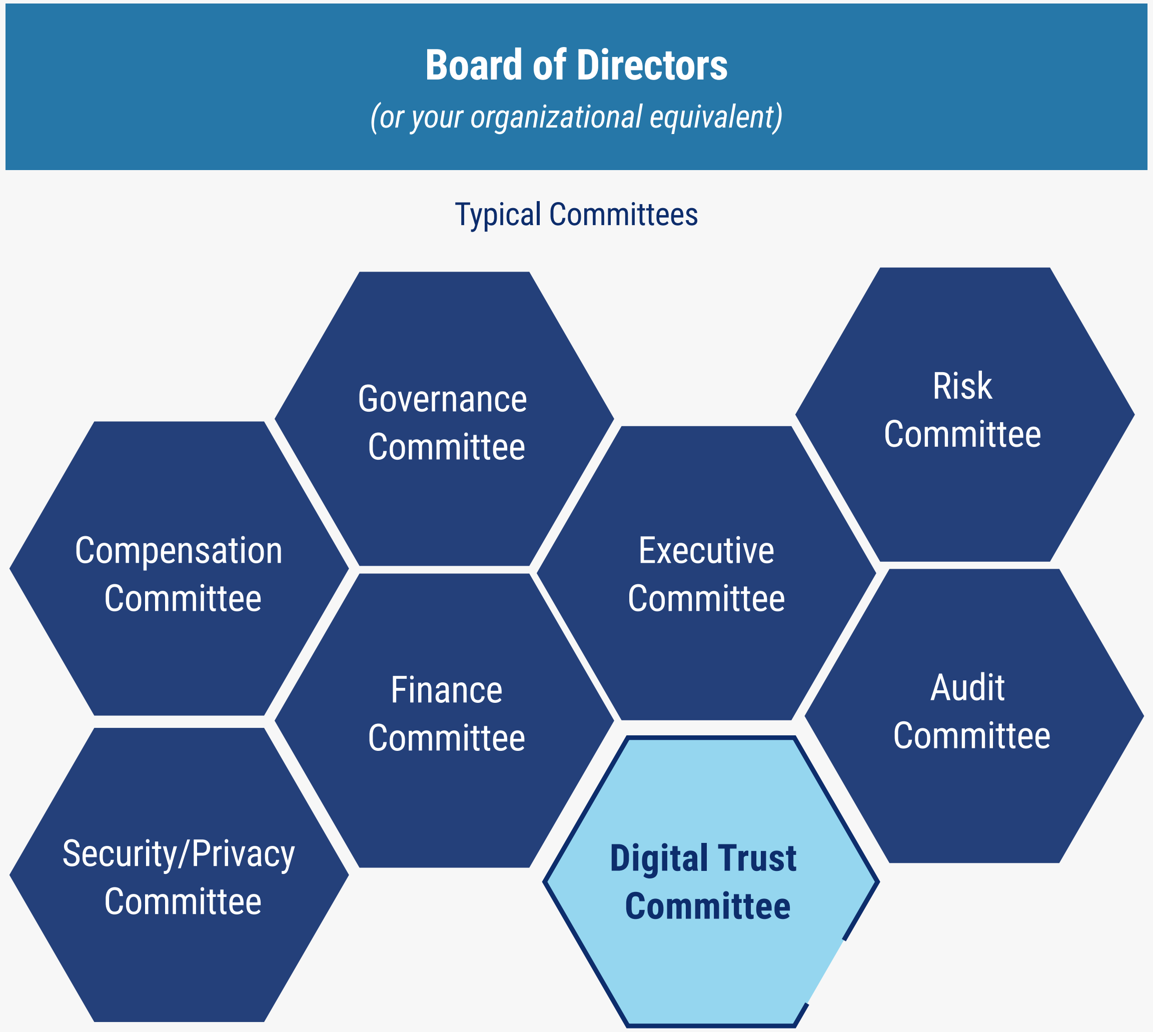
Rather than the entire board acting on all matters, committees divide the work so that far more can be accomplished. Most boards organize themselves into executive or steering committees, subcommittees, standing committees and ad hoc committees, task forces or working groups. Typical committees that may work under an organization's board of directors are shown in **figure 6**.

Enterprises have a few options when determining governing bodies for digital trust. One option is to create a digital trust committee, and another is to ensure that digital trust is integrated into other applicable committees in lieu of creating a separate, focused digital trust committee.

Digital Trust Committee

A digital trust committee is a valid option to ensure proper direction and control over digital trust efforts. The purpose of a digital trust committee is to address the needs of an organization's digital product and service consumers through the appropriate evaluation, prioritization and direction of digital trust activities, funding and programs that contribute to a trusted relationship. Consider this committee the expert review panel and point of contact for the organization on digital trust decisions, measurements, guidance and alignment with the organization's goals and objectives.

Figure 6: Typical Committees to a Board of Directors



This committee should report directly to the board but can be a subcommittee of another standing structure that is already chartered and mature.[5] If used as a subcommittee, most organizations would logically make it a part of a security/privacy committee or an audit/risk committee. Although this may be an optimal place for a digital trust group, boards must be cautious of the fact that digital trust is an outcome of good security, privacy, risk and governance practices.

Integrating Digital Trust Into Applicable Committees

Some organizations may choose not to charter a committee specifically focused on digital trust. This is understandable, given that some organizations feel overwhelmed with the number of committees in their governance structure and choose to merge and consolidate committees and therefore address digital trust matters throughout their existing committees. In this case, it is critical to ensure that digital trust topics are integrated into all committees where digital trust is relevant. Organizations should also ensure that digital trust is addressed at the proper level and that committee efforts are synchronized to avoid the duplication of efforts and conflicting guidance.

[5] It may be more practical to make the digital trust group a subcommittee that reports to an audit/risk committee or a security/privacy committee, which, as a standing committee of the board, would have a board member as its chair. However, digital trust should be a regular agenda item with board focus.

Fostering Digital Trust

Digital trust is not limited to individual interactions and transactions between providers and consumers of digitally enabled products and services. It encompasses brand reputation, product quality, reliability and the ethical use of data. Individuals might view an organization's trustworthiness based on its reputation or peer feedback on the company, its services or products. This can even occur among individuals who have never interacted or transacted directly with the company.

Therefore, organizations should demonstrate ethical behavior and trust through integrity, security, privacy, resilience, quality, reliability and confidence. Customers will abandon organizations that do not align with their values in favor of those that do. Ethics, as applied to business, are the guidelines an organization follows while conducting its operations. Acting ethically is not the same as being compliant with laws and regulations. Fostering digital trust depends on a commitment to ethical behavior, as defined by the enterprise.

People in an enterprise have their own beliefs, values, behaviors, personalities and experiences. However, since an enterprise also defines its own beliefs, values and behaviors, these attributes affect its people and inform how they should comply when acting on behalf of the organization. Governing bodies must define the organization's guidance regarding culture, ethics and behaviors and demonstrate their support for these. A policy or statement on ethics or standards of conduct is typically the most common tool to support this.

It is important for governing bodies to ensure the proper tools are in place to support and foster digital trust throughout the enterprise. This involves analyzing, articulating, communicating and governing a consistent approach to supporting digital trust. The approach must include transparency and compliance with legal, contractual and internal compliance requirements. Guiding principles should also be determined and communicated, and efforts should be made to ensure that these principles are followed for all prioritization, funding and enforcement of digitally enabled investments.

Digital Trust Principles for Boards and Governing Bodies

Principles guide organizations toward their strategic goals, and they interact with, and often depend on, each other. Regardless of the type of governing body (advisory, nonprofit, private or public), digital trust principles should be considered. Although every organization is unique, they all have one thing in common: purpose. That purpose is to provide direction and control for an organization to pursue the benefits and value needs of interested parties and stakeholders.

ISACA suggests five principles for boards and governing bodies in support of digital trust (**figure 7**). These principles fall into two areas: what the board should be doing and what the board should expect from management.

This distinction is important, as the board (or appropriate governing body) generally does not dictate management practices; the board provides the guidance needed for management to support the achievement of enterprise goals.

TO FOSTER DIGITAL TRUST:

Define, communicate and support enterprise values and principles related to digital trust.

Establish or delegate the appropriate organizational structures to assist in the governance and management of digital trust.

Allocate resources and funding for digital trust investments aligned with organizational goals and objectives.

Establish communication mechanisms that provide those with digital trust responsibilities oversight and feedback on digital trust initiatives.

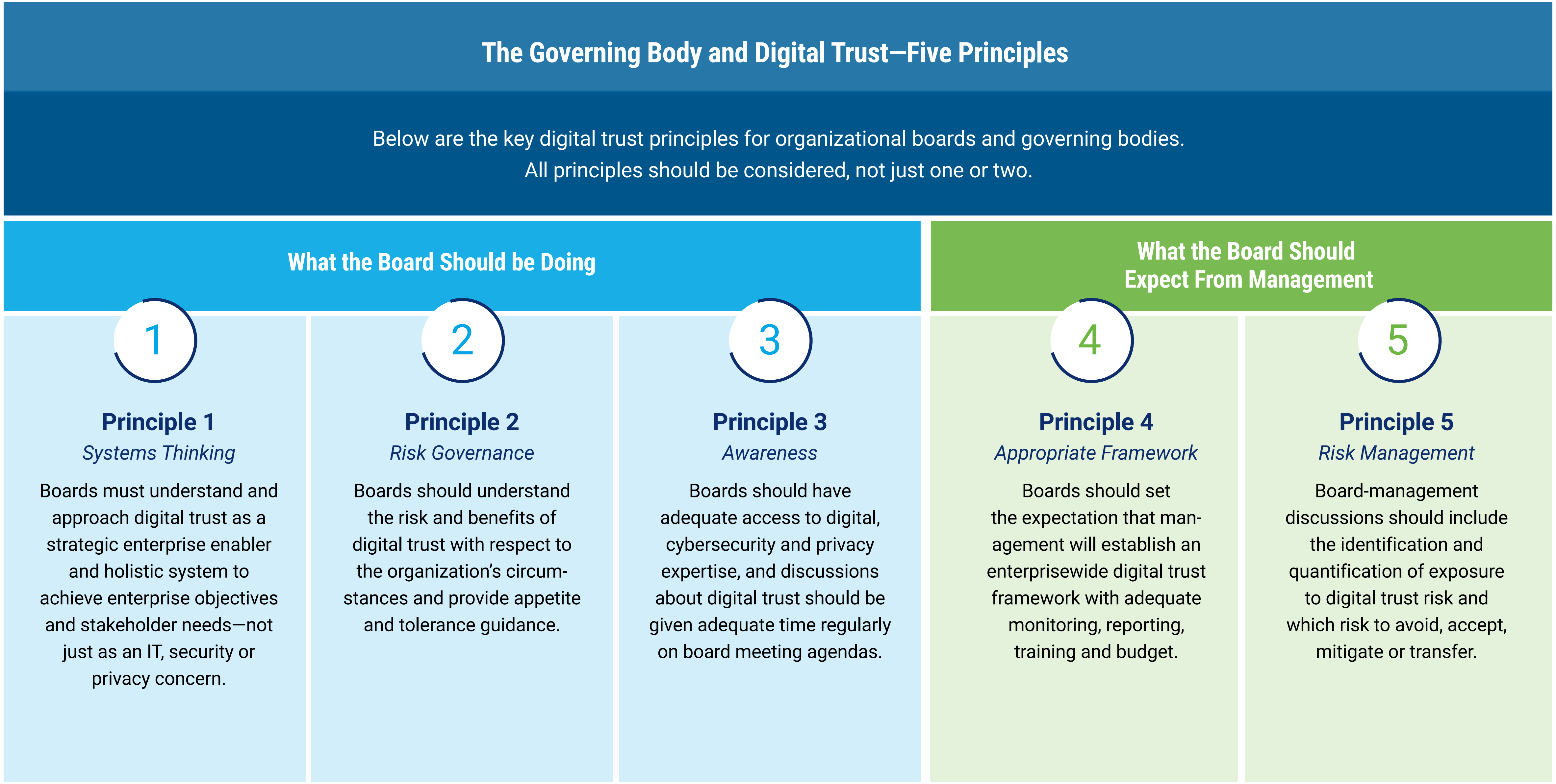
Create and monitor a reward system to promote desirable outcomes with regard to digital trust.

Actively support emergence that socializes management's support of digital trust activities (i.e., continual improvement).

Evaluate the effectiveness of the organization's digital trust practices and celebrate successes in relation to digital trust initiatives.

Create, enforce and update appropriate digital trust-related policies.

FIGURE 7: Digital Trust Principles for Governing Bodies



The Governing Body and Digital Trust—Five Principles

Below are the key digital trust principles for organizational boards and governing bodies. All principles should be considered, not just one or two.

What the Board Should be Doing

1

Principle 1

Systems Thinking

Boards must understand and approach digital trust as a strategic enterprise enabler and holistic system to achieve enterprise objectives and stakeholder needs—not just as an IT, security or privacy concern.

2

Principle 2

Risk Governance

Boards should understand the risk and benefits of digital trust with respect to the organization's circumstances and provide appetite and tolerance guidance.

3

Principle 3

Awareness

Boards should have adequate access to digital, cybersecurity and privacy expertise, and discussions about digital trust should be given adequate time regularly on board meeting agendas.

What the Board Should Expect From Management

4

Principle 4

Appropriate Framework

Boards should set the expectation that management will establish an enterprisewide digital trust framework with adequate monitoring, reporting, training and budget.

5

Principle 5

Risk Management

Board-management discussions should include the identification and quantification of exposure to digital trust risk and which risk to avoid, accept, mitigate or transfer.

PRINCIPLE 1

Systems Thinking

Boards must understand and approach digital trust as a strategic enterprise enabler and holistic system to achieve enterprise objectives and stakeholder needs—not just as an IT, security or privacy concern.

At the highest level of the organization, “systems thinking” is often synonymous with a holistic approach.

Key considerations for this principle include:

- Consider all enterprise activities as a whole, rather than as separate parts, and establish an understanding of how changes in one part of the organization can impact others.
- View digital trust as the umbrella over all privacy and cybersecurity matters.
- Integrate frameworks into the overall framework ecosystem, supporting systems thinking.
- Integrate enterprise architecture principles to model the current and future states of the enterprise “building blocks.”

PRINCIPLE 2

Risk Governance

Boards should understand the risk and benefits of digital trust with respect to the organization’s circumstances and provide guidance on risk appetite and tolerance.

There is a distinction between risk governance and risk management. Risk governance is responsible for guiding management in areas like risk appetite and tolerance and providing the delegation of authorities to management regarding actions taken.

Key considerations for this principle include:

- Identify, communicate and enforce risk appetite and tolerance levels across the organization to ensure that proper risk decisions align with the overall risk profile.
- Develop an enterprise risk register that receives inputs from other, more detailed registers throughout the organization.
- Develop appropriate authority levels for handling certain types of risk and determine escalation procedures for risk that exceeds those authority levels.
- Associate digital trust risk scenarios with business risk.

PRINCIPLE 3

Awareness

Boards should have adequate access to digital, cybersecurity and privacy expertise, and discussions about digital trust should be given regular and adequate time on board meeting agendas.

Understanding the dynamic digital trust environment requires constant communication.

Key considerations for this principle include:

- Leverage external expertise for the board to ensure the most recent industry information is considered when making digital trust decisions.
- Ensure that digital trust outcomes are linked to successes in security, privacy and quality domains.
- Create a communication plan that endorses transparency throughout the organization regarding digital trust topics.
- Continually adjust the approach to digital trust as internal/external factors and organizational goals change.

PRINCIPLE 4

Appropriate Framework

Boards should set the expectation that management will establish an enterprise-wide digital trust framework with adequate monitoring, reporting, training and budget.

The board should expect management to establish an enterprise framework to address digital trust. A framework is the supportive structure for enabling the digital trust ecosystem that supports an organization's vision, mission, values, objectives and strategies. ISACA's Digital Trust Ecosystem Framework is one approach to managing digital trust initiatives.

Key considerations for this principle include:

- Select a framework that is open, flexible and aligned with major standards and industry models.
- Ensure the framework is holistic, tailorable and addresses all aspects of the digital trust ecosystem.
- Use the digital trust framework as a complement to and an extension, not a replacement, of current frameworks in the ecosystem.

PRINCIPLE 5

Risk Management

Board-management discussions should include the identification and quantification of exposure to digital trust risk and which risk to avoid, accept, mitigate or transfer.

Not to be confused with risk governance, risk management is delegated from the board to management.

Key considerations for this principle include:

- Define a risk management process that identifies, assesses, responds to and monitors risk related to digital trust.
- Determine criteria for risk assessments such as likelihood and impact.
- Identify risk response options for digital trust, including accepting, avoiding, transferring or mitigating.
- Ensure that risk-based decisions are consistent with the risk governance guidance.

Understanding ISACA's Digital Trust Ecosystem Framework (DTEF)

Digital trust should be a consideration in all areas of an enterprise—people, technology, process and organization—and all projects and initiatives should consider digital trust in the planning, design, deployment and support phases of any digital investment that supports products and services in today's high-velocity environment.

ISACA's Digital Trust Ecosystem Framework (DTEF) defines the core ingredients that comprise a digitally trusted ecosystem that considers the accountabilities and responsibilities of all enterprise stakeholders to ensure that all digital interactions and transactions are legitimate and trusted, and it considers elements such as integrity, security, privacy, resilience, quality, reliability and confidence.

The DTEF uses systems thinking from a holistic perspective. Understanding one part of the ecosystem enables understanding of other parts. A system is an organized collection of highly integrated components (or subsystems) that aim to accomplish an overall goal. Systems thinking describes a complex network of events, relationships, technologies, processes and people that interact in expected and unexpected ways. Most importantly, employing systems thinking enables organizations to consider the implications of their decisions and to manage risk more comprehensively.

DTEF Structure

It is important to note that the DTEF is not a separate framework to add to an organization's growing list of frameworks, models, bodies of knowledge and standards. The DTEF was designed to work in conjunction with existing frameworks to avoid framework overload.

The system starts at a high level and flows down into an actionable and deployable set of outcome-based activities. As a rule, all parts of the DTEF interact with each other. At the highest level, the DTEF addresses four primary elements (nodes): people, process, technology and organization. Nodes link to each other via domains. Therefore, if any portion of this model changes, it will affect the other components in the framework, which supports the systems thinking approach. The three-dimensional structure of the DTEF is shown in **figure 8**.

The Digital Trust Ecosystem Framework was designed to work in conjunction with existing frameworks to avoid framework overload.

FIGURE 8: The Digital Trust Ecosystem Framework

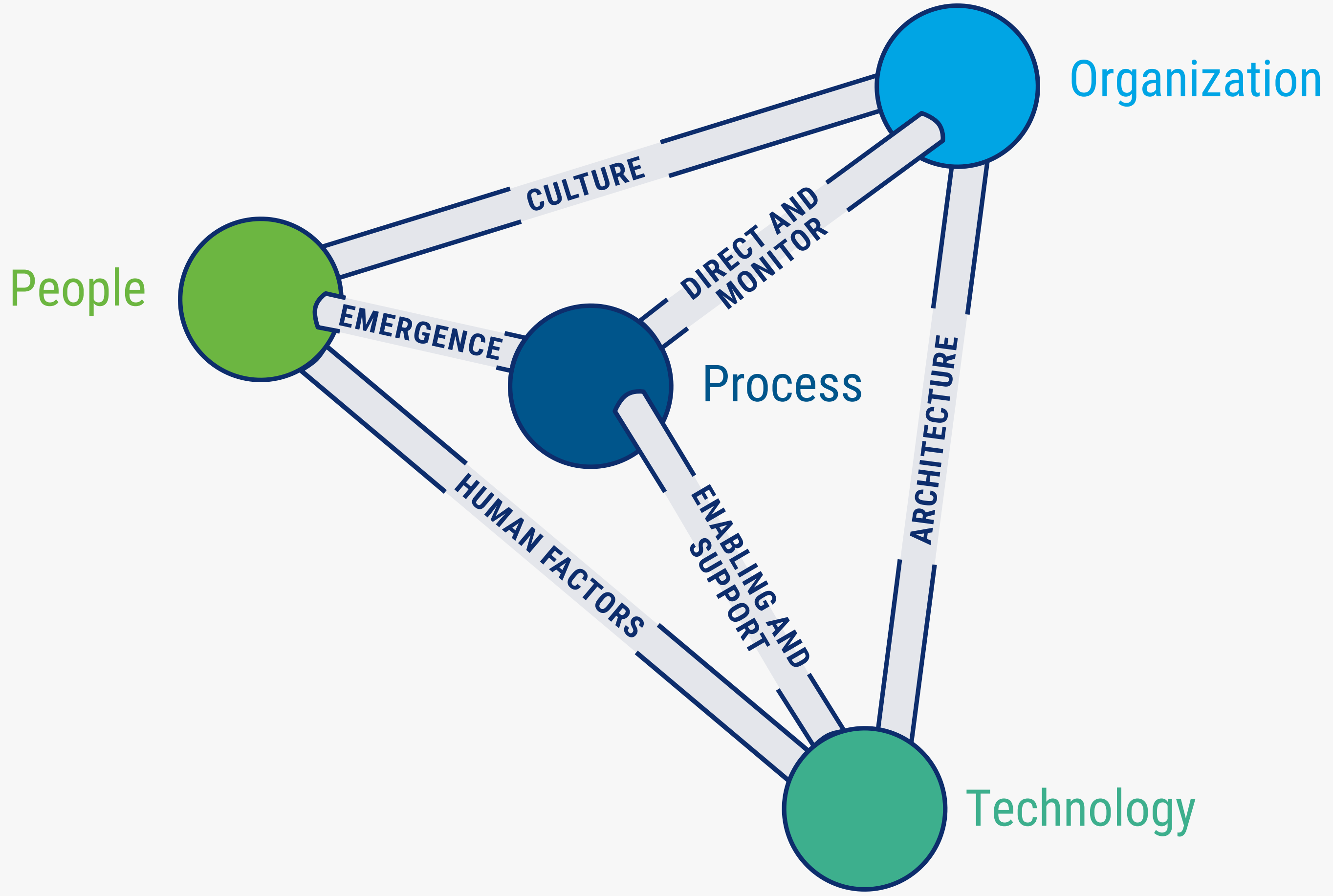
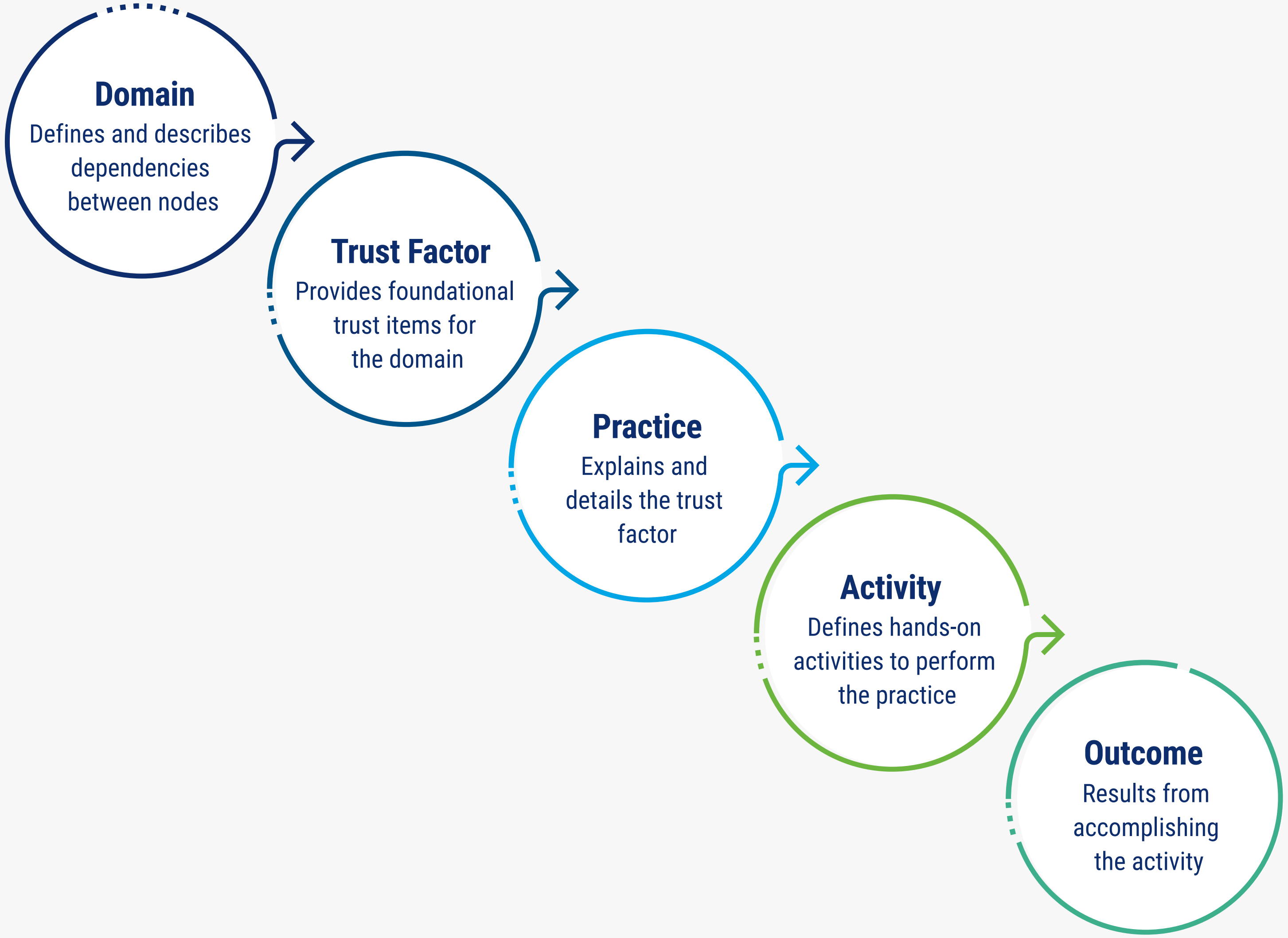


FIGURE 9: Hierarchy of the DTEF


Domain
Defines and describes dependencies between nodes
Trust Factor
Provides foundational trust items for the domain
Practice
Explains and details the trust factor
Activity
Defines hands-on activities to perform the practice
Outcome
Results from accomplishing the activity

The DTEF domains play a significant role in managing digital complexities and interconnections, and they must remain flexible and dynamic while considering emerging technologies, laws and regulations, threats, compliance issues and other influences. The DTEF domains include:

- Direct and Monitor
- Culture
- Architecture
- Enabling and Support
- Emergence
- Human Factors

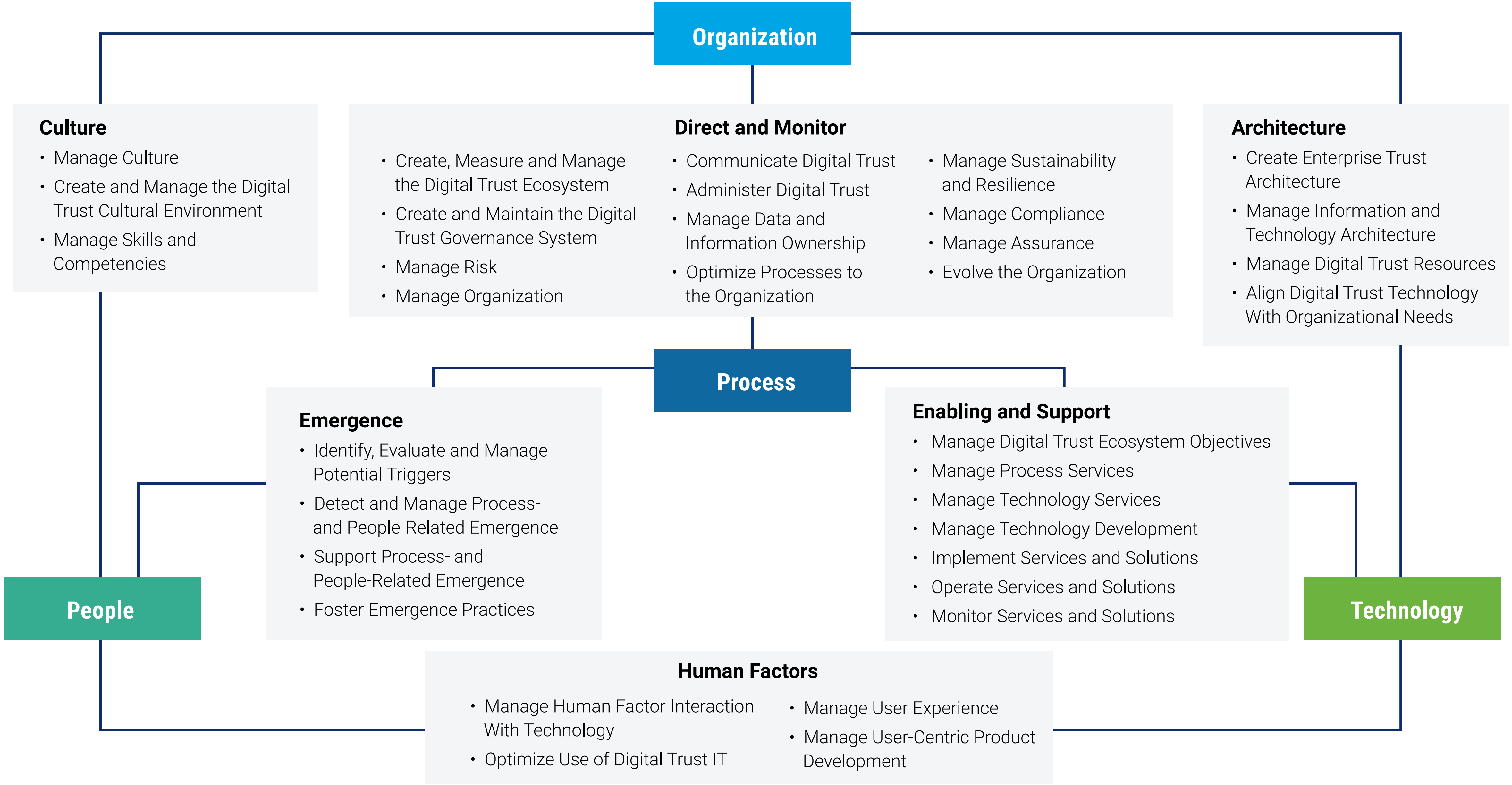
The DTEF is designed to support any organizational stakeholder with an interest in establishing and maintaining digital trust. In addition to the nodes and domains, the DTEF includes trust factors, entity controls, practices, general and key controls, activities, outcomes and links between related domains and trust factors. The hierarchy of these additional components within the DTEF is shown in **figure 9**.

Figure 10 illustrates the DTEF's nodes, domains and trust factors.

From a governance perspective, there are several key areas to consider regarding the DTEF:

- Think of the DTEF as a holistic system, where changing one area could affect one or many others.
- Resist the urge to "copy and paste" the DTEF—it is based on specific organizational values, mission, vision and objectives and should be tailored to an enterprise's specific needs.
- Position digital trust as an enterprise concern, not an IT, security or privacy issue.
- Obtain a clear understanding of the current and future business environment and the level of importance and visibility into digital trust.
- Create and manage the risk register.
- Integrate digital trust into the enterprise governance structure.
- Culture is key to a governance system because it influences behaviors and refers to norms and shared values among a group of people.
- Know the enterprise's current skills inventory as well as what desired skills are needed to support digital trust.
- Establish digital trust metrics that the organization will collect, report and act upon.

FIGURE 10: Nodes, Domains and Trust Factors



Organization

Culture

- Manage Culture
- Create and Manage the Digital Trust Cultural Environment
- Manage Skills and Competencies

Direct and Monitor

- Create, Measure and Manage the Digital Trust Ecosystem
- Create and Maintain the Digital Trust Governance System
- Manage Risk
- Manage Organization
- Communicate Digital Trust
- Administer Digital Trust
- Manage Data and Information Ownership
- Optimize Processes to the Organization
- Manage Sustainability and Resilience
- Manage Compliance
- Manage Assurance
- Evolve the Organization

Architecture

- Create Enterprise Trust Architecture
- Manage Information and Technology Architecture
- Manage Digital Trust Resources
- Align Digital Trust Technology With Organizational Needs

Process

Emergence

- Identify, Evaluate and Manage Potential Triggers
- Detect and Manage Process- and People-Related Emergence
- Support Process- and People-Related Emergence
- Foster Emergence Practices

Enabling and Support

- Manage Digital Trust Ecosystem Objectives
- Manage Process Services
- Manage Technology Services
- Manage Technology Development
- Implement Services and Solutions
- Operate Services and Solutions
- Monitor Services and Solutions

People

Technology

Human Factors

- Manage Human Factor Interaction With Technology
- Optimize Use of Digital Trust IT
- Manage User Experience
- Manage User-Centric Product Development

Conclusion

The dependence on digital technologies continues to grow, and the data generated in the interactions between providers and consumers is under more scrutiny. Consumers understand the harm that the improper handling of their information can cause, so digital trust is not optional in today's digitally enabled landscape. Enterprises that want to survive must value and prioritize digital trust.

Organizational governing bodies can help their organizations create value through the appropriate direction of digital trust priorities. Enterprises are now under immense pressure to balance conformance (meeting internal and external requirements) and performance (the ability to deliver digitally enabled products and services to consumers). The essential link is trust. An organization can meet all its compliance requirements and deliver its products and services as expected, but if a consumer has no trust in the organization, they will do business elsewhere.

There is a distinction between governance and management. From a governance perspective, governing bodies are charged with directing and controlling the organization and are in an optimal position to provide guidance on digital trust-related matters. Management receives this guidance and executes the process, practices and activities to meet the enterprise's goals, objectives and strategies.

Key to the governance of digital trust are subjects such as strategy, alignment, direction, assurance and oversight. These must support not only digital strategy but reputation as well.

Digital trust is an iterative process. Governing bodies must constantly evaluate their digital trust strategies and adjust them when areas for improvement are identified. Enterprises that can demonstrate digital trustworthiness gain considerable competitive advantage and build better relationships with their consumers.

Acknowledgments

Lead Developer

Mark Thomas
CISM, CGEIT
USA

Expert Reviewers

Joyce Chua
CISA, CISM, CDPSE, CCISO, CFE, CIA, CIPP(A), CIPP€, CIPM, FIP, IRCA, ISMS Associate Auditor, ITIL, MCP, PMP
Singapore

Larisa Gabudeanu
CISA, CISM, CRISC, CDPSE
Romania

J. Winston Hayden
CISA, CISM, CGEIT, CRISC, CDPSE
South Africa

Sanja Kekic
CRISC, CDPSE
Serbia

Michael Podemski
CISA, CISM, CRISC, CDPSE
USA

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FAISA, FACS
Australia

Patricia Voight
CISA, CISM, CGEIT, CRISC, CDPSE
USA

Board of Directors

John De Santis, Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Brennan P. Baybeck, Vice-Chair
CISA, CISM, CRISC, CISSP
Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Stephen Gilfus
Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP, NACD.DC
Former Chief Information Security Officer, United Nations Office for Project Services (UNOPS), USA

Gabriela Hernandez-Cardoso
NACD.DC
Independent Board Member, Mexico

Jason Lau
CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP
Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo
Independent Director, Former Chief Executive Officer and Executive Director, VADS Berhad Telekom, Malaysia

Maureen O'Connell
NACD.DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Erik Prusch
Chief Executive Officer, ISACA, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., Israel

Pamela Nigro
ISACA Board Chair 2022-2023
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

Gregory Touhill
ISACA Board Chair 2021-2022
CISM, CISSP
Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its more than 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *Digital Trust Board Briefing* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

X:
www.x.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/