Incentivizing Trustworthy Technologies

Spring 2023

COLUMBIA | SIPA
School of International and Public Affairs

PRESENTED TO
SAP

Table of Contents

Our Team

Nitisha Tripathi

Project Manager

Jose Pablo Ampudia

Client Liaison

Emmy Peng

Fieldwork Coordinator

Shuqi Ding

SIPA Liaison

Jian Gu

Editor

Acknowledgements

We would like to express our sincere gratitude to all those who contributed to the successful completion of this report.

First and foremost, we extend our deepest appreciation to our capstone advisor, Daniel Dobrygowski, for their invaluable guidance and support throughout the project. Their expertise, insights, and feedback were instrumental in shaping the direction of our work and ensuring its quality.

We are also grateful to the SAP for providing us with the opportunity to undertake this project and for their ongoing support throughout the process. We are particularly thankful to Debbie Greif and Michelle Barrett-Chang for their efforts.

In addition, we extend our sincere appreciation to the experts and organizations who generously shared their time, knowledge, and expertise with us. Their contributions were essential in informing our research and analysis, and we are deeply grateful for their willingness to participate.

Thank you all for your invaluable contributions.

Excecutive Summary

“Trust, But Verify” is a familiar phrase. However, what if there is no need for verification? How would our society understand and perceive technology if incorporation of trust in its development could be incentivised from the outset? This capstone project seeks to explore answers to these questions and identify how digital trust can become a distinct market category of investment for SAP.

Since its establishment in 1972, SAP has revolutionized the management of business processes and streamlining of information flow across businesses. Its position as a market leader and advocate for security and privacy has created the expectation for it to emerge as a leader in bridging the widening trust gap in use of digital technologies between industry, government and individuals. This project is focused on facilitating SAP’s efforts in this regard through three key approaches: proposing an all-inclusive definition of digital trust to reprioritise its investment objectives, analyzing emerging and established risks and trends associated with digital trust and creating a framework for SAP to understand its trust ecosystem and measure its effectiveness.

In the era of digital distrust, there is a need to change the traditional understanding of establishing and maintaining trust. Compliance is no longer an indicator of trustworthiness. To ensure targeted investment of available resources, it needs to be evaluated as an interplaying factor between Security and Privacy, rather than an independent contributor to trust. Increased importance to factors that influence trust towards a brand or company, such as, quality, availability, transparency, ethics and integrity has to be demonstrated through established and frequently monitored processes.

Deteriorating confidence in digital systems and technologies necessitates a distinct and dedicated approach towards assessing risks associated with digital trust. This project, in a departure from approaches that do not account for the ‘perspective of trust’ offered by security and privacy objectives of a company, identifies risks facing SAP with the potential to impact its trustworthiness. Additionally, it explains the existing and future regulatory, market, technological, workforce and normative trends, that are impacting/can impact the operations

Cultivation of a ‘trust measurement mindset’ can effectively position SAP as a trusted and ethical leader of security and privacy practices in the industry. The analysis and actionable recommendations provided by this project aim to contribute to this mindset by proposing a framework to incentivize SAP’s efforts towards establishment, maintenance and reinforcement of trust in its products and services. It defines the extent and nature of operation of different stakeholders in the trust ecosystem of a company like SAP, explains the phases of a trust lifecycle and proposes a detailed set of macro and micro level knowledge performance indicators to track and measure the success and failure of SAP’s efforts towards achievement of its security and privacy goals.

Chapter I: Introduction

I. Background

Technology is present in everyday activities and in every interaction between people, businesses, organizations, and governments. Our increasing reliance on technology for interaction cannot be understated; however, organizations often overlook a critical factor that enables it: the trustworthiness of the technologies they use. If trust is the "belief that something is safe and reliable"[1], digital trust is the belief that technology is safe and reliable. In other words, digital trust is the "*individuals' expectation that digital technologies and services –and the organizations providing them– will protect all stakeholders' interests and uphold societal expectations and values*."[2] In an increasingly complex era of cyber-attacks, data breaches and privacy violations, digital trust has become a necessity for the success of businesses. A fissure in the trust on technology impedes innovation, economic expansion, integration, and growth.

Erosion of trust in institutions and businesses has reached at an unprecedented level[3]. This has created a unique opportunity for businesses to make trust-building and trust-maintenance a competitive advantage. Furthermore, as digitization continues to evolve and impact each aspect of our society, the role of digital trust in enabling people, organizations, and institutions to connect and interact with confidence is expected to become even more critical. It's absence could hinder the adoption and use of digital technologies and services. This is particularly important for businesses that rely on digital channels to connect with their customers and operate.[4] Therefore, this is a pivotal moment for companies to prioritize investment in the trustworthiness of the security and privacy of their digital infrastructure, while also ensuring compliance with regulations and integrating transparent, accountable, and ethical practices from the outset.

Recent global developments have heightened the need for businesses to stay vigilant and proactive with their efforts towards trust building. The COVID-19 epidemic has accelerated the adoption of digital technology for remote work, virtual learning, and online commerce, underscoring the crucial role that digital infrastructure plays in sustaining our daily life.[5] As our reliance on technology increased, so did our dependency on digital platforms to interact with each other. With a steady rise of the usage of social media,[6] more and more data is shared with and between online platforms who have been criticized for their obscure data sharing practices, lack of accountability and transparency. Furthermore, as we continued to move online, threats to personal devices, companies, and vital infrastructure multiplied, resulting in countless incidents displaying their potential to disrupt and cause damage.[7] A crucial lesson has been highlighted by these developments – digital trust is not a one-time event but an ongoing process that requires continuous effort and investment to adapt to the evolving digital landscape and changing stakeholder expectations.

II. Purpose of the report:

To address the growing need for digital trust, we have conducted qualitative data analysis of secondary research and information gathered from interviews with market experts to develop a comprehensive framework to provide guidance on how to establish and sustain it. Our framework is designed to assist companies in all industries that produce or utilize technology at any level and aspect of their operations to define, measure, and invest adequately in building and maintaining trust with their customers. While we have specifically focused on SAP, we believe that our framework can be valuable for all enterprises that depend on technology, regardless of their industry or sector, and hopefully to the field as a whole.

In particular, this report aims to address key questions that are at the heart of the digital trust discussion, including its definition, the factors that influence trust in a brand or company, and how to build a business case for trust and trustworthy technology across industries. It provides an overview of the main components of digital trust, identifies the main risks associated with it, and presents possible mitigation strategies. Additionally, the report offers metrics that companies can use to identify areas for improvement in their overall trustworthiness, with a particular focus on security and privacy.

While this report offers valuable insights and practical guidance on building and maintaining digital trust, it is important to note that it does not provide an exhaustive list of all possible strategies or solutions. Additionally, given the constantly evolving nature of technology and the digital landscape, new risks and challenges may arise that are not covered in this report. Therefore, companies should adapt their strategies accordingly in order to ensure they maintain trust from their customers.

Chapter 2: Definitions of Digital Trust

In the previous section, we discussed the importance of establishing strong relationships with customers, partners, and stakeholders, emphasizing the need for digital trust. However, building and maintaining digital trust is not a simple task. The first challenge is to define what digital trust means and determine whether there is a universal definition or if it varies based on an organization's unique characteristics and requirements. To address these issues, this section will provide an overview of existing definitions from various entities, analyze the critical components of digital trust as identified by experts, and propose a customized definition for SAP, along with the components that SAP should prioritize to enhance customer loyalty and trust.

I. Existing Definitions and Expectations of Digital Trust

What does digital trust actually entail, and how can organizations ensure they meet the expectations of their stakeholders? To answer these questions, it is crucial to explore the existing definitions of digital trust offered by various entities. By examining these definitions, we can gain a better understanding of the key components and factors that influence digital trust. We have identified several definitions that stand out:

Organization	Key Features	Similarities to others
World Economic Forum	Individuals' expectation that digital technologies and services - and the organizations providing them - will protect all stakeholders' interests and uphold societal expectations and values[8]	Emphasizes trust in digital platforms and systems
ISACA	Confidence in the integrity of relationships, interactions, and transactions in a digital ecosystem[9]	Highlights trust in relationships and interactions
Microsoft	Confidence in security, privacy, and reliability of digital systems, processes, and data. Microsoft's mission is to empower everyone to achieve more, and the company builds its products and services with security, privacy, compliance, and transparency in mind[10]	Concentrates on security, privacy, and reliability, and the importance of compliance and transparency

Organization	Key Features	Similarities to others
McKinsey	Consumer faith in cybersecurity, data privacy, and responsible AI[11]	Focuses on cybersecurity, data privacy, and responsible AI
Deloitte	Confidence in an organization's ability to create and maintain the integrity of all digital assets[12]	Underscores transparency, accessibility, security, reliability, privacy, control, ethics, and responsibility
Okta	Confidence in an organization's ability to protect its information assets and technology resources[13]	Stresses information security and protection

II. SAP's Definition of Digital Trust

Digital trust, according to SAP, refers to the degree of assurance that an organization can appropriately govern and exploit data while adhering to robust security, management, and compliance procedures[14]. The pillars of confidence i.e., privacy, security, and compliance are all vital components of establishing and maintaining this digital trust. Furthermore, it encompasses having faith in not only technology but also people and processes to develop a safe digital environment.

To ensure security practices for their clients, SAP employs, controls and monitors dubious actions. At every stage of product development, SAP incorporates various security measures and processes to ensure that their business operations run smoothly. As a result, they automatically integrate security essentials into the overall workflow. Correspondingly, when it comes to privacy concerns, SAP is committed to safeguarding personal data against any unauthorized access from external parties. It continually educates its personnel on how best to secure customer and internal data by implementing strict policies and procedures. Moreover, adherence to compliance is essential for SAP as it aligns with NIST guidelines in conducting regulatory practices among other industry best practices. Lastly, through transparency initiatives, customer satisfaction increases since the security policy and process information is readily available through easily accessible channels. To acquire a refined comprehension of the security requirements of customers, it is necessary to actively engage with them.

Compared with others' definitions, a major difference in SAP's outlook is that it takes a holistic approach to recognize that trust is not just one aspect of digital operations, but a combination of different factors working together. Moreover, SAP's approach marks the importance of automating security activities to simplify business processes. This approach is consistent with the industry trend to use automation and artificial intelligence to improve safety and compliance operations. By automating these activities, organizations are likely to reduce the risk of human error and ensure that security and compliance requirements are always met. This also frees up resources that can be used directly in other areas of the business, ultimately increasing efficiency and effectiveness.

III. Key components of digital trust

There are several key components of digital trust that organizations must address to build and maintain trust with their users. SAP already encompasses four components in its understanding of digital trust: security, privacy, compliance and transparency[15].

1. **Security**: Building and maintaining confidence of customers (client companies), regulatory authority, employees and society of the organization:

    - to protect its assets in cloud and hybrid landscape, from internal and external threats, to update and optimize its business continuity management
    - to facilitate transparency through embedded and automated data protection systems
    - to comply with security standards and regulations
    - to subject itself to an independent security audit.

2. **Privacy**: Digital trust requires that personal data is collected, processed, and used in a manner that respects the privacy rights of individuals. Stakeholders need to be confident about how a company governs the use, processing and sharing of their data and that it is carried out without compromising on security, management, or compliance.

3. **Compliance**: The extent to which organizations adhere to relevant laws, regulations, and industry standards is defined as compliance. It is important for building trust because it demonstrates that organizations are taking responsibility for their actions and are committed to protecting user data and privacy. Compliance can help prevent data breaches and other security incidents that can damage user trust.

4. **Transparency**: It requires transparency in how digital systems and services operate, including how algorithms and data are used. This includes being transparent about the criteria used to make decisions, such as for credit scoring or job hiring, and the sources of data used in these decisions.

However, according to **Kathryn K. White**[16] "o*ther components like fairness and interoperability should also be considered*."

- **Fairness**: This ensures that digital systems and services are not biased or discriminatory, and that they treat all users in an equitable and non-discriminatory manner. This is particularly important in contexts such as hiring, lending, or insurance, where automated decision-making systems can inadvertently perpetuate bias and discrimination.

- **Interoperability**: The ability of different digital systems and services to work together seamlessly. This is crucial for ensuring that users can easily access and use the services they need, regardless of the platform or device they are using.

Christopher Chew[17] also noted that "*Trust is built when you have accountability and transparency…*"

- **Accountability**: The responsibility of organizations to be answerable for and to take ownership of any negative consequences that may result from their actions. This includes being accountable for data breaches, system failures, and other incidents that may impact a user's trust. Organizations can demonstrate accountability by having clear policies and procedures in place for managing data security and privacy, by being transparent about their data collection and processing practices and by sharing information about how they handled incidents of breaches, attacks and other failures.

- **Transparency**: The extent to which organizations are open and honest about their actions and decisions. Transparency can help build trust by providing users with a clear understanding of how their data is being collected, processed, and used. This includes providing users with clear, easy to understand and concise security and privacy policies, making it easy for them to understand, access and manage their data.

- **Control**: The ability of users to control their own data and digital experiences. This includes giving users the ability to choose what data they share, who they share it with, and how it is used. By giving users more control over their data, organizations can build trust by demonstrating that they respect users' privacy and autonomy.

Theresa Peterson[18] from Edelman Trust Institute said "*Trust is a forward-looking metric that gives companies license to act. It is built through demonstrating competence and ethics. Trust can be thought of as a currency that companies must earn—if companies have more trust in their 'trust bank,' they are more able to take risks and operate in society.*"

- **Competence**: Ability of companies to efficiently conduct their work , including business, technologies, compliance with regulations, etc. When a company is competent, it is able to deliver on its promises and meet the expectations of its stakeholders, which can build trust.

- **Ethics**: The moral principles and values that guide a company's actions and decisions. It is to see how realistic and transparent companies are to stakeholders. It can build trust by demonstrating that the company has a genuine concern for the well-being of its stakeholders.

Diana Kearns-Manolatos expects confidence, intent and imperatives to build trust.

- **Confidence**: Confidence of all stakeholders on the ability of a company to incorporate and maintain integrity of their digital assets. It's the extension of how we think about trust more broadly, in the context of any type of digital asset that one would be looking to create for an organization or for stakeholders.

- **Intent**: Deliberately taking actions to build confidence in trustworthiness of a company and making sure that a company has the capabilities required to create such confidence.

- **Imperatives**: Combination of experiences, insights, platforms, connectivity, and integrity. This combination can per perceived as the digital tech stack of the future as well as the business goals matrix of the future.

Other key components or elements of digital trust are also essential for building and maintaining trust in digital environments, like reliability, responsiveness, and reputation.

- **Reliability**: Ensuring that digital services are available when needed, and that they perform as expected without errors or downtime.

- **Responsiveness**: Digital systems and services must be responsive to user needs and concerns. This includes providing timely support and responding to feedback and complaints in a timely and effective manner.

- **Reputation**: Trustworthiness in use of technology impacts the reputation of a company as well. Perception of trust is directly proportional to the degree of efforts taken by a company to be transparent and accountable about their use of technology. Organizations that have a positive reputation for providing reliable, secure, and privacy-respecting services are more likely to build trust with their users. Similarly, absence of such services can result in a loss of trust, creating a weak and negative brand reputation.

IV. A New Definition

As previously discussed, the concept of digital trust and its components vary depending on the organization and its unique characteristics. SAP, for instance, defines digital trust as the degree of assurance that an organization can appropriately govern and exploit data while adhering to robust security, management, and compliance procedures, and has identified four components of digital trust, namely security, privacy, compliance, and transparency.

However, considering the dynamic and evolving nature of digital trust, it is essential to capture the context and nuance of a technology's operation to make it trustworthy. Our research and analysis indicates that digital trust can be distilled down to two critical elements: Security and Privacy. Compliance acts as the interplaying factor between security and privacy. Acknowledging it as a distinct component creates the wrong assumption that it guarantees trust in the technology used by a company and in the company itself. This also results in de-prioritizing investment by a company in all the other factors that influence the trustworthiness of a company, such as transparency, accountability, and reliability. In other words, being compliant with regulations and standards is a necessary prerequisite for establishing trust, but it is not sufficient on its own. Mere meeting of rules and legal requirements is not sufficient to establish trust with stakeholders.

Compliance should be viewed as the 'bare minimum' efforts made to achieve a goal and not the ultimate goal itself. A company's legal, rule and regulatory compliance is only the starting point for building trust, and it does not necessarily mean that the company is trustworthy. Furthermore, compliance is not a static concept but rather an ongoing process. As new regulations and standards emerge,ja organizations must continuously adapt their practices to remain compliant. Compliance alone, therefore, cannot guarantee digital trust since it is subject to change and may not always align with the expectations and needs of stakeholders.

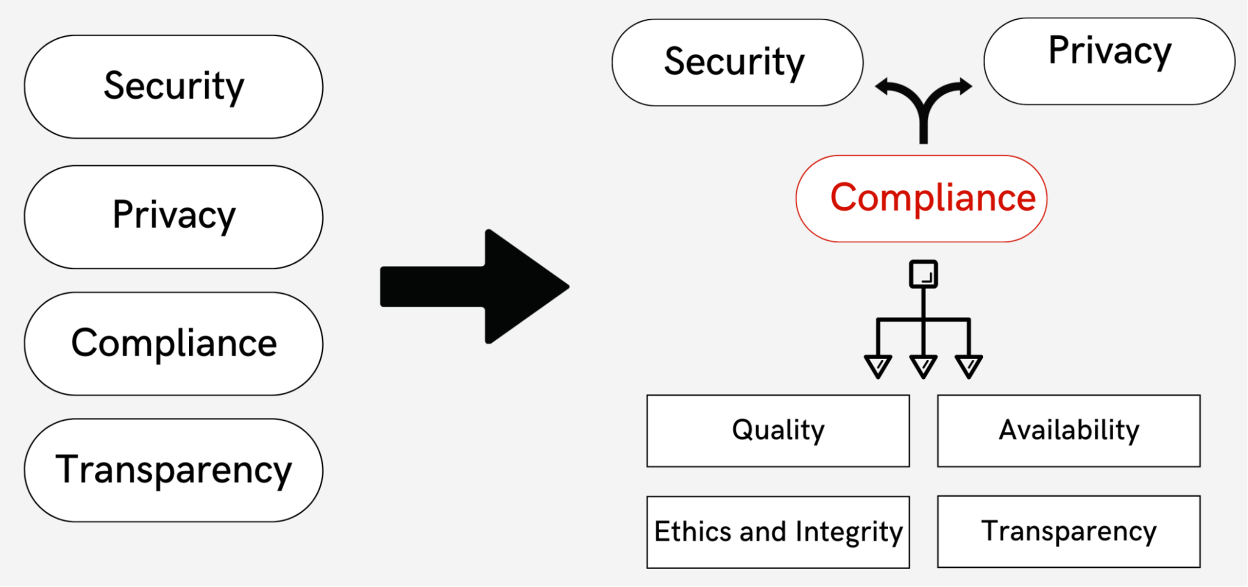


Figure 1: Proposed Change to SAP's Approach Towards Components of Digital Trust

Organizations must focus on establishing supporting building of strong foundation for security and privacy through incorporation of ethical considerations, transparency, accountability, and availability to build lasting trust with their users. This can lead to trustworthy best practices for building and maintaining security and privacy. In this regard, 'Security' refers to the measures that organizations take to protect their digital systems and services from unauthorized access, use, and modification. It encompasses a range of practices, such as access controls, encryption, and threat detection, that help safeguard sensitive data and prevent cyberattacks. 'Privacy', on the other hand, relates to how organizations collect, use, store, and share personal data. It includes practices such as data minimization, user consent, and transparent disclosure of data practices, which help ensure that users' privacy rights are respected and protected.

Chapter 3: Risks to Digital Trust

With the rapid growth of the digital ecosystem, risks to digital trust are also growing. To address these risks effectively, it is essential to classify them and develop mitigation strategies. In this section, we will explore different types of risks to digital trust and their classification. Beginning with an overview of the principles used to understand risks to digital trust, we will discuss how risks to digital trust can be classified based on a) the level of impact they create, such as high-level, medium-level, or low-level risks and b) their relationship with the trust ecosystem. Finally, we will discuss risks specific to security and privacy with compliance as an interplaying factor between them and, provide mitigation strategies to address the identified risks.

I. Risk Classification

A risk can be defined as "*A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of the following: the adverse impacts that would arise if the circumstance or event occurs; and the likelihood of occurrence. Likelihood is influenced by the ease of exploit and the frequency with which an assessment object is being attacked at present*"[19]. However, so far, risk has been restricted to an assessment of its impact on the security or privacy or compliance architecture or practices of a company. The evaluation of risks as they relate to digital trust has witnessed limited exploration.

Four key principles[20] can be considered to understand risks to digital trust:

1. **Severity:** What is the extent of effect on a stakeholder's life? (Refer to Figure 1)
2. **Simplicity:** What is the effect of complex policies and processes of security, privacy and compliance on functioning of different stakeholders i.e., does that complexity inhibit or liberate their operations?
3. **Transparency:** What is the extent and frequency of openness that is exercised in maintaining relationships with all stakeholders?
4. **Repeatability:** What is the extent to which the policies and processes of security, privacy and compliance are consistently repeated to different stakeholders?

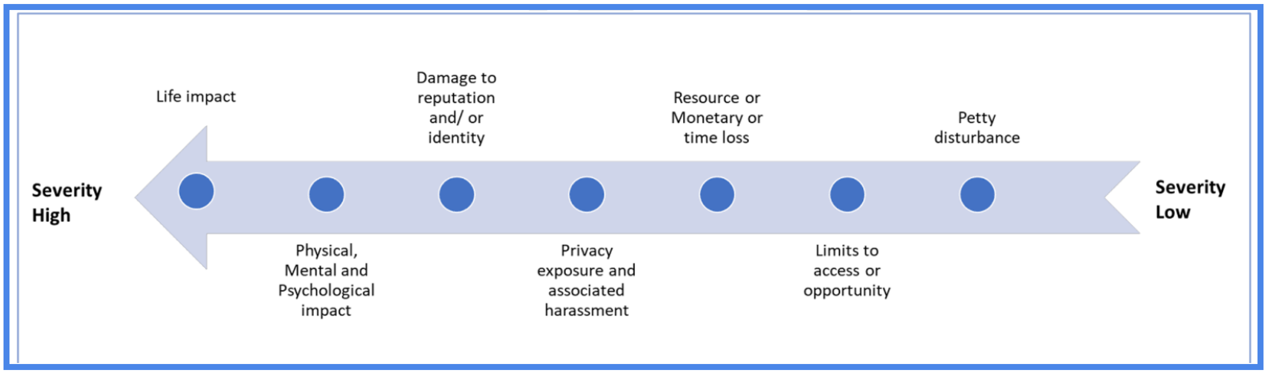

Severity High
Life impact
Physical, Mental and Psychological impact
Damage to reputation and/ or identity
Privacy exposure and associated harassment
Resource or Monetary or time loss
Limits to access or opportunity
Petty disturbance
Severity Low

Figure 2: An illustrative representation of risk consideration in terms of impact severity[21]

Assessment of risks on the basis of above principles can lead to its classification through following two approaches:

1. Based on the level of impact it creates risk to digital trust with high-level, medium-level or low-level impact

A high-level risk to digital trust is created when impact severity is such that it can cause harm to the health, safety and security of customers, government, employees and society and/or effect functioning of services essential to economy, society and government.

A medium-level risk to digital trust is created when harm may be caused or is anticipated to impact the health, safety and security of customers, government, employees and society.

A low-level risk to digital trust exists when impact severity is such that it has limited bearing on safety, health, security of customers, government, employees and society and does not harm them physically or financially and potentially limit their access to services.

2. Based on its relationship with the stakeholders within an ecosystem, risk to digital trust can be either mechanical or relational[22]

A risk to trust is mechanical when it affects the ability of the security, privacy and compliance technologies and processes of the company to deliver a predefined output, impacting the predictability of its systems.

A risk to trust is relational when all the trust actors are not in shared agreement about the 'when, where, how and why' of the technologies used.

II. Component Specific Risks & Mitigation Strategies

After establishing the groundwork and classification methods for digital trust risks, we can proceed to examine specific risks related to its key components: security and privacy. Amongst the analyzed risks are those associated with cyber-attacks, data breaches, and non-compliance with regulations, industry standards. These risks can compromise digital trust by leading to financial losses, reputational damage, and the loss of personal information.

To mitigate these risks, we provide an overview of effective mitigation strategies that individuals and organizations can implement. These strategies can assist in minimizing the impact of these risks, protect their assets and reputation, and maintain trust in the digital environment

1. Security

Category of Trust at Risk	Risk	Likelihood	Impact	Mitigation
Mechanical	Exposure of SAP Confidential data and loss of trade secret rights	Medium	High-level	Use efficiency and security enhancing tools, including but not limited to status code, vulnerability analysis tools
Mechanical	Open source violations and contamination	Medium	High-level	Third party risk management, secure process for reporting vulnerabilities with timeline for fixing them

Relational	Loss of contracts with government entities due to lax cybersecurity controls, processes as 12 May 2021 Executive Order of the President of United States has emphasized on stronger cybersecurity standards to be implemented by the private sector.	High	High-level	Compliance with NIST Cybersecurity Framework, conducting frequent security audits
Mechanical	Introduction of security vulnerabilities	High	High-level	Rigorous testing suite and change management processes
Relational	Decentralization of cybersecurity has fragmented the responsibility and accountability to multiple stakeholders in the systems.	Medium	Low-level	Open communication with partners and rivals to establish a common security defense. Training third parties on requisite security protocols/processes
Mechanical	Catastrophic cyber attack on SAP's infrastructure.	Medium	High-level	Increased public-private co-operation to pre-empt or preliminarily assess any incident and proactive investment in skilling and reskilling of workforce in critical cybersecurity skills

Mechanical	Outdated and obsolete code	Medium	Medium-level	Frequent inventory, monitoring and upgradation of softwares and hardwares to ensure that the trusted relationship of a company as a secure supplier is maintained
Relational	Customer's inability to stay up to date with the processes, systems put in place by SAP to maintain security of products.	High	Medium-level	Proactive and frequent sharing of information on updates, policies, processes on security, threat and vulnerability management displaying a commitment towards investment in the security posture of customer companies
Mechanical	Biased, Non-confidential AI systems, training data and output	Medium	Medium-level	Increased security for AI systems and their data, constant monitoring to check for bias according to voluntary frameworks, for e.g. NIST Bias framework
Relational	Lack of frequent security-specific skilling of employees to maintain trust in their ability and competence	Medium	Medium-level	Sponsored Comp TIA+ trainings, Trust Trainings for employees involving training them in trustworthiness principles and guidelines

Relational	Inability to comply with multiple and competing global regulations	Medium	High-level	Timely and frequent coordination between legal, product, engineering and trust teams through established processes
Relational	Penalties for cybersecurity breaches	High	Medium-level	Ensure compliance with existing laws, regulations and conduct necessary due diligence to prevent instances that invite liability for a company

II. Privacy

Category of Trust at Risk	Risk	Likelihood	Impact	Mitigation
Relational	Inability to meet the requirements of various data protection regulations across different regions of the world, resulting in non-compliance and potential legal and financial penalties, together with potential loss of trust and customers.	Medium	High-level	Establish a comprehensive privacy program together with a strong compliance and legal team to ensure alignment with applicable laws and regulations and regularly monitor changes in the regulatory landscape.

Relational	Third-party vendor and supplier breaches.	High	High-level	Implement strong vendor management protocols, conduct due diligence on vendors and suppliers, require vendors to sign privacy and data protection agreements, and regularly monitor vendor and supplier activity
Relational	Weak data minimization and user consent practices.	High	Medium-level	Implement strict data minimization policies and procedures, provide clear and concise explanations of user data collection and use, obtain explicit consent from users for all data collection and use, and regularly review and updating privacy policies to ensure compliance with changing regulations and standards. Delete dark privacy patterns.
Relational	Inadequate disclosure of commitments and policies related to privacy and data protection, leading to low levels of user trust and confidence.	High	Medium-level	Increase transparency and disclosure of commitments and policies related to privacy and data protection through regular and comprehensive reporting to users and stakeholders.
Relational	Poor performance compared to industry peers in terms of privacy and data protection practices, leading to lower levels of user trust and competitive disadvantage.	Medium	Low-level	Conduct regular benchmarking exercises against industry peers and implement necessary changes to improve privacy and data protection practices.

Relational	Potential damage claims by customers and individuals by inadequate use or sharing of information.	Medium	Medium-level	Ensure compliance with all regulations and guidelines, maintain transparency and communication with customers/contractors, and have a plan in place to address any breaches or violations.
Relational	Inability to incorporate user feedback and requests for privacy-related enhancements and features into SAP products and solutions, leading to lower levels of customer satisfaction and loyalty.	Low	Medium-level	Implement a structured approach for incorporating user feedback and requests for privacy-related enhancements and features into SAP products and solutions.
Relational	Inability to meet the requirements of various data protection regulations across different regions of the world, resulting in non-compliance and potential legal and financial penalties, together with potential loss of trust and customers.	Medium	High-level	Establish a comprehensive privacy program together with a strong compliance and legal team to ensure alignment with applicable laws and regulations and regularly monitor changes in the regulatory landscape.
Relational	Third-party vendor and supplier breaches.	High	High-level	Implement strong vendor management protocols, conduct due diligence on vendors and suppliers, require vendors to sign privacy and data protection agreements, and regularly monitor vendor and supplier activity

Relational	Weak data minimization and user consent practices.	High	Medium-level	Implement strict data minimization policies and procedures, provide clear and concise explanations of user data collection and use, obtain explicit consent from users for all data collection and use, and regularly review and updating privacy policies to ensure compliance with changing regulations and standards. Delete dark privacy patterns.
Relational	Inadequate disclosure of commitments and policies related to privacy and data protection, leading to low levels of user trust and confidence.	High	Medium-level	Increase transparency and disclosure of commitments and policies related to privacy and data protection through regular and comprehensive reporting to users and stakeholders.
Relational	Poor performance compared to industry peers in terms of privacy and data protection practices, leading to lower levels of user trust and competitive disadvantage.	Medium	Low-level	Conduct regular benchmarking exercises against industry peers and implement necessary changes to improve privacy and data protection practices.

Chapter 4: Trends in Digital Trust

As digital technologies continue to evolve and expand, it is essential to anticipate the potential trends that may emerge and impact the components of digital trust. In this section, we will explore the potential trends related to security and privacy, as well as to compliance and their influence on digital trust and technology.

Trends in digital trust and technology can be witnessed and forecasted from two aspects: existing trends (including regulatory, market, and technical trends), and future trends (including workforce and normative trends). By analyzing these trends, individuals and organizations can better anticipate and prepare for future challenges related to digital trust and technology. By staying ahead of emerging trends, they can develop effective strategies and solutions to mitigate risks and build a more trustworthy digital ecosystem.

I. Regulatory/Legal Trends

When it comes to digital interactions, regulatory frameworks are essential for laying down the guidelines and norms. These frameworks lay down the legal obligations of individuals and organizations pertaining to the collection, usage, and protection of digital assets or data. By staying updated on regulatory trends, stakeholders can comprehend and prepare for the fluctuating standards and demands for digital trust. This understanding facilitates proactive steps towards maintaining compliance as well as building trust with stakeholders.

1) Increasing Regulatory Requirements

Regulations are crucial in shaping the direction of the industry, guiding the operation of organizations, building trust between organizations and customers, and protecting stakeholders' rights. By having more regulations and by having more organizations comply with existing regulations, technology providers are more likely to gain trust from users and stakeholders.

Beyond the simple rise in the number of regulations, there is an increasing trend of formulating region-specific regulations by governments to regulate company operations and to protect consumer rights within respective geographical region. In the United States, California Consumer Privacy Act[23] (CCPA) became effective in January 2020, and has applied to businesses operating in California and processes the personal data of California residents. In the European Union, General Data Protection Regulation[24] (GDPR) applies to all organizations that process the personal data of individuals within the EU, regardless of where the organization is based.

There are also more security-specific and privacy-specific regulations designed to ensure that the products and services organizations provide are aimed at making users feel secure and trustworthy. For security, organizations have developed ISO 27001, SOC 2, and NIST Cybersecurity Framework[25], as security standards for technology providers to follow and comply with.

2) Moving from Self-Assessment to More Directive Control Frameworks

In an evident shift from self-assessment, there is an emergence of more directive control frameworks to regulate the industry operations. These require mandatory incident reporting, external audit, timely disclosure of ransomware incidents. For example, the EU Cybersecurity Certification Framework[26] is a set of rules and procedures designed to establish a common framework for cybersecurity certification of digital products, services, and processes. Under this framework, cybersecurity certification schemes will be created for ICT products that will specify a level of assurance for each project based on the level of risk associated with the expected use of such products.

3) Potential Regulatory Risks

The shift in perception regarding the effectiveness of cybersecurity regulations is an important trend in the risks to digital trust. While regulations can be effective in promoting cybersecurity and resilience, they can also be seen as overly duplicative and burdensome, taking resources away from core efforts to maintain and protect cybersecurity.

There is growing recognition that regulations can be effective in promoting cyber resilience, but they must be properly enforced to be effective. Regulators are increasingly imposing fines and other penalties for non-compliance, and organizations are responding by devoting more resources to compliance efforts. However, the increasing frequency and severity of cyber incidents, fines, and investigations have elevated the perception of regulations as a critical influence on organizations' cyber resilience. Business and cyber leaders support effective enforcement of regulatory requirements, as they believe that properly enforced regulations will raise the quality of cybersecurity across their sector and supply chains, ultimately making their business less prone to collateral damage from attacks on other organizations.

The continuously expanding and changing regulations can present challenges for organizations in terms of compliance and implementation. Business leaders may also fear hefty fines more than they value the contribution regulations make to development of collaborative cyber policies. Nonetheless, regulations are a valuable starting point for embedding cyber-resilience techniques across an organization, and boards actively respond to them. The increasing awareness of the demand for cyber resources within organizations suggests a need for more effective implementation and enforcement of regulations, as well as a greater understanding of the contribution that a collaborative multi-stakeholder approach can play in ensuring enactment of sustainable, balanced regulatory regime.

II. Market Trends

An organization's ability to stay on top of changing consumer tastes and preferences is crucial for success. Market trends provide an important barometer of evolving attitudes towards products and services, pointing towards what influences consumer confidence in diverse situations. By analyzing market trends, businesses gain a deeper understanding of the levers driving trust, enabling them to align their strategies accordingly.

1) Fragmentation of Responsibility and Accountability

The level of complexity and interdependence among business departments in technology and software companies is increasing rapidly and continuously. The classical boundaries separating businesses, operational technology, information technology, and connected digital products have been erased. The burden of ensuring a trustful digital environment has shifted from single actors to multiple internal and external stakeholders. To establish digital trust within a layered and complex architecture, responsibility has been subdivided. Governance models, such as the NIST Cybersecurity Framework 2.0[27] reflect the emphasis on this transition.

2) Greater Emphasis on Transparency

As consumers become increasingly anxious about the manner in which their data is gathered and handled, organizations have begun to respond with enhanced transparency measures such as more comprehensive privacy regulations and disclosures. These initiatives include streamlining individual access to personal data for review or modification purposes while empowering users through provision of greater authority over management of their information.

3) Rise of Data Trust as a Business Model

More independent third parties are involved in data control on the behalf of the company. Companies must carefully choose the data-control party based on their clients' preferences. They must also carefully scrutinize and manage how to convey data usage and information to their clients, and where and when to engage them in the process. Data trusts can provide a wide range of benefits like reduced data silos, access to trusted and audited data, and greater control, along with enhanced organizational reputation from moral and transparent data collection and usage. While digital trust improves the confidence of companies in the data and the insights developed from it, data trust can be increased by authenticating a single source of information that makes data management and sharing much easier and more trusted.

4) Incident Response Planning

Incident response planning has become a crucial aspect in preparation for cyber attacks among organizations. With such a plan in place, companies can take necessary actions during and after an attack, including notifying affected parties and reducing overall damage. In addition, incident response planning enables companies to save significant amounts of money by reducing their response costs in case of any breach. The efficiency of this plan allows quick recovery from such attacks minimizing negative financial effects.

5) Rise of Third-Party Management

To maintain stable operations, software companies often rely on third-party vendors who provide necessary elements like cloud infrastructure, data storage systems or software development tools. As these third-party vendors are subject to occasional systemic vulnerabilities within their own operation schemes, it is likely that a problem with one provider could negatively impact an organization’s overall technological setup. Consequently, companies increasingly focus on risk management measures concerning their service providers by demanding adherence to specific regulations aimed at ensuring high levels of security while also monitoring vendor actions closely.

6) Privacy by Design

To address concerns surrounding privacy, a growing number of software firms have adopted "privacy by design" protocols, meaning they implement aspects related to privacy and data protection during each phase of product creation. These principles not only lead to more robust safeguards on user information but also foster confidence with clientele while also reducing possible legal exposure from any future breaches.

III. Technology Trends

The advancement of technology has become an essential tool for facilitating digital interactions and plays a crucial part in shaping digital trust. It is therefore imperative for organizations to stay informed about emerging technological trends to make sound judgments concerning technology adoption, security protocols, and other effective tactics for nurturing and sustaining trust in the dynamic digital environment.

1) Rise of Multi-Factor Authentication

To bolster system security, various institutions have started adopting multi-factor authentication protocols that require users to provide additional credentials and a password. A code sent via text message or email is one example of such verification measures. The adoption of multi-faceted authentication adds a supplementary layer that reduces the risk of unauthorized access into user accounts..

2) Using Blockchain to Establish Security Systems

Blockchain technology offers a promising solution for companies seeking to implement decentralization. With a decentralized network of nodes securely storing and verifying data using transparent and immutable blockchain ledgers, companies can significantly reduce the risk of fraudulent activities occurring while increasing accountability amongst stakeholders. Furthermore, recording all activities allows for transparency throughout the entire process.

3) Adoption of Privacy-Enhancing Technologies

The emergence of advanced technologies has opened up possibilities for protecting sensitive information within organizations. Key among these technologies are encryption and anonymization techniques, which block unauthorized access to personal data. Furthermore, employing differential privacy measures allows companies to glean important insights without revealing identifying elements about individuals.

4) Emerging Technology Pose Risks

Emerging technology can pose significant risks to digital trust as organizations adopt new technologies to improve their operations and services. With the increasing use of technologies such as artificial intelligence (AI), machine learning, and cloud computing, the complexity of an organization's digital environment is significantly increasing, requiring them to embed cyber-risk management throughout the entire digital transformation process.

While most organizational leaders appreciate the impact of emerging technology on their cyber-risk profile, there is a need to balance the value of new technology with the potential cyber exposure that comes with it. Business and cyber leaders are closely aligned in their perspectives on emerging technology and its impact on cyber-risk strategies.

According to the Global Cybersecurity Outlook 2023 report by the World Economic Forum[28], AI and machine learning, greater adoption of cloud technology, and advances in user identity and access management are the top three emerging technologies that will have the most significant influence on organizations' cyber-risk strategies over the next two years. However, respondents did not rank other categories of emerging technology significantly lower than the top three, indicating that organizations will implement new technologies in combination, further increasing the complexity of their digital environment.

5) Usage of Automation

More automation tools are used in the operations of organizations to automate tasks and to provide services. These tools can be programmed to perform specific tasks based on predefined rules or conditions. Besides daily technical operations, automation tools have recently also been involved in safety and compliance operations. This helps in streamlining repetitive and time-consuming tasks and reduces the risk of human errors, improving efficiency, accuracy, quality, and productivity of digital products and services. A classic example of this trend is reflected in the automation of security questionnaires[29] that reduces the amount of time invested in assessing customer's satisfaction and understanding of the security controls and processes of a company.

However, our interviewees have shared the need to exercise caution with respect to the techno-solutionism approach that automation processes are likely to adopt. They emphasize on the idea that it is the everyday processes that can be automated to minimize time investment of the team in menial tasks but trust, per se, is a complex phenomena to automate.

IV. Workforce Trends

1) Expansion of understanding of the term 'workforce' & Rise of 'workforce ecosystem'

There are three components of the workforce ecosystem: an individual, an organization, or a piece of technology that is contributing to the creation of value for the organization. A study mentions[30] that *"87% or more are thinking of technology, service providers, ecosystem partners, apps and accessory providers as part of their workforce as well"*. The workforce ecosystem is being considered as a much broader and more holistic concept. In terms of creating digital trust, organizations are not only monitoring their full time employees as internal threat actors, but also including more related actors and organizations[31].

2) Growing Importance of External Contributors

As opposed to the full time and part time employees of a company, a significant portion of the company's work is being carried out by external contributors who are emerging as key technology partners. External contributors have become increasingly important, as a large extent of a company's operations is relied upon their contribution. This has created the need for companies to focus more on how to create greater integrity and trust in a complex system that has overlapping and interrelated operations.

3) Security and Privacy Policies Training & Awareness Monitoring

By investing in security and privacy knowledge training for employees and monitoring their awareness, organizations can reduce the probability of having security breaches and privacy violations because employees will gain higher sensitivity towards the idea of data protection. Secondly, when experiencing cyber attacks or data breaches, the organization can respond more promptly and deal with the attack more efficiently. By maintaining higher standards on privacy and security, organizations can increase their reputation and trustworthiness.

4) Bring Your Own Device (BYOD) and Increasing Demand for Employee Transparency

With the emergence of work from home (WFH) due to social distancing mandates during the pandemic, and continuing into the post-pandemic era with the rise of hybrid work, BYOD has become a prevailing trend. Since many employees work from home, BYOD allows them to use personal devices such as smartphones to access work-related applications and data. At the same time, the use of personal devices in the workplace has increased the necessity of transparency from employees due to the concern of data security and privacy. For instance, employers require staff to install security softwares or expect employees to comply with avoiding the use of insecure networks on personal devices during work time.

Case: IBM BYOD Solution For Distributed Devices Management

In the current era, companies that have remote workforces face significant challenges in managing and safeguarding their dispersed devices. However, IBM's MaaS360 can offer a solution by assisting in the management of these devices, conducting surveillance for any malevolent activity, and implementing various security measures to ensure their protection[32]. MaaS360 helps protect the workforce across multiple endpoints, as well as major operating systems like Android, Chrome OS, etc. MaaS360 is a Unified Endpoint Management (UEM) tool that simplifies the support of large remote workforces through a unified console. It incorporates threat management features to safeguard against SMS and email phishing attacks, consolidates each member's applications within encrypted containers, evaluates releases and implements patches across all platforms. Moreover, MaaS360 integrates AI technology, specifically Watson, to identify potential threats and improve productivity.

V. Normative Trends

1) Compliance is the Baseline Rather than the Leading Edge

Understanding the regulatory complexity around all technology solutions and restrictions for technology providers is considered a mere ‘baseline’ of creating a digital solution. Compliance is not the real leading edge in creating digital trust[33]. Building trust requires proactive adoption of more measures and steps. In addition to meeting legal and regulatory requirements, customers are demanding that software companies abide by ethical standards, and guarantee data security and privacy. Gaining trust necessitates going beyond simply complying with laws by enforcing strong security protocols, articulating transparent privacy policies, and being responsible for any infringements or violations.

76% of our interviewees argue that while compliance is an essential aspect of a company’s operations, it only checks the ‘bare minimum’ box when it comes to building trust with customers.

2) AI and Other Technologies Being Used to Support Sustainability Goals

Technology can help in exploring greenfield areas where there is a lack of developed standards and regulations. AI and other technologies (blockchains or ESG credits) can play an instrumental role in supporting sustainability goals. However, the jury is still out on whether stakeholders trust the ESG credit created by automated technologies or services/products that are produced by blockchain technology. Building a direct link or creating regulations between digital trust and AI for developing secure and private infrastructure is expected to emerge as a new trend.

3) Increasing Cyber Attacks pose risks

Cyberattacks and malicious threat actors are becoming more sophisticated, as they are promptly adapting to changes in the political, technological, and regulatory landscapes. This is resulting in higher frequency of such attacks that are increasingly tailored to target specific organizations.

The threat landscape is becoming more volatile, creating an imminent risk as cybersecurity experts' attention is expected to divert from strategically crucial security-building activities to addressing immediate tactical issues. Security leaders have reported that the variety of attacks has increased significantly since last year, and the impacts are more systemic than isolated in nature, targeting a range of connected critical infrastructure sectors. Organizations need to embed cyber-risk management across multiple parts of their activities, such as risk management, business continuity planning.

4) Formulation and adoption of Trust Labels

Apple’s privacy nutrition labels are a classic example of this endeavor. Over time, these labels have given Apple an authoritative voice on upholding strong privacy mechanisms and standards.

Incidentally, during the course of our research, we were introduced to the Digital Trust Label[34] by Swiss Digital Initiative[35], a cross sector association comprising academia, business, civil society and government. Defined as "combination of a bio Label and nutrition fact table for the digital world", this label is aimed at auditing digital services on the basis of multiple criteria, primarily security, data protection, reliability and fair user interaction.

The United States Government has also shown interest in the development of an "energy star"[36] label to indicate whether a software was developed securely. The objective is to improve software supply chain security. The acceptance of this trend is expected to increase with time as a label generates an elevated level of confidence in a company's ability to protect a customer's interest.

However, Apple has received criticism[37] from application developers for its stringent requirements on disclosing customer data that is being tracked by the company, particularly sharing information on data linked and not linked to the customers. Apple's commitment to the trust label is being questioned due to absence of privacy labels for its own phone and messages applications. It has been alleged that since these apps cannot be deleted from Apple phones and labels were introduced at a later stage, Apple is able to create such labels for other deletable applications only. It is interesting to note that despite these concerns, this initiative has been successful in enhancing the perception of trustworthiness of this company in the market.

Chapter 5: Framework to Incentivize Trustworthiness

I. Types of Trust Actors and Stakeholders

Trust Stakeholders

The digital trust ecosystem involves a complex matrix of stakeholders with varying responsibilities for assuring security, privacy, and compliance. These stakeholders can be broadly classified into three categories at the macro level: government, organizations (both for-profit and nonprofit) and humans. At the micro level, however, the ecosystem is more nuanced and comprises a variety of actors with disparate interests and priorities.

Government stakeholders consist of regulatory bodies and law enforcement agencies in charge of enforcing data protection laws and ensuring the security and privacy of digital trust services. Governments also play a crucial role in establishing the legal and regulatory framework that governs the use and development of digital trust technologies. For example, the EU general data protection regulation (GDPR) places responsibilities on entities that collect or target data pertaining to individuals and organizations operating within the European Union (EU)[38].

Organizations, both for-profit and nonprofit, are significant players in the ecosystem of digital trust. Data management organizations or cybersecurity corporations, for example, play a key role in protecting user data and assuring the dependability of digital technology. Non-profit organizations, such as consumer rights organizations or civil society organizations like Electronic Frontier Foundation (EFF), are key in promoting consumers' rights to privacy and data protection.

Lastly, the ecosystem of digital trust incorporates individual humans as key stakeholders. Individual users are obligated to use digital trust services and products responsibly, such as by establishing robust passwords and not disclosing sensitive information. Users also play a role in preventing security breaches by reporting suspicious activity and vulnerabilities.

While the stakeholders of the digital trust ecosystem can be broadly categorized into governments, organizations, and humans, there are many specific stakeholders within these groups that play a crucial role in establishing and maintaining trust in the digital environment.

Let’s take a look at some key stakeholders:

1. **Users:** They are people who use digital products or services while expecting security and privacy. Some examples include:

- Individual users: everyday consumers who use digital products and services for personal use like consumers or employees;
- Business users: enterprise employees who use digital products and services for work purposes

2. **Product/service/technology providers:** They are entities that offer digital products and services, including:

    - Business-to-Consumer (B2C) providers: e-commerce websites or social media platforms that store customer personal information and data such as credit card details, shipping addresses, and purchase histories like Amazon and PayPal
    - Business-to-Business (B2B) providers: cloud service or software companies that provide storage or enterprise management tools like Microsoft Azure or Salesforce
    - Business-to-Employee (B2E) providers: HR management platforms that handle payroll information or digital learning platforms that offer secure access to training materials for employees like Workday or Cornerstone OnDemand
    - Business-to-Government (B2G) providers: software companies provide cloud services to government agencies for data storage like IBM
    - Government-to-Constituent (G2C) providers: governmental portals that store citizens' personal information or offer vote collection and tallying like MyGov

3. **Government and regulatory institutions:** They are regulators are responsible for overseeing and enforcing digital trust policies and regulations, for example, Federal Trade Commission (FTC) in the US and General Data Protection Regulation (GDPR) in the EU

4. **Standards/guidelines institutions:** They are organizations that develop and promote standards and best practices for digital trust, for instance, International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST)

5. **Third-party auditors:** They are organizations that offer independent verification and validation of a company's security and privacy practices, including independent third-party assessments and certifications, like Deloitte and KPMG

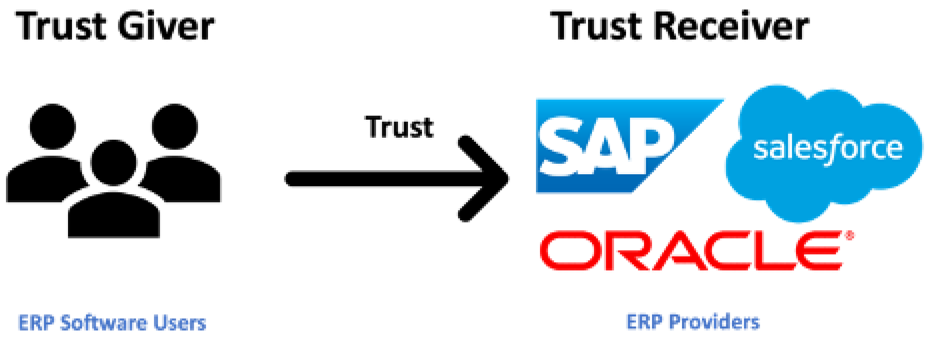
6. **Advocacy groups/individuals:** They are organizations or researchers that advocate for digital trust and privacy rights, such as International Association of Privacy Professionals (IAPP) and National Cyber Security Alliance (NCSA)

Trust Actors: Trust Givers v. Receivers

Digital trust involves creation of a dynamic relationship between trust givers and receivers. Trust givers are entities that rely on the credibility and dependability of others in order to engage in digital interactions. In this context, trust givers can be users, customers, or other entities that entrust their personal information, assets, or resources to other entities.

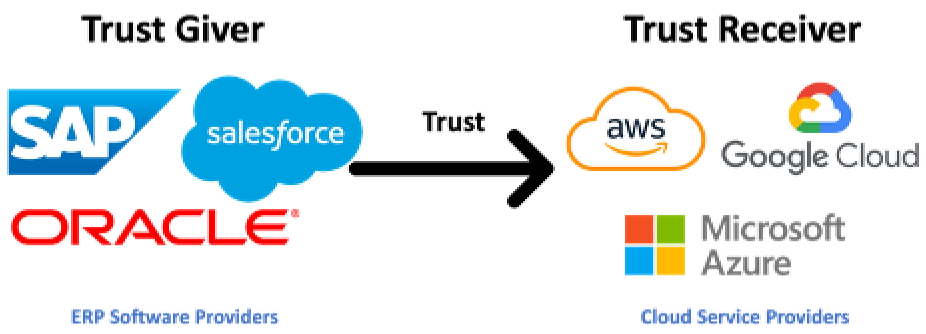
On the other hand, trust receivers are organizations that must uphold the reputation for dependability and credibility while dealing with trust givers. This category includes enterprises, service providers, and other entities that manage sensitive data or provide digital products and services. Recipients of trust are responsible for upholding the trust bestowed upon them by trust givers. In order to earn their customers' and users' trust, they must establish and maintain a reputation for privacy, security, compliance, and more.

<u>Example 1: Business Consumer Using ERP Product:</u>



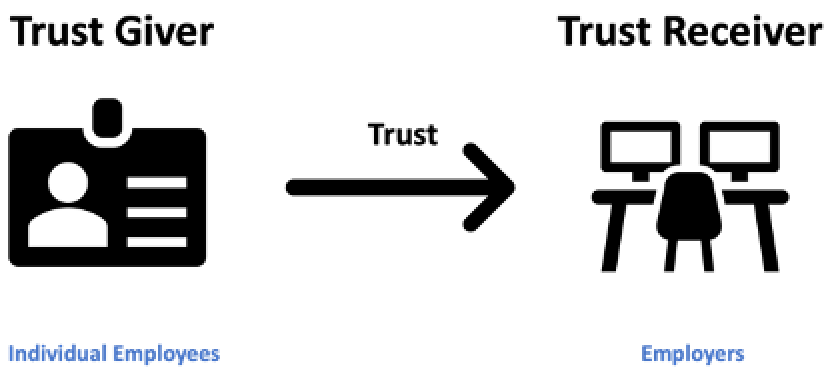
Within the digital trust ecosystem, business users of Enterprise Resource Planning (ERP) systems act as the trust givers while the companies that provide the ERP products, such as SAP, Oracle, and Salesforce, are the trust receivers. These ERP systems enable companies to effectively and seamlessly manage and integrate their main business activities, such as finance, procurement, and human resources, among others. The suppliers must build and maintain their reputation for supplying dependable, secure, and compliant software solutions if they want business users to have confidence in these ERP systems and the businesses that created them.

Example 2: Software Providers Using Third-party Cloud Service:



As they offer software solutions to companies that need dependable, secure, and compliant services, Enterprise Resource Planning (ERP) suppliers like SAP serve as trust-givers. These ERP suppliers often leverage cloud services to provide their clients with software solutions. In this instance, the organizations that offer these cloud services, like Amazon Web Services (AWS), are the trust receivers. These cloud service providers must build and maintain a reputation for providing safe, dependable, and compliant infrastructure and services if they are to uphold digital trust.

Example 3: Employees Authorizing Employers to Store Their Information:



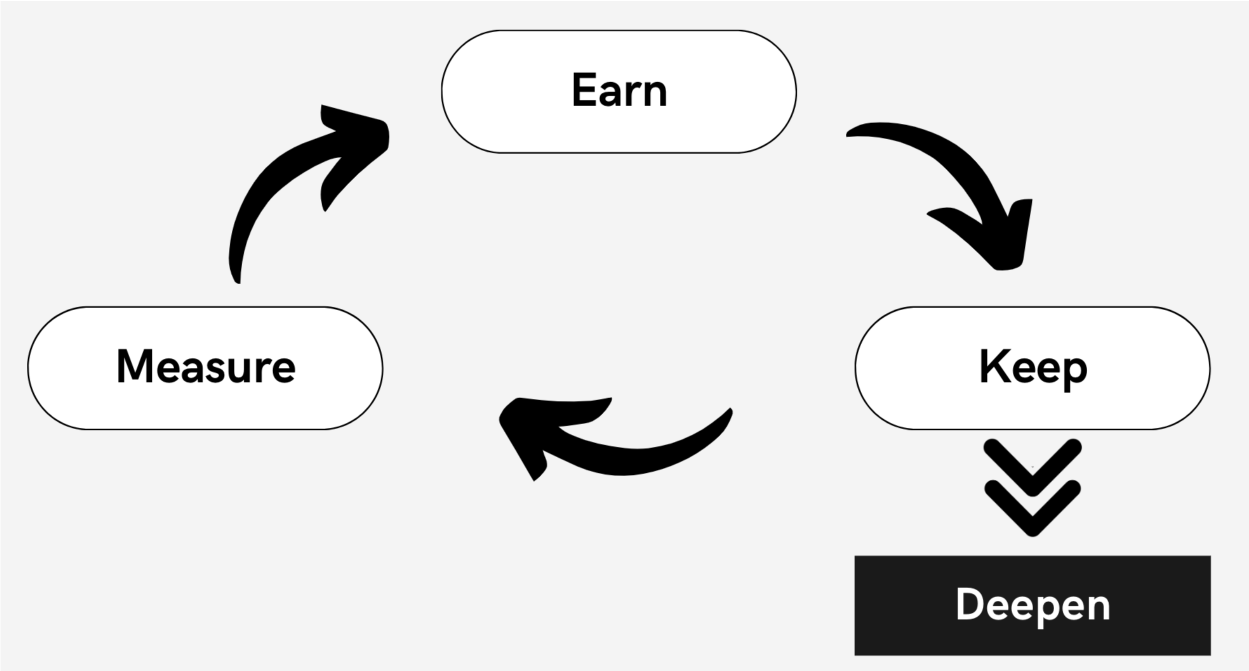
Individual employees or the workforce operate as trust givers within the digital trust ecosystem by granting their employers, who are the trust receivers, permission to retain and handle their personal and professional data. This data may include private information like social security numbers, financial information, performance evaluations, and medical records. Employers are responsible for keeping this information secure, guarding it against unauthorized access, and making sure that it is used in line with all relevant rules and laws.

Generally, trust is not a one-way street. Every institution or individual can act as both a trust giver and a trust taker depending on the scenario and context. Trust can be reciprocal, meaning that it goes both ways. As seen above, a corporation can be a trust receiver when it provides reliable services to its customers, and these customers trust the corporation to safeguard their personal information. However, the same corporation can also be a trust giver when it relies on a third-party cloud provider to store data. In this case, the corporation trusts the cloud provider to secure its data and maintain its availability.

Trust is a two-way relationship that exists within a digital trust ecosystem. To build and preserve trust and to encourage a culture of respect and trust between all parties, each stakeholder in the ecosystem must act responsibly.

II. Trust Lifecycle

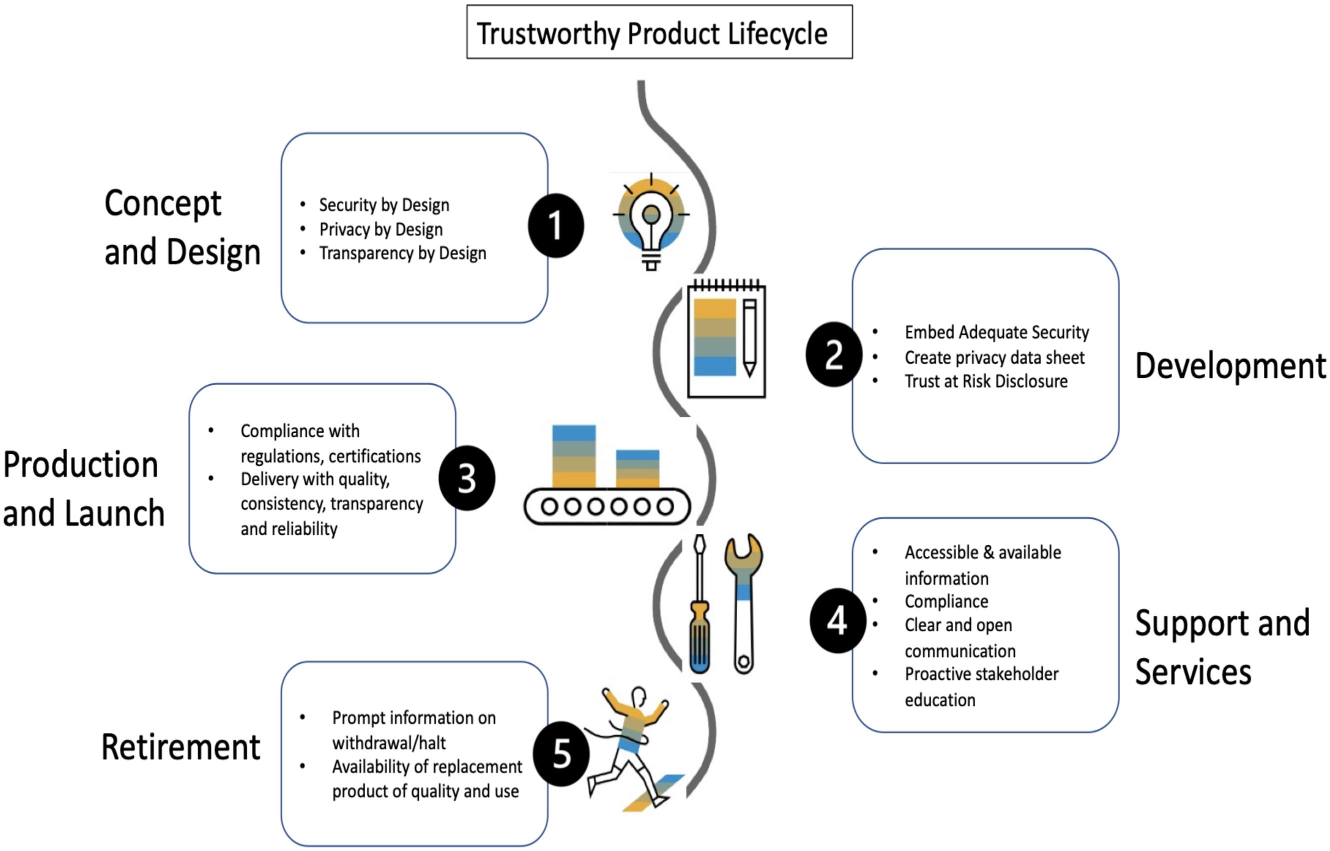
Lifecyle, as a concept, refers to a range of stages and processes that any company, its product, processes or systems goes through, beginning from its conceptualisation to retirement. Considering the fundamental role played by trust in maintaining strong and meaningful relationships with different trust stakeholders, the objective of a trust lifecycle is to establish, maintain and reinforce trust. Our analysis and research indicates that a trust lifecycle of products/services transitions through three critical phases: earning trust, keeping and deepening trust and measuring trust.



Phase I. Earn The Trust

With the increasing use of artificial intelligence-driven technologies, incidents of algorithmic manipulation and discrimination, loss of faith in societal institutions,[39] the year of 2022 seems to have marked the beginning of the cycle of distrust.[40] This has triggered the leadership of several companies to take prompt actions to integrate processes and tools that can earn the trust of different stakeholders. The decision to 'earn trust' is at the heart of digital trust.[41]

SAP has its own product lifecycle that it religiously follows. We propose the integration of following checklist in each phase of this cycle to make it a trustworthy product lifecycle:


Trustworthy Product Lifecycle
Concept and Design
1
• Security by Design
• Privacy by Design
• Transparency by Design
2
• Embed Adequate Security
• Create privacy data sheet
• Trust at Risk Disclosure
Development
Production and Launch
3
• Compliance with regulations, certifications
• Delivery with quality, consistency, transparency and reliability
4
• Accessible & available information
• Compliance
• Clear and open communication
• Proactive stakeholder education
Support and Services
Retirement
5
• Prompt information on withdrawal/halt
• Availability of replacement product of quality and use

Trust cannot be an afterthought and the most effective way of communicating this commitment is its incorporation in the product life cycle. Establishment, maintenance and enhancement of trust and trustworthiness are critical for development of a sustainable life cycle of a product. While trust is a highly contextual and cultural dependant concept, trustworthiness is the demonstrated ability and worthiness of an entity to be trusted to satisfy expectations, including satisfying expectations in the face of adversity[42].

The trust life cycle of a product, like the product life cycle, is a dynamic process that can serve as a medium for demonstrating trust and its trustworthiness. However, few steps remain key to its development:

1. Concept and Design:

When the technology is designed to nurture trust at each stage, it translates into proactive approaches known as Security by Design[43], Privacy by Design and Transparency by Design. To avoid the consequences of an adversity proactively, in the security by design approach, potential scenarios of vulnerability exploitation, attacks are predicted and risks identified to embed security controls and trust in a product. European Union's Cyber Resilience Act recommends including security in a product's lifecycle to prevent introduction of insecure products.

Similarly, data protection is integrated as a key objective of a product feature in the privacy by design approach. Data anonymisation is a classic example of this approach. Through this process, personally identified or identifiable information is modified to ensure that it is no longer identifiable.

Following a similar school of thought, Transparency by Design has emerged as a crucial dimension of product designing. SAP's customers are aware of the strength and quality of the functionality of its software but they do not have any visibility into how SAP protects the security and privacy of its customers assets and information[44]. A transparency by design approach will provide its customers the opportunity to become aware of the operation, scope and functioning of the security controls and privacy measures. It helps the product in delivering expected and intended services through the product as transparency facilitates monitoring.

As the first step in the life cycle, defining and evaluating the needs of the customer on the basis of the above approaches and incorporating those needs in the design of the product are key to establishing the foundation of a trust architecture for a product.

2. Develop:

The second stage of a trust life cycle involves the development of the nuts and bolts of the product that was designed. For SAP, there are three key considerations at this stage:

- **Embed adequate security**: Adequate Security enables delivery of required system capability despite intentional and unintentional forms of adversity, enforces constraints to ensure only desired behaviors and outcomes are realized and only authorized human to human, human to machine interactions and operations are allowed[45].

- **Privacy Data Sheet**: Integrating clarity regarding privacy considerations in a product can be accompanied by a categorisation of the kind and extent of data collection, storage by each given feature of the product. This data sheet or information needs to be documented during the development stage to ensure that each feature is developed by a deployer who is cognizant of this consideration.

- **Trust at Risk Disclosure**: The anticipated risks to trust associated with security, privacy and compliance processes, procedures and systems need to be disclosed to foster a trustworthy relationship with stakeholders.

3. Production and Launch

At the third stage of the trust lifecycle, the product has entered the production stage. In this context, including an assurance case is of paramount importance. An assurance case is the body of evidence or structured set of arguments that shows that a system satisfies specific claims[46]. Preparation of a body of evidence through the production process to demonstrate integration of principles of quality, transparency, reliability and consistency is necessary.

Another key determinant of success at this stage is the efforts taken by SAP to satisfy the trust requirements through compliance with relevant and applicable laws, regulations, standards and NIST frameworks. Before the launch of the product, demonstrating alignment with the mandatory or voluntary conditions encourages trust building and improves the perception of trustworthiness as well.

4. Services and Support

Establishing open channels of communication with the trust stakeholders is of utmost importance for this stage to successfully contribute to the trustworthiness of a product. For a stakeholder to be aware of the processes and procedures formulated by SAP to facilitate safe and efficient functioning of its products and services, SAP is required to proactively take efforts in this regard through:

- Use of an easy to access and navigate centralized source of information whose dissemination can be decentralized in a structured manner involving automation and human oversight.
- Creating a consistent and open line of communication with the concerned trust stakeholder to support a process to offer guidance, receive feedback and prompt address queries.

- Proactively partner with the customer and other relevant stakeholders to educate them on the need to adopt the innovation and existing guides, policies and processes established by SAP to help in securing and protecting their systems.

5. Retirement

If and when this stage arrives, SAP should take prompt steps to communicate the status of the product's operations including its withdrawal or suspension. Consistent and open communication is an invisible thread that binds all the elements of trust together. For the trusted relationship to continue with the customer, it is essential for the retiring product to be replaced with another product of sufficient quality.

Phase II. Keep and Deepen the Trust

Once a company has earned the trust of its stakeholders through integration of trustworthy best practices in its day to day operations associated with development of technology and provision of digital services, it enters the next phase of a trust lifecycle that focuses on keeping and deepening the trust. This phase also includes repairing of trust when it witnesses erosion due to select incidents or circumstances. While trust keeping and deepening is an ongoing process, our analysis has revealed that a focus on following factors can aid a company's efforts in this phase.

III. Factors Influencing Trust

Trust has increasingly become a critical component of business success, particularly in the digital and technological landscape of today's world. Customers, suppliers, prospects, employees, and and other key stakeholders want to know that they can rely on a company to provide secure products and services, protect their privacy, and comply with regulations. However, building and maintaining trust requires much more than mere compliance with privacy and security regulations and standards.[47]

In that regard, companies and other organizations need to prioritize the **quality, availability, transparency, and ethics and integrity** of its products and services, as factors influence their trustworthiness and can indeed build and maintain trust.[48] In the following section, we will explore these factors and how they relate to security and privacy as key components of trust.

1) Quality

Simply complying with regulations and standards may not be enough to build trust with customers and other stakeholders in today's digital age. Enterprises must go beyond regulatory compliance and focus on quality as a key factor in building trust. Customers expect high-quality products and services that meet or exceed their expectations. In that regard, several studies have shown that "*if the quality of the product, service or asset that is received does not meet consumer expectations, trust may be damaged, and the consumer may choose not to do further business with the provider*."[49]

Indeed, quality is particularly critical for building trust in the areas of security and privacy. In terms of security, quality-driven measures are necessary to prevent cyber-attacks and data breaches. A product or service that is built with poor-quality code or insufficient testing can have vulnerabilities that hackers can exploit, leading to security breaches and the loss of sensitive customer information.[50] Quality-driven security measures include regular software updates and patches to address known vulnerabilities, ongoing monitoring, and threat detection. By investing in quality security measures, SAP and other similar companies can go beyond compliance and build trust with customers by providing them with secure and reliable products and services.

Similarly, quality privacy practices are essential for building trust with customers. Enterprises that handle sensitive customer data must ensure that their products and services meet high standards for data privacy. Quality control procedures related to privacy can help ensure that data is handled with the utmost care and is only accessible to authorized personnel. This includes measures such as data encryption, access controls, and data retention policies. In addition, SAP must continually monitor and improve its privacy measures to adapt to evolving privacy regulations and changing customer needs. By prioritizing quality privacy practices, SAP can go beyond compliance and build trust with customers by providing them with peace of mind that their data is in safe hands.

A stark reminder of the importance of quality as a factor for building and sustaining trust is the Equifax data-breach case. In 2017, the consumer credit reporting agency suffered a data breach that compromised the personal information of approximately 143 million Americans. The breach was a result of poor-quality security practices, including a failure to apply necessary software updates and patches, which left the company exposed to a known vulnerability. As a consequence, Equifax lost the trust of its customers and other stakeholders, facing numerous lawsuits, regulatory investigations, and reputational damage, losing more than $1.7 billion since it was first disclosed. This incident illustrates the critical role that quality plays in establishing and preserving customer trust, particularly in the areas of security and privacy. Companies must prioritize quality-driven measures, such as ongoing testing, monitoring, and updating, to ensure that their customers' data is secure and that their reputation remains strong in the long term.[51]

Overall, quality is a key factor in building trust in a digital environment. By investing in quality control measures, a company like SAP can go beyond the baseline of compliance and build trust with customers by providing them with high-quality, reliable, and secure products and services. Quality control measures not only help build trust with customers but also improve the overall performance and efficiency of a company's operations. By prioritizing quality in their products and services, companies can reduce errors, downtime, and rework, resulting in increased productivity and cost savings. As such, quality is not just a means of building trust but also a critical factor in driving business success and growth in a digital age.

2) Availability

When it comes to building trust with customers and other key stakeholders, availability can enhance a company's trustworthiness, and while compliance with regulations may require certain data and internal information to be available for auditing purposes, going beyond those requirements can further demonstrate a company's commitment to building trust. By prioritizing uptime and ensuring that all information, systems, and services are always available to customers, a company can demonstrate its reliability, and thus its trustworthiness. In that regard, availability refers to the ability of a company's products, services, and client information to be accessible and functional when needed.[52] Any disruption in availability can lead to a loss of trust.

In terms of security, ensuring availability means protecting against malicious attacks that may compromise access to its services and information, as well as ensuring that the company's systems and data are not compromised. If a security breach occurs and the system is unavailable for an extended period, customers may lose trust in the company's ability to provide a secure and reliable service. Regarding privacy, availability means ensuring that customers' data is available to them when needed and is protected from unauthorized access or disclosure. A lack of availability of customer data can lead to privacy violations and a loss of trust in the company's ability to handle sensitive information, together with a distribution of business operations and significant financial losses.

The Amazon Web Services (AWS) outage case of 2017 highlighted the importance of availability as a factor of digital trust. The outage was caused by an employee who accidentally entered a command that caused more server capacity to be taken offline than intended. The outage lasted for several hours and caused widespread disruption, leading to significant financial losses for affected companies, including many high-profile websites and apps. Such companies relied on AWS's services to provide critical applications and services, and such disruption in availability led to a loss of their trust. Additionally, the outage raised concerns about the resilience and reliability of cloud computing services, as companies became aware of the potential risks associated with relying on a single service provider for their critical operations, costing AWS over $150 million dollars. By prioritizing availability-driven measures, such as ongoing monitoring, testing, and updates, companies can demonstrate their commitment to providing reliable and trustworthy services to their customers Any disruption in availability can lead to a loss of trust, resulting in significant financial losses, damage to reputation, and a loss of confidence among customers and other stakeholders.[53]

While compliance regulations may require certain data to be available for auditing purposes, going beyond simple compliance is a good indication of a company´s reliability. Companies can enhance their trustworthiness by prioritizing availability and taking steps to ensure that their systems and data are always accessible and protected.

3) Transparency

Beyond simply complying with regulations, companies can take transparency to the next level by being open and honest with customers and other stakeholders about the company's activities, policies, and decision-making processes. This includes being transparent about their data collection and use practices, cybersecurity measures, and compliance with regulatory requirements in a way that goes beyond what is legally required.[54] The level of transparency a company provides directly influences the trust that customers place in the company.

When it comes to privacy, transparency is vital regarding the data it collects, how it is collected, and how it is used. This information should be clearly outlined in the company's privacy policy, which should also be easy for customers to find, understand, and provide customers with the ability to control their data and give them the option to delete it if they wish.

Similarly, a company may choose to be transparent about their cybersecurity measures by sharing information about any vulnerabilities that have been detected, and the steps that are taken to address them. In this regard, transparency translates into openness regarding security practices, such as vulnerability testing and finding, patch management, together with good communication about the incidents it may suffer and its response plans to such attacks.

The 2018 Facebook Cambridge Analytica incident highlighted the significance of transparency on data collection and sharing practices to foster trust. The controversy revolved around unauthorized gathering and sharing of personal information from millions of Facebook users whose data had been harvested through a quiz app that had access to both the data of people who took the question and their Facebook friends.[55] Facebook's lack of transparency in its data collection and sharing practices significantly damaged its users' trust because they were unaware that their data was being shared without their permission, ultimately leading to a "*$134 billion loss in market value*".[56] The incident made it clear that businesses must be open and accountable for any misuse of customer data, as well as upfront about how they gather, share, and store data.

In contrast, Apple's privacy labels serve as a prime example of good transparency practices to build trust. The labels provide customers with detailed information on how their personal data is collected, used, and shared by each app, helping users make informed decisions about their privacy. Apple goes beyond regulatory requirements by providing a clear and concise breakdown of each app's privacy practices, making it easy for customers to understand how their data is being handled. Furthermore, the availability of these privacy labels also promotes transparency among app developers. The labels create a level playing field where all developers are required to provide information about their data collection and usage practices. This promotes competition and innovation while also providing customers with transparent information about app privacy practices.[57]

Besides, transparency and compliance are not two separate concepts; they are closely intertwined and work together to ensure a higher level of trust between organizations and their stakeholders. Displaying compliance certifications and international standards is a common practice for companies to showcase their commitment to digital trust. The way companies display their attestations can play a crucial role in building transparency and trust with their customers. A clear and user-friendly presentation of compliance certifications and attestations can help customers understand the security, privacy, and compliance controls that are in place and how they are being adhered to. By presenting their attestations in a transparent and accessible manner, companies can demonstrate their dedication to compliance and reassure customers that their data is being handled with care.

In conclusion, by being transparent about their security and privacy practices, beyond simply complying with what they are required by law, companies can demonstrate their commitment to protecting their customers' data and information, leading to greater trust and loyalty by its customers and other stakeholders.

4) Ethics and Integrity

Ethics and integrity play a critical role in creating a trustworthy relationship between companies, its employees, their customers, and other stakeholders. Customers expect companies not only to comply with regulation, but also to operate with honesty, fairness, responsibility, and accountability. [58]Any unethical behavior or breach of trust of either a company or its employees can quickly erode the trust that has been built, leading to financial and reputational damage.

Ethical behavior is essential to ensure the protection of customers' sensitive information. Companies that have access to vast amounts of data from their clients have the responsibility to handle this data with the utmost care by ensuring that adequate security measures are in place. Transparency and communication about security practices, including vulnerability testing, patch management, and incident response plans, can demonstrate a company's commitment to protecting customers' data.

Similarly, in terms of privacy, it's necessary to ensure that the collection, storage, and processing of data is ethical and respectful of individuals' privacy rights. Ethical behavior requires companies to be transparent about their data collection practices and to obtain explicit consent from individuals before collecting or using their personal information. Giving customers control over their data, including the option to delete it if they wish, can also demonstrate a company's commitment to privacy.

A good example of how ethics and integrity play a critical role in building and maintaining trust is the Volkswagen emissions test cheating incident of 2015, which involved the corporation selling cars that seemed to be ecologically benign while really spewing dangerous pollutants. Volkswagen accomplished this with a software in diesel engines "*that could detect when they were being tested, changing the performance accordingly to improve results*".[59] Volkswagen´s reputation was severely damaged by the scandal, leading not only to a significant financial loss, but also trust and reputational damage.

In conclusion, customers expect companies to operate with honesty and integrity, and any unethical behavior can quickly erode the trust that has been built. By ensuring ethical behavior in all areas of their operations, companies can build and maintain the trust of their customers and establish a strong reputation in the market.

Chapter 6: Knowledge Performance Indicators (KPIs) to Measure Trust

Phase III. Measure the Trust

“What is not measured cannot be improved” is especially true for trust. Owing to its dynamic nature, trust is fragile and can be easily broken by even the slightest misstep. This mandates the need of constant monitoring of established processes, tools and practices to maintain trustworthiness. At this point, a company is required to begin the third and final phase of a trust lifecycle i.e., the measurement of trust.

We have sufficiently established that trust is a context-driven and evolving phenomenon. However, to make it more tangible, we propose a set of metrics that will allow SAP to evaluate and gauge the level of trust critical stakeholders have in the organization, identify the areas of improvement, and provide guidance for targeted interventions. These metrics will allow SAP to make informed decisions, help enhance its Trust Office, and ultimately strengthen the trust between the company and its customers.

In this sense, we propose using two sets of metrics:

- **General KPIs**: Allow SAP to measure the functioning and operations of the Chief Trust Office and SAP’s trust building practices.
- **Specific KPIs**: Determine the strength and areas of opportunity of its security, privacy, and compliance practices, together with the overall reputation of the company which is a critical factor in its long-term success.

I. General KPIs

Yes/No Questions	
KPIs	**What does it indicate?**
Does SAP have a Digital Trust Center/Chief Trust Office	Digital trust center and chief trust office can play a key role in this by working to establish and enforce ethical principles and policies throughout the company. They can also help to identify and mitigate risks related to issues such as data privacy, cybersecurity, and social responsibility. Having a

	digital trust center or a chief trust office can help to build and maintain trust with stakeholders, which can in turn enhance the company's reputation and competitiveness
Does SAP have planned budget that spend specifically on the digital trust sector	Planning budget specifically for the digital trust sector can provide insight into the company's commitment to protecting users' privacy and security, which also shows the company's priorities and values
Is SAP using two-factor authentication as an option for users	Two-factor authentication requires users to provide two forms of authentication before they can access their account, which can significantly reduce the risk of unauthorized access. If the company offers two-factor authentication as an option for users, it demonstrates that the company is taking user security seriously and is committed to protecting user accounts
Does SAP have a public platform to display compliance certificates	1. Demonstrates the company takes data privacy and security seriously (especially for companies that handle sensitive personal information), as compliance certificates indicate that the company has implemented certain security and privacy controls, which helps build trust with users and stakeholders 2. Helps differentiate the company from competitors who may not be able to demonstrate the same level of compliance, and can provide a competitive advantage when bidding for contracts or partnerships 3. Ensures transparency and accountability
1. Comply to GDPR	The General Data Protection Regulation (GDPR) is a comprehensive data protection law that regulates the use of personal data of EU residents and provides individuals right to exercise control over their data
2. Comply to ISO 27001	The International Organization for Standardization 27001 Standard (ISO 27001) is an information security standard that ensures office sites, development centers, support centers and data centers are securely managed

3. Comply to SOC 1	SOC 1 (Service Organization Control 1) is a type of audit report that is intended to provide assurance about the internal controls that service organizations have in place to support financial reporting for their customers
4. Comply to SOC 2	SOC 2 (Service Organization Control 2) is a type of audit report that is intended to provide assurance about the security, availability, processing integrity, confidentiality, and privacy of the systems and data that a service organization manages on behalf of its customers
Does SAP show its pricing model to the public	Transparency in pricing builds trust with customers. Having a pricing model can also help to demonstrate the company's commitment to fairness and openness in its business practices, which can enhance its reputation and build customer loyalty over time
Are SAP's administrative, technical, and physical safeguards are appropriate for the size, complexity, nature, and scope of their activities and the sensitivity of their customers' information	This measures SAP's performance in safeguarding customer information
Does SAP perform regular risk assessments of their operations, safeguards, technology base, and procedures	
Does SAP has requirements for safeguarding customer information and ensuring that they are passed on to service providers through contractual means	

General Measurement Questions	
KPIs	What does it indicate?
% of organizations annual revenue spent on all trust KPIs	SAP's willingness to invest in incorporating digital trust in its systems/processes
Size of Chief Trust Office team (number of full time equivalent per 1000 employees)	SAP's commitment to invest in a robust team to work on the issue of digital trust
% annual growth in budget for the Chief Trust Office	SAP's commitment to providing the best possible resources to facilitate development and expansion of the digital trust team
% growth planned for the Chief Trust Office for the next three years	SAP's willingness and commitment to invest in this issue in the long-term
Availability of an easy to access/navigate trust center website/portal	SAP's commitment and willingness to provide all relevant information to the customers, irrespective of their level of sophistication of knowledge of security processes/systems
% increase or decrease in number of SAP Compliance Certifications/Standards Offerings	This indicates SAP's attitude towards compliance certifications/standards
% increase or decrease in number of complaints by customers related to compliance	This indicates areas where the company needs to improve its practices and policies
% increase or decrease in number of lawsuits filed with Courts by: 1. Regulators 2. Customers 3. Shareholders	This measure SAP's performance in compliance

II. Specific KPIs

A. Security

KPI	What does it indicate?
% increase or decrease of successful resolution of customer reported issues with security controls/processes of SAP?	This measures SAP's performance in resolving customer's concerns
% increase in hiring employees with: a) Relevant security certifications like CompTIA Security+ certification b) Training and expertise in cloud security	This measures SAP's commitment to invest in people who are skilled at building and maintaining security in SAP products/solutions, particularly cloud security as that witnesses more frequent breaches, attacks requiring higher investment
% increase or decrease in reach of a vulnerability disclosure statement? (average time taken, number of media platforms reached out to, easy to understand nature of the communication)	This measures public perception and shows SAP's performance in readiness to take steps that show compliance to the CERT Guide on Coordinated Vulnerability Disclosure that is followed by SAP (The Guide includes 'Public Awareness' as a step that involves issuing a statement on the vulnerability and its remediation plan)
Number of SAP assets (e.g. security standards/compliance documents/management guides) available in different languages of existing customers hailing from different regions	This shows SAP's efforts to provide ease of understanding to its customers from different jurisdictions
Number of languages SAP Trust Center's live chat box communicates in	This measures SAP's commitment to supporting access to, availability and comprehension of information on its business, offerings, functioning to customers according to their regions
% of security vulnerabilities reported by SAP team in comparison to those reported by customers and independent researchers	Measures performance of SAP's team (people and technology) in proactively detecting and assessing threats and vulnerabilities in comparison to other sources

Number of surveys (% increase or decrease) conducted to assess customer’s clarity in understanding of its documents on: 1. Business Continuity Management Standard 2. Cloud Services Reference Guide 3. SAP Standard, Processes,Guidelines for protecting data and information 4. Threat Management Guide 5. Vulnerability Management Guide 6. Compliance Finder (assess customer’s ease with navigating and using it)	This measures success or failure rate of SAP's trainings and SAP's efforts in ensuring that the customer understands and adopts its frameworks/guides/plans to build a more secure system on a regular basis
% of attacks/breaches/incidents of data loss due to internal frauds within SAP customer’s ecosystem in comparison to the % of attacks/breaches/incidents of data loss due to external attacks	This measures the efforts taken by SAP to educate the third parties in adopting updated and robust security practices ready to tackle existing and emerging risks/threats from not just external but internal threats
% of customers who review code developed by third parties before importing it to their SAP systems	This measures SAP’s involvement and capability to closely monitor the security posture of its customers and keep them informed about standard security practices
% of customers who have vulnerability management programs in place?	This measures success or failure rate of SAP's trainings and the efforts it takes to educate customers
% increase or decrease in detection of security vulnerabilities in products?	This measures improvement in the team's detection capabilities or indicates the ease of vulnerability violation through an attack/breach.
% increase or decrease in number of existing and new customers engaging SAP's services to transition to cloud services for their data protection	This measures the customer's trust in SAP's ability and position in the market to protect their data in cloud and their willingness to cede control over their data to SAP
% increase of decrease in number of in-person/virtual demonstrations of how SAP's security controls meet the security requirements of the customer	This measures SAP's willingness to guide the customer through each step and its commitment to facilitating transparency

Number of security questionnaires shared with a customer on a yearly basis	This measures SAP's commitment to establishing an open channel of communication with the customer to assess its concerns, issues and collect feedback
% increase or decrease in the response time of the customer to the security questionnaires	This shows SAP's commitment to establishing an open channel of communication with the customer
Number of people (% increase or decrease) involved in training the customers on security controls and helping them fill security questionnaires	This measures SAP's commitment in helping its customer in adopting security best practices
Regarding the automation tool of SAP that analyzes the response of security questionnaires, % increase or decrease in errors in its analysis of questions and % increase or decrease in human oversight required in operation of this tool	This measures effectiveness of SAP's automation efforts
Number of third parties engaged for specified tasks, for eg., to assess security questionnaires and conduct compliance and an assessment of the impact of this outsourcing on the customers through measurement of increase or decrease in customer retention	This measures the effectiveness of SAP's outsourcing processes, performance assessment of engaged third parties and customer's satisfaction with this three-way relationship
Number of security audits conducted in an year and % increase or decrease in sharing of relevant information by SAP about the audits with concerned stakeholders	This measures SAP's commitment to upholding transparency by sharing the direct impact of the audits on its existing security or privacy practices with different trust stakeholders to keep them informed
Number of people specifically appointed or with specific expertise (in the CTO) to handle crisis management between SAP and its security vendors	This measures SAP's commitment to supporting an open and effective channel of communication with different stakeholders

B. Privacy

Metrics	What does it indicate?
% (increase or decrease) in customer churn rate after a privacy breach or incident.	This shows the impact of privacy incidents on customer loyalty and trust
% of vendors/suppliers who sign a privacy and data protection agreement.	This shows SAP's commitment to privacy and data protection in its partnerships with vendors and suppliers.
% (increase/decrease) in successful resolution of customer reported privacy issues with SAP's products/solutions.	This shows SAP's performance in protecting customer privacy and addressing issues promptly.
% increase or decrease in data/privacy breaches.	This shows SAP's overall security posture and ability to protect sensitive information.
% of SAP products that undergo privacy impact assessments before launch, and % of products that undergo privacy audits by third-party assessors.	This shows SAP's compliance with privacy regulations and guidelines in its product development process.
% increase or decrease in the number of privacy-related complaints or investigations filed against SAP by regulatory bodies or authorities.	This shows SAP's compliance with privacy laws and regulations and its reputation in the industry.
% increase or decrease in the number of privacy-related lawsuits or legal actions taken against SAP by customers or third parties.	This shows SAP's liability and risk exposure related to privacy issues.
% increase or decrease in $ number of penalty for breach of privacy regulations	This measures the negative impact of SAP's privacy compliance cases
% increase or decrease in the time taken to detect and respond to privacy incidents involving SAP products/solutions.	This shows SAP's incident response capabilities and ability to mitigate risks.
% increase or decrease in the number of vulnerabilities identified and fixed in SAP products/solutions related to privacy.	This shows SAP's commitment to proactive security and privacy measures.
% increase or decrease in the number of privacy and data protection impact	This shows SAP's commitment to privacy by design and privacy risk management.

assessments conducted by SAP for new products/solutions or changes to existing ones.	
% increase or decrease in the number of privacy training programs and resources provided by SAP to employees and customers.	This shows SAP's commitment to privacy education and awareness.
% of employees who complete mandatory privacy training and certification.	This shows the level of compliance among SAP employees with privacy policies and regulations.
% increase or decrease in the number of privacy-related audits or assessments conducted by third-party organizations.	This shows SAP's transparency and accountability to privacy standards and requirements.
% increase or decrease in the number of privacy-related enhancements or features added to SAP products/solutions based on customer feedback and requests.	This shows SAP's responsiveness to customer privacy needs and concerns.
% increase or decrease in the overall customer satisfaction rating for SAP products/solutions in terms of privacy and data protection. (Surveys)	This shows SAP's reputation and competitiveness in the market with respect to privacy concerns.
% increase or decrease of disclosures of personal information without notifying a customer	This shows SAP's commitment to transparency with its customers regarding privacy and data protection, as well as its dedication to keeping customers informed and empowered
% increase or decrease of disclosures of nonpublic personal information without giving the customer the opportunity to opt out beforehand	This shows SAP´s commitment to transparency and availability by providing customers with control over their sensitive data.

C. Reputation

Metric	What does it indicate?
Brand Awareness	How familiar people are with the SAP brand, and how likely they are to recognize and recall it. Brand awareness can be measured through surveys, social media mentions, and other forms of audience feedback.
Net Promoter Score (NPS)	Net Promoter Score (NPS) is a customer loyalty and satisfaction measurement taken from asking customers how likely they are to recommend your product or service to others on a scale of 0-10[60].
Social Media Sentiment	This metric measures the overall sentiment surrounding SAP on social media platforms such as Twitter, Facebook, and LinkedIn. By analyzing the tone of mentions and comments, sentiment analysis can reveal whether the company is viewed positively or negatively by the public.
Media Coverage	This measures the frequency and tone of news articles and media mentions of SAP. By monitoring media coverage, the company can gain insights into the topics that are most important to the public, and whether the coverage is positive or negative. Some of the social media monitoring softwares are that provide sentiment analysis to help companies understand their brand perception on social media are: Brandwatch; Hootsuite Insights; Sprout Social; Talkwalker; and Meltwater.
Employee Satisfaction	A company's reputation is often closely tied to the satisfaction of its employees. By surveying employees and monitoring turnover rates, SAP can gain insights into the company's culture and reputation as an employer, which can in turn impact public perception.
Goodwill/Reputation	The RepTrak Platform is the world's leading cloud-based corporate reputation intelligence platform providing trusted data and insights about your company's corporate reputation and other intangible assets by measuring how stakeholders feel, think, and act towards your company. The RepTrak Platform provides you and your team with ongoing performance data on how stakeholders evaluate your company when it comes to your corporate reputation, brand, and ESG using online surveys and the media[61].

Chapter 7: Recommendations

Recommendation 1: Improve Customer Interface

Make an easily navigable website: To have the right intention cemented in trustworthiness is not enough, it needs to be shown. The first stage of communication of a new customer with SAP begins with the Trust Center Website. At present, navigating the portal for information on SAP's existing efforts to facilitate transparency in communication is a complex and time consuming process. Few specific recommendations are:

- Disaggregate all compliance related documents or information under two categories i.e. Security and Compliance. Refer to *Appendix I* for a sample compliance tracker that SAP can consider for preparation of a compliance tracker which clearly communicates its progress in terms of complying with various standards, certificates, attestations, in an easy to understand manner on its trust portal.
- Segregate Internally and externally published documents, for e.g. on online news portals, to give customer clarity on SAP's positioning on an issue.
- Eliminate privacy dark patterns from the portal

Recommendation 2: Prepare a Privacy Data Sheet for Public Consumption

Customers should have clarity on what SAP is planning to do with their data. To eliminate any possibility of surprise for the customers through unplanned and unauthorized use of customer's data, frame a privacy data sheet. The existing privacy statement is not easy for an average consumer to understand, lacks simplicity and, more importantly, does not offer a product-wise disclosure of data collection, storage and consent-taking practices .

- Prepare this sheet in an easy to understand manner, while specifying for each SAP product available for customers, where and which kind of data SAP collects, doesn't collect, stores and doesn't store.
- Share this data sheet on the trust center portal to ensure ease of access and availability.

Recommendation 3: Develop a communications strategy that prioritizes trust

Our analysis indicates that SAP's vulnerability disclosure statements are not easily available in public forums, restricting the ability of existing or prospective customers to be aware of the steps taken by SAP to proactively address security vulnerabilities. Availability of clear and crisp information on incidents where SAP successfully resolved customer's concerns in a crisis and retained its trust can also enhance the trustworthiness of its services.

Recommendation 4: Expand the definition of Trust

At present, SAP relies on security, privacy, compliance and transparency as the components of trust-building that increase the confidence of different stakeholders in its ability to cater to their needs and requirements. Our analysis indicates that SAP can increase its trustworthiness if it accounts for other components as well (e.g. fairness, accountability, reliability, ethics, competence).

With the growth of emerging technology and its increasing adoption in the market, the meaning of trust and trustworthiness is changing. To keep up with the evolving requirements of the customers, adoption of an all-inclusive approach towards trust-building is crucial.

Recommendation 5: Adopt a broader set of KPIs

SAP's existing focus for measuring trust and its related considerations is limited to the stakeholder's engagement with its events, training, website. This is insufficient to comprehensively assess the success or failure of the efforts being made towards strengthening security, privacy and related compliance mechanisms.

Reputation management and assessment is key to understanding the public perception of a company. If the objective is to measure the trustworthiness of a company's brand in the market or amongst its stakeholders, it is even more important to invest in establishing KPIs that measure a company's reputation.

Recommendation 6: Create a Trust Label or Join as a Collaborator in Formulation of a Trust Label

Use of labels by companies in the market to establish and indicate their commitment to transparent and safe data practices is not a new phenomenon. From Apple Inc to a cross-sector collaborative effort like the Swiss Digital Initiative to the United States Government, there is a public acknowledgement of the power of a trust label in enhancing the trustworthiness of a digital product.

A SAP Label that unequivocally establishes its authority on processes, policies and controls that speak to its intentions and proactive actions to building and maintaining the trust of its stakeholders can go a long away in making trust a viable market category. Alternatively, the presence of existing labels such as, the Digital Trust Label, also establishes the vital role played by collaboration between industry, government and non-profit organizations. SAP's contribution to such an effort can indicate its commitment to multi-stakeholder approach towards building and maintaining trust. If it joins such initiatives as a partner, it can create awareness around the issue and offer a domain-specific expertise to develop a more robust and global trust label.

Recommendation 7: Prioritize compliance as a factor influencing trust

Compliance is the lowest possible bar of trustworthiness that can be achieved by any company. At present, SAP is relying on it as a prominent component of building and maintaining trust. However, considering the advancement in technologies, increasing awareness of customers, expansion of the threat landscape including data breaches and security attacks, it is crucial for SAP to acknowledge that compliance is not a separate component of trust but a factor that needs to be incorporated when establishing various processes and policies to strengthen security and privacy. This shift in mindset will change its goalposts and redirect investment priorities, positioning SAP to emerge as a trust leader in the market.

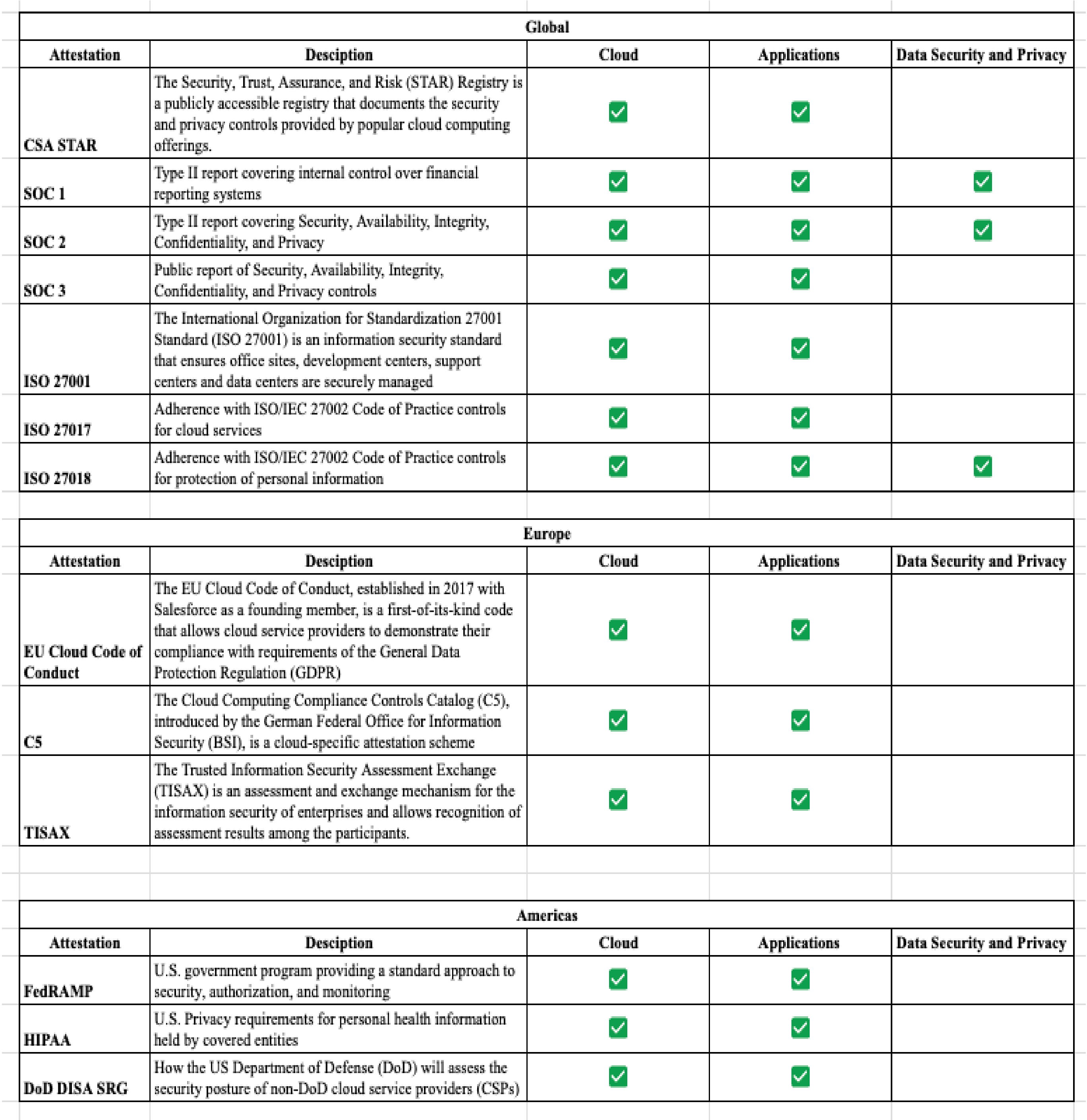
Recommendation 8: Adopt mechanisms to show to the customers how their data is being protected

Trust is a continuous process. Earning it is important but it is equally crucial to keep that trust and deepen it at every stage of the relationship with a stakeholder.

Our research shows that the industry is currently battling survey fatigue at a large scale. There is a heavy reliance on surveys to assess the sentiment of customers towards the services being provided by a company or evaluate the stakeholder's understanding of the policies and protocols of a company. While this effort is successful in earning the trust of the stakeholder, it is not able to assist in keeping it.

Adopting a mechanism through which the results of the surveys are proactively shared with the stakeholders to communicate the impact of their inputs or feedback and its direct relation with the improvement in existing operations of SAP, its trustworthiness as a supplier of digital products and services is an efficient and effective way of tackling this issue.

Appendix 1: Sample Compliance Tracker



Global				
Attestation	Desciption	Cloud	Applications	Data Security and Privacy
CSA STAR	The Security, Trust, Assurance, and Risk (STAR) Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings.	✅	✅	
SOC 1	Type II report covering internal control over financial reporting systems	✅	✅	✅
SOC 2	Type II report covering Security, Availability, Integrity, Confidentiality, and Privacy	✅	✅	✅
SOC 3	Public report of Security, Availability, Integrity, Confidentiality, and Privacy controls	✅	✅	
ISO 27001	The International Organization for Standardization 27001 Standard (ISO 27001) is an information security standard that ensures office sites, development centers, support centers and data centers are securely managed	✅	✅	
ISO 27017	Adherence with ISO/IEC 27002 Code of Practice controls for cloud services	✅	✅	
ISO 27018	Adherence with ISO/IEC 27002 Code of Practice controls for protection of personal information	✅	✅	✅

Europe				
Attestation	Desciption	Cloud	Applications	Data Security and Privacy
EU Cloud Code of Conduct	The EU Cloud Code of Conduct, established in 2017 with Salesforce as a founding member, is a first-of-its-kind code that allows cloud service providers to demonstrate their compliance with requirements of the General Data Protection Regulation (GDPR)	✅	✅	
C5	The Cloud Computing Compliance Controls Catalog (C5), introduced by the German Federal Office for Information Security (BSI), is a cloud-specific attestation scheme	✅	✅	
TISAX	The Trusted Information Security Assessment Exchange (TISAX) is an assessment and exchange mechanism for the information security of enterprises and allows recognition of assessment results among the participants.	✅	✅	

Americas				
Attestation	Desciption	Cloud	Applications	Data Security and Privacy
FedRAMP	U.S. government program providing a standard approach to security, authorization, and monitoring	✅	✅	
HIPAA	U.S. Privacy requirements for personal health information held by covered entities	✅	✅	
DoD DISA SRG	How the US Department of Defense (DoD) will assess the security posture of non-DoD cloud service providers (CSPs)	✅	✅	

Reference

1. “trust”, Cambridge Dictionary, May 2023, https://dictionary.cambridge.org/dictionary/english/trust

2. “Earning Digital Trust: Decision-Making for Trustworthy Technologies.” World Economic Forum, 15 Nov. 2022, https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies/

3. Sucher, Sandra J., Gupta, Shalene. “The Power of Trust.”

4. ISACA. (2022) Digital Trust Ecosystem Framework: Introduction and Approach. ISACA, n.d.

5. Idem.

6. “Social media fact sheet.” Pew Research Center: Internet, Science &amp; Tech. 7 Apr. 2015, https://www.pewresearch.org/internet/fact-sheet/social-media/

7. “Triple digit increase in cyberattacks: What next?” Accenture, 4 Aug. 2021, https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks

8. “About Digital Trust.” World Economic Forum, May 2023, https://initiatives.weforum.org/digital-trust/about

9. “Understanding the Full Digital Trust Ecosystem.” ISACA, 13 May 2022, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/understanding-the-full-digital-trust-ecosystem

10. “Product Overview.” Microsoft Trust Center, May 2023, https://www.microsoft.com/en-us/trust-center/product-overview

11. Boehm, Jim., Grennan, Liz., Singla, Alex., Smaje, Kate. “Why Digital Trust Truly Matters.” Mckinsey & Company, 12 Sep. 2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

12. Golden, Deborah., Goldhammer, Jesse., Parekh, Jay., Kearns-Manolatos, Diana., Aubley, Curt., Morris, Michael. “Earning Digital Trust: Where to Invest Today and Tomorrow.” Deloitte, 16 Feb. 2022, https://www2.deloitte.com/us/en/insights/topics/digital-transformation/digital-trust-solutions.html

13. “What is Digital Trust, and How Does It Enable Modern Digital Business?” Okta, 2 Feb. 2022, https://www.okta.com/uk/blog/2022/02/what-is-digital-trust-and-how-does-it-enable-modern-digital-business/#:~:text=Digital%20trust%20refers%20to%20the,information%20assets%20and%20technology%20resources

14. Romney, Bruce., Lovisa, Sandro., Zimmerman, Ben., Malhotra, Pavi. “ The DNA of Digital Trust: Data Protection and Privacy for the Intelligent Enterprise.” SAP, and Ernst & Young, 2020, https://www.sap.com/docs/download/2020/01/b8a4e28c-7e7d-0010-87a3-c30de2ffd8ff.pdf

15. Kvochko, Elena. “Fostering Trust in a Digital World - Establishing a Trust Organization.” 10 Feb. 2023, https://www.linkedin.com/pulse/fostering-trust-digital-world-establishing-elena-kvochko%3FtrackingId=R%252Bm6RtZAR168631tAdPE3w%253D%253D/?trackingId=R%2Bm6RtZAR168631tAdPE3w%3D%3D

16. Interview with Kathryn K. White, Accenture Fellow at World Economic Forum

17. Interview with Christopher Chew, IAPP Privacy Engineering Advisory Board
18. Interview with Theresa Peterson, Edelman Trust Institute
19. "NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations." National Institute of Standards and Technology, Sep. 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf
20. "STANDARD No.: TEC 57050:2022 (Draft) Fairness Assessment and Rating of Artificial Intelligence Systems." Telecommunications Engineering Center, Department of Telecommunications, Ministry of communications, Dec. 2022, https://www.tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
21. ForHumanity, a non-profit public charity, with 1100+ members from 72 different countries that provides services, on behalf of humans, to governments and regulators, such as NIST, https://forhumanity.center/
22. "Earning Digital Trust: Decision-Making for Trustworthy Technologies." World Economic Forum, 15 Nov. 2022, https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies/
23. "CCPA and CPRA", International Association of Privacy Professionals, https://iapp.org/resources/topics/ccpa-and-cpra/
24. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), https://gdpr-info.eu/
25. "Cybersecurity Framework", National Institute of Standards and Technology, https://www.nist.gov/cyberframework
26. "Cybersecurity Certification Framework", European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework
27. "Discussion Draft of the NIST Cybersecurity Framework 2.0 Core", National Institute of Standards and Technology, April 23, 2024. https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf
28. "Global Cybersecurity Outlook 2023." World Economic Forum, 18 Jan. 2023, https://www.weforum.org/reports/global-cybersecurity-outlook-2023
29. Interview with Mark Ciminello, Vice President and Chief Architect, Chief Trust Office, SAP Global Security, SAP
30. Atlman, Elizabeth J., Schwartz, Jeff., Kiron, David., Jones, Robin., Kearns-Manolatos, Diana. "Workforce Ecosystems: A New Strategic Approach to the Future of Work." 13 Apr. 2021, https://sloanreview.mit.edu/projects/workforce-ecosystems-a-new-strategic-approach-to-the-future-of-work/
31. Interview with Diana Kearns-Manolatos
32. "Bring Your Own Device (BYOD) Solutions." IBM, May 2023, https://www.ibm.com/products/maas360/byod
33. Interview with Diana Kearns-Manolatos

34. “Digital Trust Label.” Swill Digital Initiative, May 2023, https://www.swiss-digital-initiative.org/digital-trust-label/

35. Headquartered in Geneva, Switzerland

36. “FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks.” The White House, 12 May 2021,

37. Chen, Brian. “What we learned from Apple’s new Privacy Labels”, The New York Times, Jan. 27, 2021. https://www.nytimes.com/2021/01/27/technology/personaltech/apple-privacy-labels.html

38. “What is GDPR, the EU’s new data protection law?” GDPR.EU, May 2023, https://gdpr.eu/what-is-gdpr/

39. “2023 Edelman Trust Barometer.” Edelman, May 2023, https://www.edelman.com/trust/2023/trust-barometer

40. Ibid.

41. “Earning Digital Trust: Decision-Making for Trustworthy Technologies.” World Economic Forum, 15 Nov. 2022, https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies/

42. NIST Standard SP 800-160

43. “Cybersecurity Agencies Publish New Guidance on Safe Software Design: Here's Why It Matters.” World Economic Forum, 19 Apr. 2023, https://www.weforum.org/agenda/2023/04/cybersecurity-secure-by-design-software-guidance/

44. Interview with Mark Ciminello

45. NIST Standard SP 800-160

46. Ibid.

47. Interview with Mark Ciminello, Pascal Marmier, Michelle Barret, Shannon Donahue, and Jill Crasman.

48. Samuelson, David. “Digital Trust: The Key to Successful Transformation.” ISACA, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/digital-trust-the-key-to-successful-transformation.

49. Digital Trust: A Modern Day Imperative.” ISACA, 2022, https://www.isaca.org/resources/white-papers/digital-trust-a-modern-day-imperative.

50. Hamilton, Hannah. “Digital Trust. Why It's Important for Your Business.” *Digital Trust. Why It's Important for Your Business*, Jamf, 29 Nov. 2022, https://www.jamf.com/blog/digital-trust-5-reasons-it-matters-for-your-business/#:~:text=A%20good%20cybersecurity%20and%20data,to%20mitigate%20data%20retention%20risks

51. Fruhlinger, Josh. “Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?” CSO Online, CSO, 12 Feb. 2020, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

52. Digital Trust: A Modern Day Imperative.” ISACA, 2022, https://www.isaca.org/resources/white-papers/digital-trust-a-modern-day-imperative.

53. Hersher, Rebecca. “Amazon and the $150 Million Typo.” *NPR*, NPR, 3 Mar. 2017, https://www.npr.org/sections/thetwo-way/2017/03/03/518322734/amazon-and-the-150-million-typo.

54. Digital Trust: A Modern Day Imperative." ISACA, 2022, https://www.isaca.org/resources/white-papers/digital-trust-a-modern-day-imperative.
55. Langone, Alix. "What to Know about Facebook's Cambridge Analytica Problem." Time, Time, 29 Apr. 2021, https://time.com/5205314/facebook-cambridge-analytica-breach/.
56. Mirhaydari, Anthony. "Facebook Stock Recovers All $134B Lost after Cambridge Analytica Data Scandal." *CBS News*, CBS Interactive, 11 May 2018, https://www.cbsnews.com/news/facebook-stock-price-recovers-all-134-billion-lost-in-after-cambridge-analytica-datascandal/.
57. Chen, Brian X. "What We Learned from Apple's New Privacy Labels." *The New York Times*, The New York Times, 27 Jan. 2021, https://www.nytimes.com/2021/01/27/technology/personaltech/apple-privacy-labels.html.
58. Digital Trust: A Modern Day Imperative." ISACA, 2022, https://www.isaca.org/resources/white-papers/digital-trust-a-modern-day-imperative.
59. Hotten, Russell. "Volkswagen: The Scandal Explained." BBC News, BBC, 10 Dec. 2015, https://www.bbc.com/news/business-34324772.
60. "Net Promoter System." Bain & Company, May 2023, https://www.netpromotersystem.com/
61. "2023 Global RepTrak 100." RepTrap, 2023, https://www.reptrak.com/rankings/?page=9#ranking-list