RUBICON

ADVISORY GROUP

SPENCER: A Framework for Maintaining Digital Trust- v1.0

RUBICON ADVISORY GROUP

Table of Contents

Table of Figures

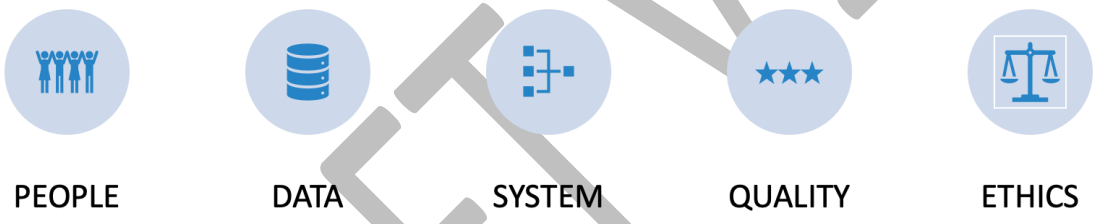
Building Digital Trust: The Cornerstone of Modern Enterprise Success

The Digital Landscape Unveiled

In today's fast-paced, interconnected world, where every click, tap, and swipe generates vast amounts of data, the concept of digital trust has become a cornerstone of modern enterprise success. In this narrative we will explore the pressing need for digital trust, the invaluable benefits it brings, and the compelling drivers that propel organizations toward its cultivation.

Digital Trust Ecosystem

Comprised of five foundational dimensions, three of which consist of what we would constitute "Digital" – that is the Digital Identities (***who*** *our relationship is with*), Data (***what*** *we're entrusted with*) and Systems (***where*** *data we've been entrusted with is stored, processed and transits)* – in which transactions performed. The remaining two are a bit more nuanced and introduce a spectrum of subtle differences and degrees – all stemming from observations, reputation and experiences – held by various, disparate stakeholders.



The Need for Digital Trust

Imagine a world without Digital Trust—a world where your personal information, financial data, and confidential business details are constantly at risk. Cyberattacks loom on the horizon and privacy violations lurk around every digital corner. In such a landscape, the very foundation of trust, which underpins our digital interactions, begins to crumble.

Digital trust is the assurance that the digital world can be a safe, secure, and reliable space for individuals and organizations alike. It encompasses the belief that data will be handled with integrity, that privacy will be respected, and that security measures will safeguard against cyber threats.

The Benefits of Digital Trust

Building digital trust is not merely an obligation; it's a strategic imperative that yields significant rewards. Consider the following benefits:

Enhanced Reputation: Trustworthy organizations earn the respect and loyalty of customers, partners and stakeholders. Positive reputations are priceless assets in today's competitive marketplace.

Reduced Risk: Trust-driven security and privacy practices mitigate the risk of data breaches, legal liabilities and financial losses.

Customer Loyalty: When customers trust your commitment to safeguarding their data, they are more likely to remain loyal and engage with your brand over the long term.

Compliance Assurance: Trust-focused organizations inherently align with data protection regulations, avoiding costly penalties and legal entanglements.

Competitive Advantage: Trust becomes your unique selling proposition, setting you apart in an increasingly crowded digital ecosystem.

The Values of Digital Trust

Digital Trust is not just a meaningless phrase; rather it should embody core values that guide ethical and responsible behavior in the digital age. At a high-level, when we look at the concepts of Digital Trust, we see the following:

Reliability: Trustworthy organizations consistently deliver on promises, ensuring data and services are available when needed.

Honesty: Transparency and truthfulness build trust by fostering open and honest communication with stakeholders.

Integrity: Trust hinges on upholding high ethical standards, respecting privacy, and safeguarding data.

Consistency: The reliability of security measures and data practices builds trust by demonstrating a commitment to consistency over time.

Vulnerability: Acknowledging and addressing vulnerabilities showcases an organization's dedication to improvement and resilience.

The Drivers Toward Digital Trust

Several drivers propel enterprises toward the cultivation of digital trust, the following is a summary overview of those drivers:

Customer Expectations: Today's customers demand trustworthiness. Organizations that fail to meet these expectations risk losing their clientele.

Regulatory Landscape: Evolving data protection regulations require organizations to prioritize trust or face severe consequences.

Cyber Threats: The ever-evolving threat landscape necessitates robust security measures to protect sensitive data.

Globalization: In a connected world, digital trust is essential for international partnerships and expansion.

Innovation: As organizations innovate and leverage emerging technologies, trust becomes integral to their success.

It is the author's opinion and professional belief that Digital Trust is no longer an option, a "*nice to have*"; Trust has been the lifeblood of most businesses – regardless of industry, market or sector. By understanding its need, embracing its benefits and values, and harnessing the drivers that lead to its cultivation, organizations can thrive in today's highly connected, data-driven world, earning the trust and loyalty of their stakeholders while safeguarding their digital futures.

Stakeholder Digital Trust Expectations

In order to ensure proper alignment with stakeholders, each organization needs to identify the relevant stakeholders, both internal and external. These stakeholders are going to have different expectations on your organization's Digital Trust posture. Your responsibility is to work with Senior Management and work to align with the expectation of the constituents you serve, understanding that you cannot please everyone.

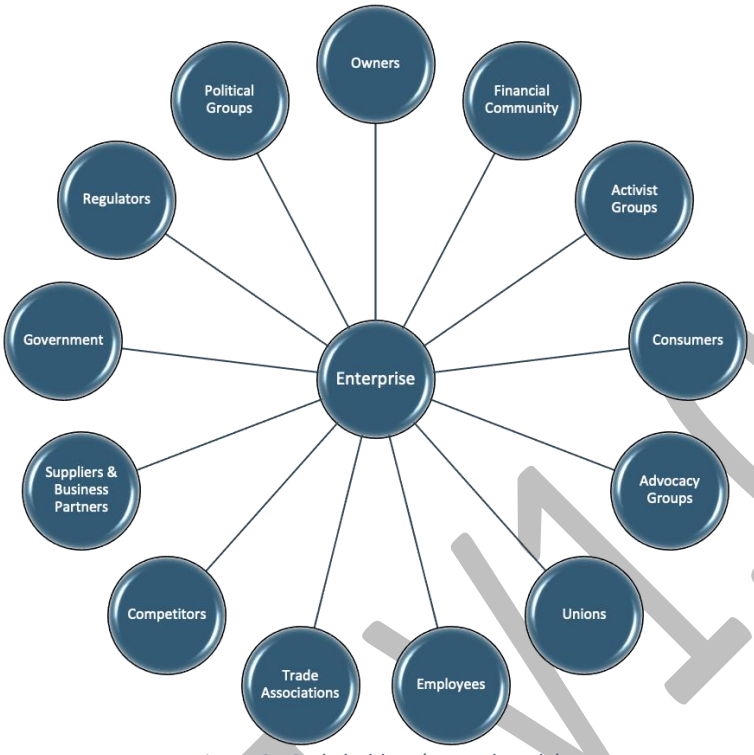


Figure 2 - Stakeholders (example only)

Identify Stakeholder Expectations

Determining the expectations of key stakeholders can at first can appear to be a herculean task; considering that we have stakeholders inclusive of those internal to our organization, such as Boards, Senior Management, and employees in addition to those who are external to our organizations and can include customers, partners and regulators.

Each will have their own expectations regarding Digital Trust. We should collaborate and work with our counterparts and internal stakeholders in Legal (Compliance), Human Resources (Employees) and Procurement (Business Partners), and Marketing & Sales (Customer) to conduct surveys, facilitate interviews, and solicit feedback to gather insights and perspective.

Each group of legitimate stakeholders will hold distinct expectations related to your enterprise's Digital Trust posture, reflecting their specific interests and concerns. Building and maintaining trust with these diverse stakeholders is essential for the enterprise's long-term success, reputation, and sustainability in the modern business age.

To that end, the following is meant to explore the unique expectations and perspectives of various stakeholders in the context of an enterprise's Digital Trust posture and not intended to be exhaustive, your mileage will vary region to region, enterprise to enterprise:

Activist Groups

Activist groups often focus on social and environmental issues. They expect the enterprise to demonstrate ethical behavior and responsible data practices as part of its Digital Trust commitment, aligning with their causes.

Advocacy Groups

Advocacy groups champion specific causes and expect the enterprise's Digital Trust posture to align with these causes. They may focus on issues such as data privacy, sustainability, or social responsibility.

Boards, Senior Management & Owners

Owners are primarily concerned with the financial performance and long-term sustainability of the enterprise. They expect the Digital Trust posture to protect the company's reputation and assets, ensuring consistent profitability and growth.

Competitors

Competitors closely watch each other's moves. They may expect the enterprise to maintain a strong Digital Trust posture to avoid incidents hat could benefit competitors and damage the enterprise's reputation.

Consumers

Consumers demand privacy, security and reliability. They expect the enterprise to protect their personal data, deliver secure digital services, and provide responsive customer support, enhancing their trust in the brand.

Employees

Employees value job stability, a safe work environment and fair treatment. They expect the Digital Trust posture to safeguard their data, foster a culture of security awareness and provide training to enhance their digital skills.

Financial Community

Investors and financial institutions seek stability and transparency. They expect the enterprise's Digital Trust posture to safeguard data, prevent cyber threats, and provide accurate financial reporting to maintain stock value and attract investments.

Government

Government agencies seek to protect national interests and ensure regulatory compliance. They expect the enterprise to comply with relevant laws and regulations, cooperate in cybersecurity efforts and contribute to national security.

Politicians

Politicians may be interested in constituents' concerns related to Digital Trust. They expect the enterprise to engage constructively in policy discussions and advocate for responsible digital practices. They may also expect enterprises to ensure the privacy and protection of data entrusted to them by their constituents nor that data be used to manipulate their constituents.

Regulators

Regulators enforce industry-specific rules and standards. They expect the enterprise to adhere to these regulations, maintain accurate records, and provide timely reports on privacy, security and compliance matters.

Suppliers & Business Partners

Suppliers and partners rely on trust to maintain productive relationships. There is a bi-directional expectation that the Digital Trust posture will ensure data privacy, security and integrity in supply chain operations.

Trade Associations

Trade associations aim to promote industry standards and best practices. They expect the enterprise to actively participate in industry initiatives related to Digital Trust and contribute to the development of guidelines and standards.

Unions

Unions represent employees and prioritize job security, fair treatment, working conditions, and employee privacy. They expect the Digital Trust posture to protect employee data and ensure the ethical use of technology in the workplace.

The Criminal Perspective of Digital Trust

We've discussed the legitimate stakeholders – however, we are dedicated a section specifically for the unnamed stakeholder and are going to now provide you the perspective of cybercriminals, an enterprise's Digital Trust posture is a perpetual challenge, a puzzle to be solved, and an opportunity for exploitation and making away with their ill-gotten gains. Criminals view security measures as obstacles to overcome rather than trust-building mechanisms.

This perspective should provide insight into the importance of an enterprises maintaining a robust and dynamic security posture to stay one step ahead in the ever-evolving digital threat landscape. It's a game of cat and mouse where staying vigilant and proactive is essential to safeguarding the digital trust of all other stakeholders.

From the Perspective of Cybercriminals: Unveiling Vulnerabilities

Cybercriminals, often operating in the shadows of the digital world, they see an enterprise's Digital Trust posture quite differently from other stakeholders. To them, it's not about trust; it's

about finding vulnerabilities, opportunities, and weaknesses they can exploit for gain. These individuals or groups are well-versed in the art of cybercrime, social engineering, and exploiting human errors. From their perspective, a strong Digital Trust posture is simply another challenge to overcome.

Identifying Weak Links

Cybercriminals view an enterprise's Digital Trust posture as an intricate puzzle with potential weak links. They meticulously analyze the digital ecosystem, probing for any signs of vulnerability. This could range from unpatched software, misconfigured security settings, to unsuspecting employees who can be tricked into revealing sensitive information.

The Value of Data

To cybercriminals, the data is the currency of the day. They understand that behind every firewall and encryption lies a treasure trove of valuable information – customer data, intellectual property, financial records, and more. These individuals are motivated by financial gain, espionage, or simply the thrill of breaching security measures.

Exploiting Human Factors

Cybercriminals recognize that human beings are often the weakest link in the chain. They use techniques like phishing and social engineering to manipulate employees into divulging sensitive information or clicking on malicious links. They may even target disadvantaged, disgruntled or marginalized employees as potential insiders to action on their objectives.

The Game is Afoot

To cybercriminals, your enterprise's security and privacy measures are just part of a continuous cat-and-mouse game. They thrive on innovation, constantly adapting their tactics to bypass security defenses. For them, a strong Digital Trust posture is a challenge, an obstacle to overcome, and a source of motivation; a trophy to be claimed!

Exploiting Emerging Technologies

Cybercriminals are quick to exploit emerging technologies often much faster than we adopt reasonable and appropriate controls to protect them. They see the rapid adoption of IoT devices, cloud services, and mobile platforms as new attack vectors. In their view, these technologies often outpace security protocols, providing them with opportunities to take advantage and exploit.

Economic Motivations

At the end of the day, most cybercriminals are driven by financial gain. They will view an enterprise's weak or immature Digital Trust posture as a potential source of income through ransomware attacks, data breaches, or selling stolen information. For most cyber-criminal syndicates, they operate similar to a traditional, legitimate business. They have established operations, customer base, marketing & sales, and they are seeking any method possible to monetize their skills and capabilities for profitable gains.

Lack of Trust in Security Measures

Ironically, cybercriminals often have little trust in the security measures implemented by enterprises. They are (and all too often, rightly so) confident in their ability to find and exploit vulnerabilities; we must do better at protecting the data and information we are entrusted with.

A Collective Call to Action: Fostering and Maintaining Digital Trust

We live in an omniconnected world, data flows freely and technology is woven into the very fabric of our lives, the concept of Digital Trust has never been more critical. It's a shared responsibility that involves a multitude of stakeholders, each playing a unique role in shaping the landscape of trust and security. From legitimate stakeholders to those with malicious intent, the digital realm is a complex web of relationships, expectations and vulnerabilities.

The Imperative of Digital Trust

For legitimate stakeholders like businesses, governments, consumers and activists, Digital Trust is the cornerstone of our digital age. It's the foundation upon which innovation, commerce, and communication thrive. It's the assurance that our data is safe, our privacy is respected, and our digital experiences are secure.

The Challenges We Face

As mentioned, this trust is constantly under siege. Cybercriminals, driven by financial gain, power or notoriety, relentlessly exploit weaknesses in our digital defenses. They view our systems as puzzles to solve, and our data as a currency to steal. This constant threat underscores the urgency of action.

A Shared Responsibility

It is understood that maintaining Digital Trust is not the responsibility of a single entity or organization. It's a shared responsibility that spans the public and private sectors: governments, businesses and individuals. We all have a role to play in the Digital Trust Ecosystem.

For the Enterprise

Businesses must invest in robust cybersecurity measures, protect customer data as if it were their own, and foster a culture of security within their organizations. They must continuously innovate to stay ahead of cyber threats, recognizing that security is not just a cost but a strategic imperative.

For Governments and Regulators

This is not going to be a popular opinion; however, Governments will need to play a pivotal role in shaping the regulatory environment that guides digital trust. They must craft policies that strike a delicate balance between security and privacy, enforce regulations to hold bad actors accountable, and collaborate internationally to combat cybercrime.

For Consumers and Advocacy Groups

Consumers must be vigilant custodians of their own digital security. They should demand transparency from businesses about how their data is used and advocate for strong privacy protections. Advocacy groups play a crucial role in raising awareness and holding organizations accountable.

For Everyone

Because we live in this interconnected world, we are all part of the solution. From the way we manage our passwords and the caution we exercise when clicking on links to what information we decide to share and with whom, our individual actions matter. Only together can we begin to address cyber threats.

We exist in this complex digital landscape, one in which we and cybercriminals alike coexist, we must come together to safeguard our digital future. Work with your stakeholders to build a digital world that is secure, transparent and worthy of trust.

Introduction to the SPENCER Framework: Building and Maintaining Digital Trust

In today's interconnected and data-driven world, the concept of Digital Trust has emerged as a cornerstone of success for organizations across industries. Digital Trust encompasses the confidence that individuals, customers, and stakeholders have in an organization's ability to protect their data, act ethically, and maintain compliance with regulations. It is not solely a technical concern but a strategic imperative that spans security, privacy, ethics, and transparency.

To navigate the complex landscape of Digital Trust, organizations need a structured approach that addresses various dimensions of trust-building. This is where the SPENCER Framework comes into play. The SPENCER Framework is a comprehensive model that helps organizations establish, maintain, and strengthen Digital Trust effectively.

Understanding the SPENCER Framework:

The SPENCER Framework comprises seven key component areas, each represented by a letter in the acronym:

Security Measures (S): Security is the foundation of Digital Trust. It encompasses practices, processes, and technologies that protect an organization's systems, data, and assets from cyber threats. Robust security measures help ensure the confidentiality, integrity and availability of information.

Privacy Protection (P): Data privacy is a fundamental aspect of Digital Trust. This component focuses on safeguarding individuals' personal information, respecting their privacy choices, and complying with data protection regulations.

Ethical Behavior (E): Trust extends beyond technical measures. Ethical behavior involves conducting business with integrity, fairness and adherence to moral principles. It includes ethical decision-making, transparency, and honesty.

Non-Invasive Practices (N): Trust should not come at the cost of intrusiveness. Non-invasive practices emphasize user-friendly, respectful data collection, and user control over their information. It aligns with privacy by design principles.

Compliance & Reporting (C): Compliance with laws and regulations is essential for Digital Trust. This component ensures that organizations not only meet legal requirements but also maintain transparency and accountability through reporting mechanisms.

Education & Training (E): People are a crucial part of the trust equation. Education and training programs equip employees and stakeholders with the knowledge and skills needed to protect data, make ethical decisions and contribute to trust-building efforts.

Regular Audits & Reporting (R): Continuous improvement and transparency are vital for Digital Trust. Regular audits and reporting activities help organizations identify vulnerabilities, measure compliance, and communicate their trustworthiness to stakeholders.

How the SPENCER Framework Maintains Digital Trust:

The SPENCER Framework is a holistic approach, recognizing that Digital Trust cannot be achieved through isolated efforts. It encourages organizations to:

Integrate Trust-Building: By addressing multiple dimensions of trust within a single framework, organizations can ensure that security, privacy, ethics and compliance are integrated into their operations and culture.

Adapt to Evolving Threats: Digital Trust is not static; it evolves with emerging threats and changing expectations. The SPENCER Framework provides a dynamic approach, encouraging organizations to continuously assess and adapt their practices.

Empower Stakeholders: Through non-invasive practices, user-friendly transparency, and ethical behavior, organizations empower stakeholders with choices and information, strengthening their trust.

Demonstrate Accountability: Compliance and reporting mechanisms hold organizations accountable for their actions and decisions, fostering trust by showcasing transparency and adherence to regulations.

Promote a Culture of Trust: Education and training initiatives instill trust-consciousness within the organization, making trust-building a collective effort.

Summary Thoughts

SPENCER Framework is a versatile tool that equips organizations to navigate the complex landscape of Digital Trust. By embracing this framework, organizations can proactively build and maintain trust with their customers, clients, partners and stakeholders, ultimately ensuring their long-term success in the digital age. Whether you're a technical expert or a non-technical leader, the SPENCER Framework provides a common language and approach to trust-building in the digital realm.

Overview of the SPENCER Framework

The goal of the SPENCER Framework is to provide a holistic approach to building and maintaining Digital Trust for the enterprise. It is a work-in-progress. The Framework underscores the collaboration between business and information technology in achieving trustworthiness and responsible digital practices. By integrating these key components, organizations can navigate the complex digital landscape while fostering trust among customers, clients, partners, and stakeholders.

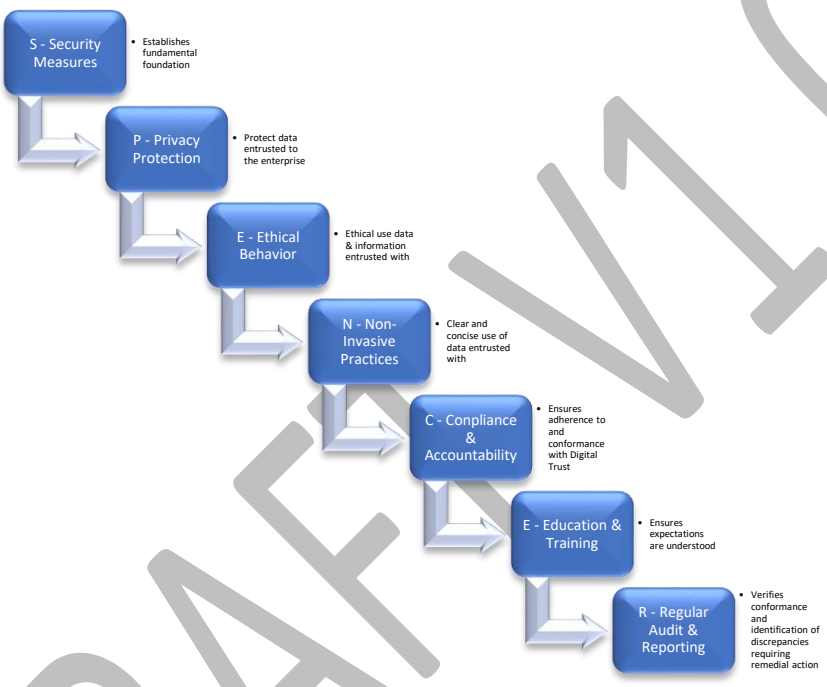


Figure 3 – The SPENCER Framework Digital Trust Waterfall

Security Measures

Security Measures encompass essential practices and technologies that protect an organization's digital assets and data. From a business perspective, they ensure the organization's reputation and financial stability by safeguarding information. In the realm of information technology, Security Measures involve deploying technologies like firewalls and encryption to defend against cyber threats and maintain data confidentiality, integrity, and availability.

Privacy Protection

Privacy Protection is all about respecting individuals' rights and securing their personal data. It builds trust with customers, enhances brand reputation, and ensures compliance with data protection laws. In IT, Privacy Protection includes encryption, access controls, and data anonymization techniques to safeguard personal information from unauthorized access, breaches, and misuse.

Ethical Behavior

Ethical Behavior in business means conducting operations with honesty, integrity and fairness. It is essential for building a positive corporate culture, attracting customers, and fostering long-term relationships. From an IT perspective, Ethical Behavior involves adhering to ethical guidelines in technology development, deployment and use. It ensures that technology is designed and used in ways that align with ethical principles.

Non-Invasive Practices

Non-Invasive Practices prioritize a user-centric approach, respecting individuals' privacy choices, providing user-friendly experiences, and minimizing intrusiveness. This enhances user trust and satisfaction from a business perspective. In IT, Non-Invasive Practices involve designing systems and applications that prioritize user consent, data transparency, and user control, ensuring that technology is respectful of user preferences.

Compliance & Reporting

Compliance & Reporting are critical for ensuring that the organization adheres to legal and regulatory requirements. This mitigates legal risks, builds transparency, and demonstrates a commitment to responsible business practices. From an IT perspective, IT professionals play a crucial role in compliance by implementing technical controls and ensuring data handling practices align with regulations. Reporting mechanisms help track and communicate compliance efforts.

Education & Training

Education & Training programs empower employees to make informed decisions, act ethically, and contribute to trust-building. They foster a culture of trust, improve employee engagement, and reduce risks associated with human error from a business perspective. In IT, IT professionals benefit from education and training on cybersecurity, data protection, and ethical technology use. It ensures that IT staff are equipped to implement and maintain secure and ethical technology solutions.

Regular Audits & Reporting

Regular Audits & Reporting involve assessing the organization's performance in security, privacy, ethics and compliance. These activities build accountability, allow for continuous improvement, and provide stakeholders with transparency. In IT, Audits & Reporting include conducting security assessments, vulnerability scans, and privacy audits. These activities help identify weaknesses and ensure that IT practices align with organizational goals and standards.

The SPENCER Framework

As previously stated, the SPENCER Framework is comprised of the following seven key components; these key components are:

- **S**ecurity Measures
- **P**rivacy Protections
- **E**thical Behavior
- **N**on-Invasive Practices
- **C**ompliance & Accountability
- **E**ducation & Training
- **R**egular Auditing & Reporting

Each of the key components includes various supporting fundamental practices and each practice consists of several individual processes. These processes in turn are supported by one or more activities.

Figure 4 Key Component Organizational Structure

A limited number of example metrics accompanies each practice as an example; these metrics are intended to be used to measure the achievement of the practice in meeting the desired objective and to ensure that the progress can be effectively managed.

Security Measures

The following need to be tailored to the organization and are provided with the aim of the establishing adequate practices, along with their associated processes and activities, with the goal to creating a starting a foundation for a formal Digital Trust framework with the goal of aligning the organization's Digital Trust posture.

Example metrics are provided to help gauge the effectiveness of each practice and contribute to achieving the overall objective.

Key Practice 1: Access Control Management

Description: Ensure proper access control measures are in place to protect sensitive information and systems.

Supporting Processes

User Authentication and Authorization

Description: Manage user access to systems and data through authentication and authorization.

Activities:

- User account creation
- Authentication validation
- Authorization assignment.

Example Metrics:

- User access provisioning time
- Access review completion rate

Access Monitoring and Logging

Description: Monitor and log access to detect and respond to unauthorized activities.

Activities:

- Log generation and centralized aggregation
- Log analysis
- Real-time or near-real-time monitoring and alerting

Example Metrics:

- Number of unauthorized access attempts
- Log retention period compliance

Incident Response and Escalation

Description: Establish procedures for identifying, reporting, and responding to security and privacy incidents.

Activities:

- Incident identification
- Incident triage analysis
- Incident notification, containment, and resolution

Example Metrics:

- Mean time to detect incidents
- Mean time to resolve incidents

Key Practice 2: Data Encryption

Description: Implement encryption mechanisms to protect data at rest and in transit.

Supporting Processes:

Data Classification and Encryption Policy

Description: Classify data and define encryption requirements based on sensitivity.

Activities:

- Data classification
- Encryption policy creation
- Key management

Example Metrics:

- Percentage of classified data
- Key rotation frequency

Encryption Implementation and Key Management

Description: Deploy encryption solutions for data protection and manage encryption keys securely.

Activities:

- Encryption tool selection
- Encryption configuration
- Key generation
- Key storage
- Key rotation

Example Metrics:

- Percentage of data encrypted
- Unique key utilization rate

Key Practice 3: Patch Management

Description: Maintain an effective patch management process to address vulnerabilities promptly.

Supporting Processes:

Vulnerability Assessment and Scanning

Description: Identify system vulnerabilities through regular scanning.

Activities:

- Threat modeling
- Vulnerability scanning
- Risk assessment
- Patch prioritization.

Example Metrics:

- Vulnerabilities detected
- Patch deployment time

Patch Testing and Deployment

Description: Test and deploy patches to mitigate known vulnerabilities.

Activities:

- COTS Patch testing (non-prod environment)
- Custom application patch testing (non-prod environment)
- Deployment scheduling

Example Metrics:

- Patch deployment success rate
- Time to test patches

Patch Verification and Compliance

Description: Verify that patches are correctly applied and systems are compliant.

Activities:

- Verification procedures
- Time to deploy critical patches
- Compliance audits

Example Metrics:

- Patch compliance rate
- System security posture

Key Practice 4: Network Security

Description: Implement network security measures to safeguard the organization's network infrastructure.

Supporting Processes:

Firewall Configuration and Monitoring

Description: Configure and monitor firewalls to control incoming and outgoing network traffic.

Activities:

- Firewall rule management
- Traffic monitoring

Example Metrics:

- Firewall rule effectiveness
- Firewall rule change requests

Network Segmentation

Description: Segment the network to isolate critical assets and reduce the attack surface.

Activities:

- Network design
- VLAN configuration
- Segmentation policy enforcement

Example Metrics:

- Segmentation coverage
- Compliance with network access policy

Key Practice 5: Security Awareness Training

Description: Provide ongoing security awareness training to educate employees about security and privacy risks and best practices.

Supporting Processes:

Training Needs Assessment

Description: Identify training needs based on job roles and security & privacy awareness gaps.

Activities:

- Training assessment
- Skills gap analysis
- Training content development

Example Metrics:

- Training needs identified
- Skills improvement rate

Training Delivery and Evaluation

Description: Deliver training programs and evaluate their effectiveness through assessments.

Activities:

- Training sessions
- Quizzes
- Knowledge retention assessments

Example Metrics:

- Training completion rate
- Post-training assessment scores

Key Practice 6: Security Incident Response Planning

Description: Develop and maintain a comprehensive incident response plan to mitigate and recover from security incidents.

Supporting Processes:

Incident Response Plan Development

Description: Create an incident response plan that defines roles, responsibilities, and procedures.

Activities:

- Drafting Incident Response Plan & Playbook
- Stakeholder review
- Incident categorization

Example Metrics:

- Plan completion status
- Incident categorization accuracy

Incident Simulation and Testing

Description: Conduct regular incident simulations and tests to ensure readiness.

Activities:

- Tabletop exercises
- Simulation scenarios
- Response time tracking

Example Metrics:

- Simulation frequency
- Response time improvement.

Key Practice 7: Security & Privacy Compliance Audits

Description: Conduct regular audits to ensure adherence to security & privacy policies, standards, and regulations.

Supporting Processes:

Audit Planning and Scope Definition

Description: Define the audit plan, scope, and objectives based on business driver requirements.

Activities:

- Audit plan development
- Scope definition
- Risk assessment

Example Metrics:

- Audit plan adherence
- Scope coverage

Audit Execution and Reporting

Description: Perform audits, gather evidence, and generate audit reports.

Activities:

- Audit fieldwork
- Evidence collection
- Report generation

Example Metrics:

- Audit completion time
- Findings resolution rate

Privacy Protection

The following addresses data privacy policies, consent management, data access control, data encryption, and privacy training, contributing to a comprehensive privacy protection strategy.

Key Practice 1: Data Privacy Policy and Governance

Description: Establish and govern data privacy policies and procedures to ensure compliance with privacy laws and regulations.

Supporting Processes:

Privacy Policy Development

Description: Develop comprehensive data privacy policies and guidelines.

Activities: Policy drafting, legal review, stakeholder consultation.
Example Metrics: Policy completion status, alignment with regulations.

Privacy Impact Assessments (PIAs)

Description: Conduct PIAs to assess the impact of data processing activities on privacy.

Activities:

- PIA documentation
- Data flow analysis
- Risk assessment

Example Metrics:

- PIA completion rate
- Risk mitigation effectiveness

Data Privacy Governance

Description: Establish a governance framework for monitoring and enforcing data privacy policies.

Activities:

- Governance board formation
- Policy enforcement
- Compliance audits

Example Metrics:

- Governance effectiveness
  Compliance audit results.

Key Practice 2: Data Minimization and Consent

Description: Implement practices to collect and process only necessary data and obtain consent when required.

Supporting Processes:

Data Classification and Inventory

Description: Classify data and maintain an inventory to identify sensitive information.

Activities:

- Data classification
- Data Asset Inventory management
- Data mapping

Example Metrics:

- Data classification accuracy
- Inventory completeness

Consent Management

Description: Develop processes to obtain, record, and manage user consents.

Activities:

- Consent capture
- Consent record maintenance
- Opt-out mechanisms

Example Metrics:

- Consent capture rate
- Opt-out requests

Key Practice 3: Data Access Control

Description: Implement controls to ensure that data is accessed only by authorized personnel for legitimate purposes.

Supporting Processes:

Access Control Policy

Description: Define access control policies and procedures.

Activities:

- Policy creation
- Role-based access control
- Permissions management

Example Metrics:

- Policy violations
- Policy exceptions
- Unauthorized access attempts

User Authentication and Authorization

Description: Implement strong user authentication and authorization mechanisms.

Activities:

- User authentication methods
- Access requests
- Role assignments

Example Metrics:

- Authentication success rate
- Access requests approved

Key Practice 4: Data Encryption and Security

Description: Protect data through encryption and security measures.

Supporting Processes:

Data Encryption

Description: Implement data encryption for data in transit and at rest.

Activities:

- Encryption deployment
- Key management
- Encryption audits

Example Metrics:

- Encryption coverage
- Key management compliance

Security Incident Response

Description: Establish processes for detecting and responding to data breaches.

Activities:

- Incident detection
- Incident response planning
- Ransomware Readiness
- Breach notification readiness

Example Metrics:

- Incident response time
- Breach notification compliance

Key Practice 5: Data Privacy Impact Assessment (DPIA)

Description: Conduct DPIAs to identify and mitigate privacy risks associated with data processing activities.

Supporting Processes:

DPIA Framework Development

Description: Establish a framework for conducting DPIAs, including criteria for risk assessment.

Activities:

- Framework design
- Policy development
- Engagement with various stakeholders
- Stakeholder alignment

Example Metrics:

- Framework satisfaction
- Alignment score

DPIA Execution

Description: Conduct DPIAs for all new data processing initiatives and significant changes.

Activities:

- Data mapping
- Risk assessment
- Mitigation planning

Example Metrics:

- Number of DPIAs conducted
- Risk reduction rate

Key Practice 6: Consent Management and Transparency

Description: Implement processes to ensure transparent data collection and obtain informed consent from data subjects.

Supporting Processes:

Consent Framework

Description: Develop a clear and comprehensive consent framework that aligns with privacy regulations.

Activities:

- Framework creation
- Stakeholder review
- Legal review
- Communication strategy

Example Metrics:

- Framework completeness
- Legal compliance

Consent Monitoring and Documentation

Description: Monitor and document consent for data processing activities.

Activities:

- Consent tracking
- Records management
- Auditing

Example Metrics:

- Consent audit results
- Compliance rate

Key Practice 7: Data Minimization and Retention

Description: Implement policies and procedures to limit data collection to the minimum necessary and establish retention schedules.

Supporting Processes:

Data Inventory and Classification

Description: Maintain an inventory of collected data and classify it based on sensitivity.

Activities:

- Data categorization
- Inventory management
- Data flow mapping

Example Metrics:

- Data categorization accuracy
- Inventory completeness

Data Minimization Review

Description: Regularly review data collection practices to minimize unnecessary data.

Activities:

- Data review, policy updates
- Stakeholder feedback

Example Metrics:

- Reduction in collected data
- Policy review frequency

Key Practice 8: Incident Response and Notification

Description: Develop a robust incident response plan for privacy breaches and notify affected individuals promptly.

Supporting Processes:

Incident Response Plan

Description: Create an incident response plan that addresses privacy breaches.

Activities:

- Plan development
- Stakeholder readiness training
- Technical readiness training
- Tabletop exercises

Example Metrics:

- Plan completeness
- Training participation

Incident Investigation and Notification

Description: Investigate privacy incidents, assess impact, and notify affected parties.

Activities:

- Incident investigation
- impact assessment
- Notification process

Example Metrics:

- Incident resolution time
- Notification effectiveness

Ethical Behavior

The following should aid in establishing a strong ethical code, ensuring its effective communication and monitoring, and promoting ethical leadership within the organization. They contribute to a culture of ethics and integrity.

By giving the proper consideration and focus on the development and communication of ethical codes, whistleblower protection, ethical decision-making, and stakeholder engagement. These initiatives promote a culture of ethical behavior within an organization and help address ethical challenges effectively.

Key Practice 1: Ethical Code Development and Implementation

Description: Develop and enforce an ethical code of conduct that guides behavior within the organization.

Supporting Processes:

Ethical Code Creation

Description: Formulate a comprehensive ethical code tailored to the organization's values and mission.

Activities:

- Stakeholder input
- Drafting code of ethics
- Reviewing code with stakeholders
- Soliciting approval for code of ethics

Example Metrics:

- Code completion time
- Stakeholder satisfaction

Code Communication and Training

Description: Communicate the ethical code to all employees and provide training on its principles.

Activities:

- Disseminating the Code of Ethics
- Training sessions on the Code of Ethics
- Receiving employee acknowledgment of the Code of Ethics

Example Metrics:

- Training completion rate
- Onboarding to Acknowledgement Lag Time
- Tracking Staff Acknowledgment

Ethical Behavior Reporting Mechanism

Description: Establish a confidential reporting mechanism for employees to report ethical concerns or violations.

Activities:

- Reporting system setup
- Ensuring accessibility
- Providing whistleblower protections

Example Metrics:

- Incident reports
- Resolution time

Key Practice 2: Ethical Behavior Monitoring and Enforcement

Description: Implement processes to monitor adherence to ethical standards and enforce consequences for violations.

Supporting Processes:

Ethical Behavior Assessment

Description: Conduct regular assessments to gauge employee compliance with the ethical code.

Activities:

- Assessment planning
- Conducting surveys
- Performing data analysis

Example Metrics:

- Frequency assessments are conducted
- Compliance scores

Incident Investigation and Resolution

Description: Investigate reported ethical violations and take appropriate actions.

Activities:

- Developing investigative procedures
- Performing investigations
- Collecting evidence
- Resolving incidents
- Performing root-cause analysis

Example Metrics:

- Investigation duration
- Resolution effectiveness

Key Practice 3: Ethical Leadership and Role Modeling

Description: Promote ethical behavior through leadership and by setting positive examples.

Supporting Processes:

Leadership Training and Development

Description: Provide leadership training programs that emphasize ethical leadership.

Activities:

- Training design
- Ethical leadership coaching
- Soliciting Feedback

Example Metrics:

- Leadership participation
- Feedback scores

Ethical Role Models Recognition

Description: Recognize and reward employees who consistently demonstrate ethical behavior.

Activities:

- Nomination process
- Recognition events
- Rewarding ethical behavior

Example Metrics:

- Nomination frequency
- Recognition awards

Key Practice 4: Whistleblower Protection

Description: Implement mechanisms to protect employees who report ethical violations.

Supporting Processes:

Whistleblower Program Setup

Description: Establish a confidential whistleblower reporting program.

Activities:

- Program design
- Establish reporting channels
- Develop communication plan

Example Metrics:

- Program completeness
- Reporting volume

Investigation and Response

Description: Investigate reported violations and respond appropriately.

Activities:

- Conduct investigations into reported violations
- Work to develop resolution for founded reports of violations
- Report on investigations
    - Reported
    - Investigated
    - Closed (Unfounded claims)
    - Closed (Founded claims)
    - Resolutions

Example Metrics:

- Violations reported
- Investigation closure time
- Resolution effectiveness

Key Practice 5: Ethical Decision-Making Framework

Description: Develop a framework to guide ethical decision-making in complex situations.

Supporting Processes:

Framework Design and Integration

Description: Create an ethical decision-making framework and integrate it into business processes.

Activities:

- Design and develop an ethical decision-making framework
- Review and seek feedback on framework
- Gain approval for framework from stakeholder
- Integrate the processes into the enterprise
- Conduct training on the framework

Example Metrics:

- Framework completeness
- Integration effectiveness
- Feedback results

Ethical Reviews

Description: Conduct ethical reviews of high-impact decisions or projects.

Activities:

- Review process design
- Review committee formation
- Conduct review of high-impact decisions and projects

Example Metrics:

- Review completion rates
- Decision impact assessment results

Key Practice 6: Stakeholder Engagement

Description: Engage with stakeholders to understand and address ethical concerns and expectations.

Supporting Processes:

Stakeholder Feedback Collection

Description: Establish feedback mechanisms for stakeholders to express ethical concerns.

Activities:

- Setup appropriate mechanisms to solicit and retain feedback
- Coordinate with general counsel
- Develop appropriate response plans to address ethical concern

Example Metrics:

- Feedback volume
- Response time

Ethical Impact Assessment

Description: Assess the ethical impact of business activities on stakeholders.

Activities:

- Conduct impact assessments
- Identify and collect appropriate metrics for assessment
- Perform root-cause analysis
- Develop mitigation planning
- Report on impact assessment reports

Example Metrics:

- Impact assessment completeness
- Mitigation effectiveness

Non-Invasive Practices

These practices, along with their supporting processes and activities, focus on data minimization, consent management, data anonymization, and user transparency to ensure that data collection and processing are non-invasive and respect individual privacy rights.

The following focuses on user privacy preferences, privacy impact assessments, privacy by design, and privacy incident response to further promote non-invasive data practices and safeguard user privacy.

Key Practice 1: Data Minimization

Description: Implement practices to collect and retain only the data necessary for the intended purpose.

Supporting Processes:

Data Inventory and Classification

Description: Create an inventory of all data collected and classify it by sensitivity.

Activities:

- Inventory data, considering both direct and indirect data elements
- Map data according to data classification
- Develop data classification criteria,
- Identify data owners who are responsible for data.

Example Metrics:

- Inventory completeness
- Classification accuracy

Data Retention Policy

Description: Establish a data retention policy specifying how long data should be retained.

Activities:

- Draft and develop Data Retention Policy with general counsel
- Review Data Retention Policy with stakeholders
- Communicate Data Retention Policy with staff
- Facilitate training on Data Retention requirements

Example Metrics:

- Policy exceptions
- Policy violations
- Compliance rate

Key Practice 2: Consent Management

Description: Develop processes for obtaining and managing user consent for data collection and processing.

Supporting Processes:

Consent Collection

Description: Implement methods to collect clear and informed consent from users.

Activities:

- Design a reasonable user consent forms relating to user's privacy and data collection
- Provide clear and easy to understand user training and education
  Design methods used to manage informed consent of users

Example Metrics:

- Consent rate
- Consent accuracy

Consent Revocation

Description: Enable users to easily revoke their consent at any time.

Activities:

- Establish mechanisms which allow users to easily revoke consent
- Support user requests to alter, update and/or revoke consent
- Ensure that appropriate audit trails are maintained which demonstrate changes and revocation of user consent

Example Metrics:

- Revocation requests
- Processing time

Key Practice 3: Data Anonymization

Description: Implement techniques to anonymize or pseudonymize data to protect individual identities.

Supporting Processes:

Anonymization Techniques

Description: Choose and apply appropriate anonymization methods.

Activities:

- Select appropriate data anonymization instrumentation
- Advise and work with SME's to ensure data is properly masked
- Testing to ensure anonymization techniques are effective

Example Metrics:

- Anonymization completeness
- Data utility assessment results

Regular Anonymization Audits

Description: Periodically audit and verify the effectiveness of anonymization techniques.

Activities:

- Plan anonymization readiness assessments
- Plan anonymization audit plan
- Collect sample data
- Analyze data for anonymization of data
- Assess the effectiveness of the mechanisms in place to allow for data anonymization

Example Metrics:

- Audit frequency
- Audit findings

Key Practice 4: User Transparency

Description: Communicate transparently with users about data collection, processing and purposes.

Supporting Processes:

Privacy Notices and Policies

Description: Create clear and comprehensive privacy notices and policies.

Activities:

- Collaborate with general counsel on existing privacy policies for potential gaps
- Draft privacy notice and policies (as necessary) with general counsel
- Review privacy policies with stakeholders
- Solicit feedback on privacy policies from stakeholders
- Ensure ease of accessibility to enterprise privacy notices and policies

Example Metrics:

- Notice completeness
- User comprehension

User Education

Description: Educate users about their data rights, choices, and privacy practices.

Activities:

- Create audience appropriate educational content
- Conduct and facilitate user training
- Collect feedback

Example Metrics:

- User engagement
- Education program effectiveness

Key Practice 5: User Privacy Preferences

Description: Develop mechanisms to allow users to specify their privacy preferences and tailor their experience accordingly.

Supporting Processes:

Privacy Preference Settings

Description: Create user-friendly privacy settings that allow users to customize data sharing and processing.

Activities:

- Design a user-friendly user interface design
- Develop a robust method allowing users to exercise their privacy preferences
- Test to ensure conformance with the user's privacy preferences

Example Metrics:

- Adoption rate of privacy settings
- User feedback

Preference Management

Description: Implement a system to manage and honor user privacy preferences.

Activities:

- Develop a mechanism to retain privacy preferences of stakeholders
- Ensure mechanism can be updated to reflect near-real-time privacy preference
- Enforce privacy consent preferences

Example Metrics:

- Preference accuracy
- System performance

Key Practice 6: Privacy Impact Assessments (PIAs)

Description: Conduct Privacy Impact Assessments to evaluate and mitigate potential privacy risks associated with new projects, processes, or technologies.

Supporting Processes:

PIA Framework

Description: Establish a standardized framework for conducting PIAs.

Activities:

- Create or tailor PIA templates for use
- Develop PIA guidelines development
- Conduct training on performing a PIA

Example Metrics:

- PIA completion rate
- Quality of assessments

PIA Implementation

Description: Integrate PIAs into project development cycles and ensure that identified risks are addressed.

Activities:

- Review privacy impact analysis
- Plan risk mitigation efforts
- Track projects for conformance

Example Metrics:

- Time to risk mitigation
- Project compliance

Key Practice 7: Privacy by Design

Description: Embed privacy considerations into the design and development of products, systems, and processes from the outset.

Supporting Processes:

Privacy Design Principles

Description: Define and communicate privacy design principles for all projects.

Activities:

- Develop privacy design principles
- Develop integration guidance, both technical and non-technical
- Conduct training and awareness campaigns

Example Metrics:

- Adoption of design principles
- Project alignment

Privacy Testing

Description: Incorporate privacy testing and validation as part of the quality assurance process.

Activities:

- Create test cases for ensuring privacy
- Automate testing
- Analyze test results

Example Metrics:

- Number of privacy issues identified/reported
- Resolution rate

Key Practice 8: Privacy Incident Response

Description: Establish a robust incident response plan for addressing privacy breaches or incidents promptly and effectively.

Supporting Processes:

Incident Detection

Description: Implement mechanisms for early detection of privacy incidents.

Activities:

- Monitoring for privacy violations and incidents
- Setting up alerts
- Detecting anomalies

Example Metrics:

- Incident detection time
- False positives

Incident Response Team

Description: Formulate a cross-functional team responsible for incident management.

Activities:

- Help identify and form the team
- Training for privacy incidents
    - Technical
    - Business
- Defining incident response roles

Example Metrics:

- Incident resolution time
- Team readiness

Compliance & Reporting

Here we focus on regulatory compliance management, data retention and disposal, privacy impact assessments, and compliance audits to strengthen the organization's commitment to compliance and accountability in data handling and protection.

Additionally, we'll include aspects of incident response, vendor risk management, policy enforcement and training, and continuous compliance monitoring, ensuring a robust and accountable approach to data security and privacy.

Key Practice 1: Regulatory Compliance Management

Description: Establish processes to ensure compliance with relevant laws, regulations, and standards governing data protection and privacy.

Supporting Processes:

Regulatory Landscape Assessment

Description: Regularly assess and monitor changes in data protection regulations and standards.

Activities:

- Research and assess any changes to regulatory requirements
- Perform a compliance-based gap analysis
- Track updates to the regulatory landscape
- Report on changes and advise as to methods to address in an ethical manner

Example Metrics:

- Timeliness of updates
- Compliance status

Compliance Roadmap

Description: Develop a comprehensive compliance roadmap outlining key milestones and actions.

Activities:

- Create a roadmap to achieve continuous compliance
- Determine the various roles, activities, and supporting resources needed to support compliance efforts within the enterprise
- Identify resources required needed to achieve milestones and complete associated actions
- Assign tasks to the appropriate roles and resources
- Ensure resources are properly optimized

Metrics:

- Milestone achievement
- Resource utilization

Key Practice 2: Data Retention and Disposal

Description: Implement processes for data retention, archiving, and secure disposal in accordance with legal requirements and internal policies.

Supporting Processes:

Data Classification

Description: Classify data based on sensitivity and define retention requirements.

Activities:

- Categorize data and information based upon defined regulatory standards relating to sensitive and user privacy preference
- Work with data owners to ensure that data classification occurs at the time of creation and is properly categorized, identified and handled according to the defined requirements.
- Work with technical subject matter experts to ensure that data classification is properly enforced
- Design and draft supporting policy, procedures and processes needed to support data classification within the enterprise
- Facilitate user training on the policy, procedures, processes, and technologies used to support data classification and the importance in maintaining Digital Trust

Example Metrics:

- Accuracy of data classification
- Policy exceptions
- Policy violations
- Policy conformance

Data Archiving and Purging

Description: Establish procedures for archiving and purging data based on its lifecycle.

Activities:

- Develop a strategy, based on data retention requirements and policy, to ensure the safety and security of archived data and information
- Develop and provide mechanisms to automate the data disposal process
- Manage and maintain audit trail documentation to support the proper retention and purging of data and information

- Ensure third-party service providers issue a Certificate of Destruction once there is no longer a valid business need or if user privacy preferences change
- Monitoring

Example Metrics:

- Archiving efficiency
- Data purging accuracy

Key Practice 3: Privacy Impact Assessments (PIAs)

Description: Conduct Privacy Impact Assessments (PIAs) for projects and initiatives involving personal data to identify and mitigate privacy risks.

Supporting Processes:

Policies and Procedures

Description: Develop PIA policies and procedures, including criteria for assessing risks.

Activities:

- Create or tailor PIA template
- Develop guidelines for operationalization of PIAs into business-as-usual practices
- Manage and maintain documentation relating to PIA
- Facilitate training and education on PIA processes
- Support risk analysis, evaluation and assessment efforts

Example Metrics:

- Completeness of PIAs performed
- Timeliness of PIAs performed
- Policy exceptions
- Policy violations

PIA Implementation

Description: Integrate PIAs into project development cycles and ensure that identified risks are addressed.

Activities:

- Review PIAs with affected project teams
- Work with project teams to ensure integration with the development cycles
- Plan reasonable risk mitigations in accordance with the enterprises risk appetite and tolerance criteria
- Work with project teams to ensure that risks are properly captured
- Track risks through to completion and resolution

Example Metrics:

- Timely mitigation efforts
- Project compliance

Key Practice 4: Compliance Audits and Assessments

Description: Conduct regular compliance audits and assessments to verify adherence to policies and regulations.

Supporting Processes:

Audit Planning

Description: Plan and schedule compliance audits and assessments.

Activities:

- Work with the appropriate stakeholders to develop and properly define the audit scope
- Ensure that the goals and objectives of the audit are clearly defined and communicated to the appropriate stakeholders
- Identify needed resources required to execute the audit
- Work with affected stakeholders to plan and schedule the audit

Example Metrics:

- Audit schedule adherence
- Scope Accuracy
- Scope Completeness

Audit Execution

Description: Execute audits according to the predefined plan, including data sampling and interviews.

Activities:

- Identify appropriate sources of data/information to support conformance
- Collect appropriate data to determine effectiveness
- Conduct interviews
- Maintain audit documentation (field notes, working papers, etc.)
- Analyze data and determine conformance with the requirements
- Draft and deliver report to the appropriate stakeholders

Example Metrics:

- Audit findings accuracy
- Timeliness.

Key Practice 5: Incident Response and Reporting

Description: Establish processes for detecting, reporting, and responding to security incidents in a timely and effective manner.

Supporting Processes:

Incident Detection

Description: Implement mechanisms for identifying privacy and security incidents promptly.

Activities:

- Establishing network and user behavioral baselines
- Ensure completeness of log-source generation
- Establish methods to properly collect, analyze and alert logs being received
- Tune and test intrusion detection/prevention systems to ensure effectiveness and to reduce background noise
- Ensure that threat hunting activities are being performed within the enterprise environment

Example Metrics:

- Incident detection time
- Number of false positives

Incident Reporting

Description: Define procedures for reporting security incidents to relevant stakeholders, including authorities if required.

Activities:

- Develop appropriate IR procedural documentation for reporting privacy and security incidents
- Establish protocols for notification and escalation of incidents
- Work with general counsel to identify and align legal compliance requirements with incident response efforts and activities

Example Metrics:

- Timeliness of reporting
- Completeness of documentation

Incident Response Plan (IRP)

Description: Develop and maintain an IRP outlining roles, responsibilities, and actions during privacy and security incidents.

Activities:

- Creating an enterprise reasonable and appropriate IRP
- Identifying key roles & responsibilities of the IR team
- Training IR members in relationship to their respective roles
- Facilitating tabletop exercises

Example Metrics:

- IRP effectiveness
- Staff readiness

Key Practice 6: Vendor Risk Management

Description: Implement processes for assessing and managing security and privacy risks associated with third-party vendors.

Supporting Processes:

Vendor Assessment

Description: Evaluate the security and privacy practices of vendors before engagement.

Activities:

- Perform vendor risk assessments
- Conduct due diligence
- Assess risk of vendor to the enterprise
- Assess risk to those who have entrusted their data and information to the enterprise

Example Metrics:

- Vendor risk assessments completed vs. outstanding
- Vendor risk posture

Contractual Controls

Description: Define security and privacy requirements in vendor contracts and agreements.

Activities:

- Work with general counsel to ensure appropriate contract clauses are included
- Review contracts with general counsel to identify potential gaps or unnecessary risks
- Ensure a right to audit compliance, privacy and security are included in all enterprise contracts

- Ensure “right to audit” clause is scheduled and performed, in accordance with vendor risk posture and risk introduced to the enterprise
- Establish appropriate privacy and security requirements within both the contract and Service Level Agreements (SLAs)
- Include those vendors that have access to enterprise systems or process data on behalf of the enterprise in incident response practices
- Monitor SLAs
- Enforce contractual obligations

Example Metrics:

- Contract compliance
    - SLAs met vs. breached
- Dispute resolution

Key Practice 7: Policy Enforcement and Training

Description: Ensure policies related to security, privacy, and compliance are enforced consistently, and employees receive appropriate training.

Supporting Processes:

Policy Enforcement

Description: Implement mechanisms to enforce security, privacy, and compliance policies.

Activities:

- Develop business-appropriate access control management processes and identify enforcement methods.
- Review policies with stakeholders
- Monitor policy for violations and approved exceptions
- Identify and report risks based on policy non-conformance

Example Metrics:

- Policy exceptions
- Policy violations
- Access control effectiveness

Employee Training

Description: Develop and deliver training programs to educate employees about security, privacy, and compliance.

Activities:

- Develop appropriate, audience relevant education and training curriculum
- Perform employee assessments
- Develop awareness and training campaigns for the enterprise

Example Metrics:

- Training completion rates
- Knowledge assessment results

Key Practice 8: Continuous Compliance Monitoring

Description: Establish ongoing monitoring processes to ensure continuous compliance with relevant regulations and standards.

Supporting Processes:

Regulatory Monitoring

Description: Monitor changes in regulations and standards relevant to the organization.

Activities:

- Work with general counsel in researching applicable regulatory requirements
- Develop a framework of applicable regulations with general counsel
- Perform a gap analysis
- Track updates and changes to the regulatory landscape

Example Metrics:

- Timeliness of updates
- Compliance status

Compliance Audits

Description: Conduct regular compliance audits to verify adherence to policies and regulations.

Activities:

- Work with compliance team in the planning audits
- Working with compliance team to schedule and executed planned audits
- Working with the appropriate stakeholders on resolving any findings which introduce unnecessary risk to the enterprise

Example Metrics:

- Audit schedule adherence
- Findings resolution time

Education & Training

As with any changes within an organization, your desired and expected outcomes are only a result of proper education and training. Here we are going to place focus on security awareness, incident response training, privacy training, and ongoing awareness campaigns, ensuring a well-informed and prepared workforce.

These address compliance, technology proficiency, and cybersecurity awareness, ensuring employees have the knowledge and skills needed for their roles and responsibilities within the organization.

Key Practice 1: Security Awareness Training

Description: Provide ongoing security awareness training to employees to enhance their knowledge and understanding of security best practices.

Supporting Processes:

Training Needs Assessment

Description: Identify specific training needs based on employee roles and responsibilities.

Activities:

- Identify the core fundamental skills required by each employee role, commensurate with their responsibilities within the enterprise
- Interview sample set employees to gain their understanding of privacy and security
- Conduct a skills gap analysis
- Analyze results to determine common trends, misunderstandings, or other gaps in understanding privacy and security concepts
- Develop and deliver security awareness training

Example Metrics:

- Training needs identified
- Skills gap improvement

Training Program Development

Description: Create customized training programs based on identified needs.

Activities:

- Design audience-appropriate curriculum
- Develop adequate content to ensure learning objectives are satisfied
- Create training material for broad range of relevant subject matters
- Manage, maintain and update training materials to ensure relevancy of topics

- Ensure that training records are managed and maintained throughout the employment lifecycle
- Engage with stakeholders to identify training needs
- Conduct training assessments to identify gaps in existing training requirements

Example Metrics:

- Training materials developed
- Curriculum updates

Training Delivery

Description: Deliver training sessions through various channels, including in-person and online.

Activities:

- Review and tailor training to audience needs
- Deliver training
- Facilitate training workshops
- Solicit feedback from attendees

Example Metrics:

- Training sessions conducted
- Completion rates
- Knowledge retention reports
- User feedback

Key Practice 2: Security Incident Response Training

Description: Provide specialized training to employees involved in incident response to ensure effective and coordinated responses to security incidents.

Supporting Processes:

Incident Response Team Formation

Description: Identify and assemble an incident response team with defined roles.

Activities:

- Identify IR team members, needs to be multidisciplinary
- Create and clearly define the various IR roles and responsibilities
- Assess the skills of all time members
- Conduct formal IR team training
- Facilitate team tabletop exercises

Example Metrics:

- Team participation in exercises
- Tabletop exercises conducted
- Trainings conducted
- Overall team readiness

Simulated Incident Drills

Description: Conduct regular simulated incident drills to test the response team's capabilities.

Activities:

- Establish the goals for both the incident drill and the associated roles
- Develop credible, real-world incident scenarios to be simulated
- Record responses from each member
- Solicit feedback from the IR Team on the scenario simulated
- Evaluate member responses based on established goals
- Facilitate lessons learned sessions
- Capture, manage and maintain records of lessons learned
- Identify gaps in controls
- Identify opportunities for improvement
- Report on results of incident drill

Example Metrics:

- Drill frequency
- Response Results (effectiveness)

Key Practice 3: Privacy Training

Description: Provide comprehensive privacy training to employees, ensuring they understand and adhere to privacy regulations and best practices.

Supporting Processes:

Privacy Regulations Awareness

Description: Educate employees on relevant privacy regulations and their implications.

Activities:

- Facilitate sessions to promote privacy awareness
- Promote audience appropriate awareness efforts
- Ensure employees understand the implications if they should fail to comply
- Report on updates on changes to applicable privacy laws
- Manage, maintain and track employee attendance records

Example Metrics:

- Employees' awareness levels
- Regulatory update reports

Privacy Policy Training

Description: Train employees on the organization's privacy policies and procedures.

Activities:

- Facilitate training on changes to the enterprise Privacy policy
- Ensure mechanisms are in place where staff must acknowledge policy training
- Maintain and manage training records

Example Metrics:

- Policy acknowledgment rates
- Compliance checks

Key Practice 4: Security and Privacy Awareness Campaigns

Description: Conduct awareness campaigns to keep security and privacy topics at the forefront of employees' minds.

Supporting Processes:

Campaign Planning

Description: Plan and design awareness campaigns with engaging content.

Activities:

- Create awareness campaign content
- Work with stakeholders to schedule campaigns
- Identify the appropriate communication channels
- Maintain and management campaign records to identify effectiveness and engagement trends

Example Metrics:

- Campaign effectiveness
- Engagement rates

Campaign Execution

Description: Implement awareness campaigns and measure their impact.

Activities:

- Deliver campaign to appropriate staff and applicable service-providers

- Develop surveys to gauge effectiveness and measure awareness
- Collect and analyze feedback
- Track and trend campaign data over time to identify methods which work and ensures greatest participation and knowledge retention

Example Metrics:

- Participation rates
- Knowledge retention

Key Practice 5: Compliance Training

Description: Provide specialized training to employees on regulatory compliance requirements relevant to your industry and organization.

Supporting Processes:

Regulatory Mapping

Description: Identify and map specific regulatory requirements to relevant employee roles.

Activities:

- Manage and maintain inventory of applicable and relevant regulatory library
- Map applicable regulatory requirements in context to associated business operations
- Analyze applicable regulatory requirements and determine enterprise compliance
- Assess applicable and relevant compliance requirements based on defined roles

Example Metrics:

- Mapping completeness
- Role-specific compliance assessments

Customized Compliance Training

Description: Develop tailored compliance training modules based on mapped regulatory requirements.

Activities:

- Design customized compliance training curriculum
- Develop audience appropriate content
- Create compliance training materials
- Deliver compliance training materials
- Maintain and management of training materials
- Maintain and management of staff training records

Example Metrics:

- Training modules developed
- Curriculum updates

Compliance Training Delivery

Description: Deliver compliance training sessions through various channels, ensuring employee understanding and adherence.

Activities:

- Facilitate audience appropriate compliance training sessions
- Develop mechanisms to reinforce and support compliance training efforts (e.g., e-learning, quizzes, testing, etc.)
- Deliver compliance training
- Perform periodic knowledge retention assessments

Example Metrics:

- Training sessions conducted
- Compliance assessment scores.

Key Practice 6: Technology Training

Description: Provide training on specific technologies and tools used within the organization to maximize their effectiveness and security.

Supporting Processes:

Technical Skills & Proficiency Assessment

Description: Assess the technology proficiency of employees and identify skill gaps.

Activities:

- Test users on their technical proficiency assessments
- Analyze results to identify skills gap
- Develop appropriate training and education programs to close skill gaps

Example Metrics:

- Proficiency testing scores
- Skills improvement scores

Technology Training Program

Description: Develop a comprehensive training program for each technology or tool in use.

Activities:

- Design audience appropriate curriculum
- Develop adequate content relating to the relevant technologies
- Create appropriate, user-friendly technology training materials

Example Metrics:

- Training materials developed
- Curriculum updates

Technology Training Delivery

Description: Deliver technology training sessions through various channels, ensuring employees can effectively use the tools.

Activities:

- Facilitating technology training and user familiarization sessions
- Conducting hands-on workshops with relevant technologies
- Assessing user proficiency

Example Metrics:

- Training sessions conducted
- Proficiency assessment scores

Key Practice 7: Cybersecurity Training

Description: Provide cybersecurity training to all employees to enhance their ability to recognize and respond to security threats.

Supporting Processes:

Security Threat Awareness

Description: Educate employees on common cybersecurity threats, tactics, and techniques.

Activities:

- Facilitating Threat awareness sessions
- Coordinating phishing simulations
- Collecting and providing threat intelligence updates

Example Metrics:

- Threat awareness levels
- Phishing simulation results

Cybersecurity Best Practices

Description: Train employees on cybersecurity best practices, including password management, secure communication, and data protection.

Activities:

- Facilitate best practice workshops
  Developing and delivering secure communication guidelines
- Auditing password technical policy enforcement to ensure adherence to approved enterprise standards

Example Metrics:

- Best practice adherence rates
- Policy compliance checks

Regular Audits & Reporting

To ensure a systematic approach to auditing, reporting, and addressing issues, contributing to the organization's overall Digital Trust objectives.

The goal is to promote a risk-focused planning, leverage data analytics and automation, engage stakeholders effectively, and improve the quality and relevance of audit reporting for better governance and compliance outcomes.

Key Practice 1: Audit Planning

Description: Develop a comprehensive plan for conducting regular audits of the organization's policies, processes, and controls.

Supporting Processes:

Audit Scope Definition

Description: Clearly define the scope of each audit, specifying what aspects of the organization will be audited.

Activities:

- Facilitate scoping meetings with all relevant stakeholders
- Ensure current and relevant risk assessment is available or if a risk assessment will need to be conducted
- Map audit objectives to the corresponding enterprise requirements
- Ensure audit objectives align with enterprise goals and objectives
- Define, document and communicate the objectives of the audit to the relevant stakeholders

Example Metrics:

- Scope documentation completeness
- Alignment with risk assessments

Audit Resource Allocation

Description: Allocate the necessary resources, including personnel, tools, and budget, for conducting audits effectively.

Activities:

- Plan and schedule appropriate audit resource, in collaboration with relevant stakeholders
- Determine level of effort for audit resources
- Develop audit budget requirements
- Select the appropriate audit team members
- Track planned vs. actual burn rates

Example Metrics:

- Resource allocation completeness
- Budget adherence

Audit Schedule Creation

Description: Develop a detailed audit schedule, specifying when each audit will take place and its duration.

Activities:

- Create an audit schedule/calendar
- Identify and assign roles to the appropriate audit team members
- Communicate schedule with affective stakeholders
- Scheduling meetings

Example Metrics:

- Audit schedule adherence
- Audit timelines

Key Practice 2: Audit Execution

Description: Conduct thorough audits according to the predefined scope and schedule, assessing compliance and identifying areas for improvement.

Supporting Processes:

Data Collection

Description: Gather relevant data, documents, and information needed to assess the audited areas.

Activities:

- Collect relevant data from authoritative sources
- Request and review relevant documentation
- Facilitate interviews with appropriate, authoritative business and technical subject matter experts
- Manage and monitor progress to ensure schedule is maintained
- Identify potential opportunities for improvement (findings, gaps, or deficiencies)
- Manage and maintain all evidence and artifacts associated with the audit

Example Metrics:

- Data completeness

Audit Testing

Description: Perform testing and examination of controls, processes, and activities to evaluate their effectiveness.

Activities:

- Identify appropriate controls
- Test controls to ensure expected and effective outcomes are met
- Identify appropriate processes
- Perform walkthroughs of identified processes
- Test processes to ensure expected outcomes are generated
- Analyze data

Example Metrics:

- Test results
- Control effectiveness ratings

Issue Identification

Description: Identify and document any issues, discrepancies, or non-compliance found during the audit.

Activities:

- Track and monitor identified issues through resolution
- Facilitate and record efforts associated with root cause analysis
- Manage and maintain all relevant documentation of findings

Example Metrics:

- Issue identification rates
- Root cause analysis completeness

Key Practice 3: Reporting and Remediation

Description: Compile audit findings, create reports, and ensure timely remediation of identified issues.

Supporting Processes:

Audit Reporting

Description: Prepare comprehensive audit reports detailing findings, recommendations, and corrective actions.

Activities:

- Drafting reports with sufficient information with recommendations
- Drafting remediation plans
- Review reports with appropriate stakeholders to ensure completeness
- Work with the relevant stakeholders to develop business cases
- Manage and maintain historical audit evidence and reports
- Analyze past audits to identify trends

Example Metrics:

- Report completeness
- Distribution timelines

Issue Resolution

Description: Track and monitor the resolution of identified issues and non-compliance.

Activities:

- Track identified issues through resolution
- Assign action items to appropriate teams and individuals
- Collect progress on issue resolution efforts
- Report on updates to issue status to the appropriate stakeholders

Example Metrics:

- Issue resolution rates
- Action item completion

Continuous Improvement

Description: Implement process improvements based on audit findings and lessons learned.

Activities:

- Review audit findings to ensure audit standard aligns with the enterprise requirements
- Facilitate, manage and maintain information from lessons learned sessions
- Analyze key and supporting business and technology processes

- Identify key business and technology processes which can be optimized
- Work with stakeholders to identify potential future-state maturity levels of enterprise practices
- Analyze industry best practices to determine appropriateness of integration
- Perform a gap-analysis between desired enterprise future-state and appropriate best practice
- Develop roadmap to close gaps

Example Metrics:

- Improvement initiative completion
- Process enhancement impact

Key Practice 4: Risk Assessment and Audit Planning

Description: Assess organizational risks and plan audits accordingly to focus on high-risk areas.

Supporting Processes:

Risk Identification and Assessment

Description: Identify and assess risks associated with different aspects of the organization.

Activities:

- Facilitate threat scenario workshops
- Developing threat models based on threat scenarios
- Performing risk analysis
- Evaluating results of risk analysis in context of enterprise risk appetite and risk tolerance criteria
- Assess risks in context of available controls
- Identify potential gaps that would allow a unacceptable, inherit risk to persist
- Recommend reasonable and appropriate mitigation, commensurate with the inherent risk identified

Example Metrics:

- Number of identified risks
- Risk severity rankings

Risk-Based Audit Planning

Description: Develop audit plans that prioritize areas with higher risks for more frequent and in-depth audits.

Activities:

- Map risks to objectives, operations or threats to the enterprise
- Adjusting audit plan to address risks which are defined as unacceptable by the enterprise
- Allocate appropriate resources to monitor and report on status of identified, unacceptable risks

Example Metrics:

- Audit plan alignment with risk assessments
- Identified risks exceeding risk acceptance or risk criteria thresholds

Key Practice 5: Data Analytics in Auditing

Description: Utilize data analytics techniques to enhance the effectiveness of audits.

Supporting Processes:

Data Preparation and Analysis

Description: Collect, normalize, and analyze data using available data analytics tools and techniques.

Activities:

- Defining data quality rules with the appropriate stakeholders
- Collect audit data from authoritative sources
- Normalize data, ensuring that it can be properly modeled, organized structured to meet the analytics requirements
- Ensure data validity, identify errors or other issues to ensure accuracy and appropriateness of the data set
- Process data for analysis
- Analyze data to identify deficiencies, trends or support claims of conformance.

Example Metrics:

- Data quality

Continuous Monitoring

Description: Implement continuous monitoring systems to detect anomalies and issues in real-time.

Activities:

- Establish network and user behavior baseline activity to reduce noise and identify anomalies more effectively and efficiently
- Work with the business owners to determine and define appropriate Service Level Agreements to respond to anomalies and issues
- Identifying authoritative log sources

- Defining required elements to be captured by log sources
- Setting up instrumentation to support continuous monitoring
- Ensuring appropriate staff resources are allocated to identify and respond to alerts and issues in support of defined SLAs
- Configure systems to alert based on defined criteria
- Developing meaningful monitoring dashboards

Example Metrics:

- Number of detected anomalies
- Response time to anomalies

Key Practice 6: Audit Automation

Description: Automate audit processes and reporting to increase efficiency and reduce manual effort.

Supporting Processes:

Audit Workflow Automation

Description: Automate the workflow of audit activities, from planning to reporting.

Activities:

- Performing business process mapping
- Performing business process analysis
- Developing data flow diagrams
- Capturing and visualizing information flows
- Researching automation capabilities available to the enterprise
- Adequate understanding of the Enterprise Business architecture
- Adequate understanding of the Enterprise Information Technology architecture
- Adequate understanding of the Enterprise Security architecture
- Adequate understanding of the Enterprise Privacy architecture
- Assessing available automation capabilities and gaps in skills and competencies of the staff
- Design automated workflow design in context of the available capabilities, skills and competencies of the enterprise
- Seeking approval to implement appropriate automation instrumentation
- Monitoring and validating results of automation efforts

Example Metrics:

- Time saved through automation
- Error reduction

Key Practice 7: Stakeholder Engagement

Description: Engage stakeholders throughout the audit process to ensure transparency and alignment with organizational goals.

Supporting Processes:

Stakeholder Communication

Description: Establish clear channels of communication with stakeholders to gather input and provide updates.

Activities:

- Facilitate stakeholder meetings or updates, according to the needs of the stakeholders involved or affected
- Identify how the audit has been aligned with satisfying enterprise goals
- Develop communication plans for how each stakeholder will be kept abreast of the progression of the audit
- Regularly report on status and progress
- Solicit and collet feedback for analysis and improvement

Example Metrics:

- Stakeholder satisfaction
- Communication effectiveness

Key Practice 8: Audit Reporting Enhancement

Description: Enhance audit reporting to provide more actionable insights and recommendations.

Supporting Processes:

Interactive Reporting

Description: Create interactive audit reports with the ability for drill-down capabilities to provide detailed information and allow for additional context and/or insight perspectives.

Activities:

- Collaborate with stakeholders to capture their desired views and understand their perspectives
- Identify the reporting metrics which are the most valuable to the individual stakeholders
- Design reports/dashboards that allow for various elements to provide additional context and insights to be gained
- Implement interactive reporting mechanisms

Example Metrics:

- User engagement with interactive reports
- Report usability

Predictive Analytics in Reporting

Description: Incorporate predictive analytics to forecast potential risks and trends based on audit data.

Activities:

- Develop predictive models to identify potential risk to the enterprise (e.g., FAIR, HARM, etc.)
- Integrate data from disparate sources to ensure completeness in analysis efforts
- Analyze data to identify trends and insights into potential risks to the enterprise

Example Metrics:

- Accuracy of predictive models
- Actionable insights generated

How to Adopt the SPENCER Framework: Building and Maintaining Digital Trust

The SPENCER Framework offers a structured approach to build and maintain Digital Trust within your organization. To effectively adopt this framework it's important to involve executives, management and technology personnel collaboratively.

By tailoring operations to align with the spirit and intent of these guidelines and collaborating effectively, executives, management, and technology personnel can adopt and use the SPENCER Framework to build and maintain Digital Trust, positioning the organization for long-term success in the digital era.

Executive Overview

Understand the Importance of Digital Trust

Start by recognizing the critical role that Digital Trust plays in the organization's success, including reputation, customer loyalty, and compliance.

Commit to a Culture of Trust

Lead by example and promote ethical behavior, transparency, and a commitment to privacy and security at all levels of the organization.

Allocate Resources

Ensure that adequate resources, both financial and human, are allocated to support trust-building initiatives, including security, privacy, and compliance efforts.

Set Clear Objectives

Define specific Digital Trust objectives aligned with organizational goals and communicate these objectives to the entire team.

Establish Accountability

Assign accountability for Digital Trust initiatives to a designated executive or committee responsible for overseeing trust-building efforts.

Support Training and Education

Encourage and support ongoing education and training programs to ensure that employees are well-informed about trust-related topics.

Review and Report

Regularly review progress, audit findings, and reports related to Digital Trust. Use these insights to make informed decisions and improve trust-building efforts.

Management

Align with Business Goals

Understand how Digital Trust aligns with the organization's strategic goals. Ensure that trust-building initiatives are integrated into broader business plans.

Identify Key Stakeholders

Identify the key stakeholders who are affected by or contribute to Digital Trust efforts, including customers, partners, and regulatory authorities.

Develop Trust Policies

Collaborate with legal and compliance teams to develop and maintain comprehensive policies and standards for security, privacy, and ethical behavior.

Implement Security Measures

Work closely with technology personnel to implement security measures such as firewalls, encryption, and access controls to protect data and systems.

Privacy Protection & Transparency

Implement practices that respect user privacy, gain consent when necessary, and ensure transparency in data handling practices.

Promote Ethical Behavior

Foster a culture of ethical behavior by modeling ethical decision-making and creating channels for reporting ethical concerns.

Compliance & Reporting

Establish mechanisms for monitoring compliance with regulations, conducting regular audits, and reporting on compliance efforts.

Information Technology

Understand the Framework

Familiarize yourself with the SPENCER Framework, its components, and the role of technology in building Digital Trust.

Security Implementation

Implement robust security measures, including intrusion detection systems, encryption, and regular vulnerability assessments.

Privacy by Design

Integrate privacy considerations into technology design and development processes, ensuring data protection from the outset.

Ethical Technology Use

Ensure that technology solutions align with ethical guidelines and respect user preferences and rights.

Training and Awareness

Stay updated on the latest cybersecurity threats and privacy regulations. Provide training and awareness programs for employees.

Audit and Compliance

Collaborate with compliance teams to ensure that technology practices align with regulatory requirements. Facilitate audits and reporting efforts.

Incident Response

Develop and regularly test incident response plans to address security breaches and privacy incidents promptly and effectively.

General Guidelines for All

Collaboration

Foster cross-functional collaboration among executives, management, and technology personnel to ensure alignment and effective execution of Digital Trust initiatives.

Continuous Improvement

Embrace a culture of continuous improvement by regularly evaluating trust-building efforts, learning from incidents, and adjusting strategies accordingly.

Transparency

Communicate trust-building efforts transparently to stakeholders, including customers, partners, and employees, to build and maintain trust.

Benchmark and Best Practices

Stay informed about industry benchmarks and best practices in trust-building and leverage them to enhance your organization's approach.

Feedback Loop

Establish mechanisms for collecting feedback from stakeholders to understand their trust-related concerns and expectations.

External Expertise

Consider engaging external experts or consultants for specialized guidance in areas like security, privacy, and compliance.

Business Case: Adopting the SPENCER Framework to Maintain Digital Trust

Executive Summary

Digital Trust is paramount in today's interconnected world, impacting reputation, customer loyalty, and regulatory compliance. To build and maintain Digital Trust effectively, we propose adopting the SPENCER Framework. This comprehensive framework integrates security, privacy, ethics, and compliance efforts, positioning us as a trustworthy organization in the digital era.

I. Introduction – The Digital Trust Imperative

In an era where data breaches and privacy concerns dominate headlines, Digital Trust has become the linchpin of success. It directly influences customer confidence, competitive advantage, and regulatory compliance. To thrive in this environment, we must prioritize Digital Trust.

II. The SPENCER Framework – A Holistic Approach

The SPENCER Framework provides a structured approach to building and maintaining Digital Trust. It comprises seven key components:

Security Measures

Ensures robust protection against cyber threats.

Privacy Protection

Safeguards personal data while respecting privacy.

Ethical Behavior

Fosters a culture of ethics and transparency.

Non-Invasive Practices

Prioritizes user-centric and non-intrusive data handling.

Compliance & Reporting

Ensures adherence to regulations and transparent reporting.

Education & Training

Equips employees with knowledge to make trust-conscious decisions.

Regular Audits & Reporting

Enables continuous improvement and transparency.

III. Benefits of Adopting SPENCER

Enhanced Reputation

Demonstrates our commitment to trust, attracting and retaining customers.

Reduced Risk

Mitigates the risk of data breaches, regulatory fines, and legal liabilities.

Competitive Advantage

Sets us apart as a trustworthy partner and industry leader.

Customer Loyalty

Builds lasting customer relationships based on trust and transparency.

Compliance Assurance

Ensures alignment with evolving data protection regulations.

Improved Employee Engagement

Cultivates a culture of trust and ethical behavior.

Continuous Improvement

Provides a structured approach for ongoing enhancements.

IV. Implementation Plan

Executive Buy-In

Secure leadership support and commitment to prioritize Digital Trust.

Cross-Functional Teams

Establish teams spanning leadership, management, and technology personnel.

Assessment and Gap Analysis

Evaluate the current state of Digital Trust efforts.

Framework Customization

Tailor the SPENCER Framework to our unique needs and objectives.

Resource Allocation

Allocate budget and human resources to support trust-building initiatives.

Training and Education

Develop training programs and awareness campaigns.

Technology Integration

Implement necessary security and privacy technologies.

Regular Auditing

Conduct regular audits and assessments.

Reporting Mechanisms

Establish clear reporting channels for incidents and compliance.

Continuous Improvement

Continuously refine and adapt trust-building efforts based on metrics and feedback.

V. Metrics and Measurement

Define key performance indicators (KPIs) for each component of the SPENCER Framework. Regularly measure and report progress, adjusting strategies based on results.

The following KPIs should provide a robust view of your organization's adoption of the SPENCER Framework, in context of each key component of the SPENCER Framework.

Adoption and Management KPIs for the SPENCER Framework

Framework Adoption

- Framework Awareness - Percentage of employees and stakeholders who are aware of the SPENCER Framework.
- Framework Training Completion - Percentage of employees who have completed training on the SPENCER Framework.
- Adoption Rate - Percentage of relevant teams or departments that have implemented the SPENCER Framework's components.

Security Measures

- Security Framework Alignment - Percentage of security measures that align with the SPENCER Framework's security guidelines.
- Integration of SPENCER Security Guidelines - Percentage of critical systems or processes that have integrated security measures in alignment with the SPENCER Framework.

Privacy Protection

- Privacy Framework Alignment - Percentage of privacy protection practices that align with the SPENCER Framework's privacy guidelines.
- SPENCER Privacy Integration - Percentage of systems or applications that incorporate privacy protection measures as per the SPENCER Framework.

Ethical Behavior

- Ethical Culture Assessment - Score based on an assessment of the organization's ethical culture using SPENCER Framework guidelines.
- Ethical Behavior Integration - Percentage of business operations and decision-making processes that align with the SPENCER Framework's ethical guidelines.

Non-Invasive Practices

- User-Centric Implementation - Percentage of systems or processes designed with a user-centric approach following the SPENCER Framework.
- Non-Invasive Feedback - Feedback and survey scores on the user-friendliness and non-invasiveness of systems and applications following SPENCER Framework principles.

Compliance & Reporting

- Compliance Adherence - Percentage of compliance-related activities and practices following the SPENCER Framework's compliance guidelines.
- Reporting Transparency - Score indicating the transparency of reporting mechanisms as per the SPENCER Framework.

Education & Training

- Framework Training Effectiveness - Assessment of the effectiveness of SPENCER Framework training programs through employee feedback and assessments.
- Knowledge Transfer - Percentage of employees who have successfully integrated SPENCER Framework knowledge into their roles.

Regular Audits & Reporting

- Audit Conformance - Percentage of audit findings and processes that align with the SPENCER Framework's audit and reporting guidelines.
- Framework-Based Incident Response - Percentage of incidents handled according to SPENCER Framework incident response procedures.

VI. Cost-Benefit Analysis

Quantify potential cost savings from reduced security incidents and legal liabilities. Estimate revenue growth due to improved customer loyalty and trust.

VII. Risks and Mitigations

Identify potential challenges in adopting the SPENCER Framework and develop mitigation plans.

The following are potential challenges that you may identify or be raised and are purely for reference purposes. Please tailor to your organization as appropriate.

Adopting the SPENCER Framework for maintaining Digital Trust can be a transformative process, but it may also come with various challenges. The following are potential challenges and mitigations used to address them:

Challenge 1: Lack of Awareness and Understanding

Mitigations:
Conduct awareness sessions and training for employees at all levels to familiarize them with the SPENCER Framework. Develop comprehensive documentation and guidelines to help employees understand the framework's components and their relevance. Create a communication plan to regularly update stakeholders on the framework's progress and impact.

Challenge 2: Resistance to Change

Mitigations:
Involve key stakeholders, including executives and management, early in the adoption process to gain their support. Clearly communicate the benefits of adopting the SPENCER Framework, such as improved trust, reduced risks, and compliance. Implement a change management strategy that includes training, coaching, and support for employees as they adapt to new practices.

Challenge 3: Resource Constraints

Mitigations:
Conduct a resource assessment to identify the budget, personnel, and technology requirements for framework adoption. Prioritize initiatives based on their impact on trust and allocate resources accordingly. Explore partnerships with external experts or organizations to fill resource gaps.

Challenge 4: Framework Customization

Mitigations:
Tailor the SPENCER Framework to align with the organization's specific industry, size, and objectives. Involve cross-functional teams, including legal, compliance, IT, and HR, to ensure customization meets organizational needs. Continuously review and update the customized framework to remain adaptable to evolving challenges and requirements.

Challenge 5: Measurement and Metrics

Mitigations:
Define clear key performance indicators (KPIs) for each component of the SPENCER Framework. Implement technology solutions and tools to collect, analyze, and report on KPIs effectively. Regularly review and adjust KPIs to ensure they remain relevant and aligned with trust-building objectives.

Challenge 6: Resistance to Ethical Behavior and Cultural Change

Mitigations:
Develop and communicate a code of conduct and ethical guidelines that align with the SPENCER Framework. Provide ongoing ethics training and awareness programs for employees. Encourage a culture of transparency and accountability, where ethical behavior is celebrated and rewarded.

Challenge 7: Complexity of Compliance

Mitigations:
Establish a compliance team or committee responsible for interpreting and implementing regulations aligned with the SPENCER Framework. Invest in compliance management software and tools to streamline reporting and adherence. Conduct regular compliance audits to identify gaps and areas needing improvement.

Challenge 8: Resistance to Regular Audits and Reporting

Mitigations:
Educate employees and stakeholders about the importance of regular audits and reporting for trust-building. Ensure that audit processes are transparent and clearly communicate the purpose of audits. Implement automation tools for audits and reporting to minimize disruption to daily operations.

Challenge 9: Maintaining Consistency

Mitigations:
Develop detailed guidelines and procedures for each component of the SPENCER Framework. Establish a centralized repository for documentation and resources related to the framework. Conduct regular reviews and updates to maintain alignment with best practices and industry standards.

Challenge 10: Monitoring and Continuous Improvement

Mitigations:
Create a dedicated team or role responsible for monitoring framework adoption and effectiveness. Implement a feedback loop that involves stakeholders and employees in identifying areas for improvement. Encourage a culture of continuous improvement by celebrating successes and learning from setbacks.

VIII. Conclusion: A Digital Trust-Centric Future

In an age where trust is paramount, adopting the SPENCER Framework is an imperative strategic move. It ensures our organization remains at the forefront of trustworthiness, positioning us for long-term success in the digital era.

IX. Recommendation

We recommend adopting the SPENCER Framework to build and maintain Digital Trust. This investment will not only protect our organization but also empower us to thrive in an environment where trust is the currency of success.

By adopting SPENCER, we solidify our commitment to Digital Trust and set the stage for a future where trust is our competitive advantage.

The SPENCER Digital Trust Canvas

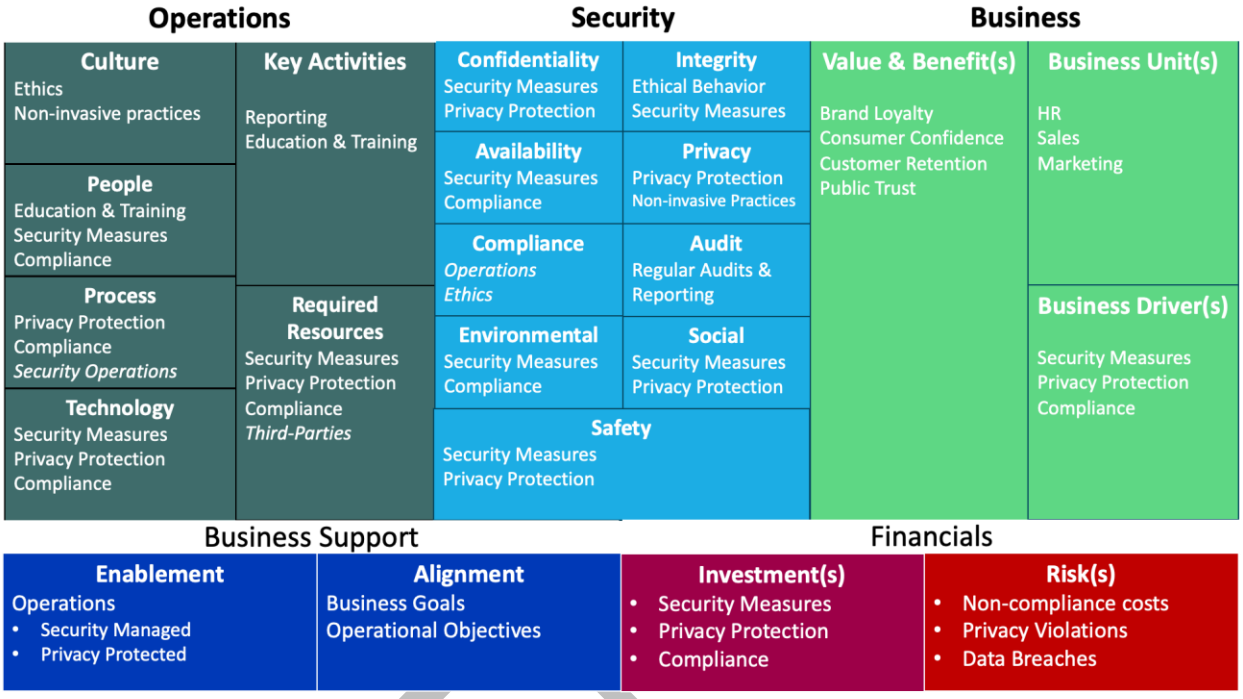


Figure 5 - SPENCER Canvas for maintaining Digital Trust

The SPENCER Canvas Model

Goals & Objectives

The primary goal of Digital Trust Modeling process is to quickly identify, link, visualize and communicate, at a high-level, the various elements associated with a business, information technology, privacy, and information/cyber security initiatives within the enterprise.

The goal of using Digital Trust Modeling is not meant to replace Business Cases; rather it is intended to quickly aid in understanding needs and potential impacts of specific initiatives, in a logical and cohesive manner to further build business cases and promote definition of requirements for those initiatives.

Terms

Initiative – any change to, introduction of, or retirement of a technology, process or control within an enterprise.

Example initiatives may include, but are not limited to, the following:

- Adding/Removing access to data repositories
- Changing the flow of client or other sensitive data within the environment
- Changing the network's architecture
- Decommissioning an legacy application
- Decreasing of budget
- Deploying new firewalls
- Establishing new control objectives.
- Exposing an API to internet
- Introducing a new business process
- Introducing a new client service offering
- Modifying existing control settings
- Offering new customer service offering
- Removing existing controls
- Retiring an internal service offering
- Training staff on a new system or application
- Training staff on new regulatory compliance requirements

Why use Digital Trust Modeling?

1. Quickly and easily understand and visualize the various elements of an initiative.
2. Allows for high-level focus from various enterprise standpoints
3. Flexible in nature
4. Ultimately it provides a business aligned focus as it pertains to an initiative
5. Creates and identifies linkages and provides traceability between the elements
6. Easy to communicate to all audiences
7. Expediency and timeliness

Background

The Digital Trust Modeling process was designed to address common misconceptions between the perceived "simple changes" made within an enterprise and how to properly maintain overall Digital Trust. The goal of the process is to help both Business and IT understand how requests may impact an enterprise's overall Digital Trust posture.

The process can be executed from either a business perspective, moving through the model right to left or from the technology perspective, moving from left to right through the model. This allows for initiatives originating from the business unit to flow from Business to IT, as well identifying how implementations, changes, enhancements or maintenance services introduced by IT may impact the enterprise.

The goal of the process is meant to create a dialogue and promote a better understanding between business and technology departments, with the focus of the process being to identify and capture high-level information, relationships, and impacts of an initiative, as well as how an initiative may influence other areas within the enterprise, which may not have been previously considered when the initiative was initially proposed or is being considered.

Each of the primary elements is populated with sufficient information needed to quickly visualize relationships of an initiative and how their interactions with other aspects of the model. This often results in better understanding of the business needs and drivers for IT staff, as well as provide sufficient rationalization and justification needed by the business when considering how they make investments.

Of note, the centerline of the model represents the **Enterprise's Information & Cyber Security Alignment** element. This is where most control objectives can get lost in translation, resulting in a breakdown of communications and misunderstandings between various lines of business and Information Technology. The purpose of this element is NOT to identify potential controls required to address a specific threat or subsequent risk; rather to capture and document the result of the initiative has on those respective various sub-elements.

When we study an enterprise's consideration and proposal of an initiative, we must understand what that means to both the enterprise as a whole and the business unit that is proposing the initiative and the outcome it plays on the overall Enterprise Information Security posture and by extension Business Risk. There are a number of initiatives that an enterprise may choose to undergo in order to achieve their defined enterprise strategy.

To ensure consistency and in order to establish a foundational baseline, when we say *enterprise strategy* we define this as "the set of goals, measures and milestones required to achieve success, as defined by the governing body." To better understand how an initiative plays into enabling an enterprise to achieve their strategy, we must understand that it is the combination of the goals and milestones, how they may relate to the market and the customers being supported; inclusive

of any number of products and services being offered; the various channels for delivery of those products or services; and the environment in which the enterprise operates in.

A defined strategy ensures that the enterprise runs effectively and efficiently, by:

1. Ensuring that there is a clearly defined direction
2. Alignment and optimization of the operating model needed to achieve the strategy
3. Understanding the risks present
4. Ensure continued alignment between business and IT
5. Monitoring for changes within the operating environment
6. Monitoring progress in both the implementation and execution of the strategy

In order to enable and promote the continued alignment of IT capabilities and investments with those of the business and ensure business risks relating to Information Security are properly captured, conveyed and understood, we've developed this process which is designed to enable maintaining Digital Trust within the defined boundaries and thresholds desired by the enterprise.

The Nine Elements

The Digital Trust Canvas Modeling process considers nine core elements and corresponding sub-elements, which can quickly flesh out and help both the line of business and IT understand the implications of a change or a solution before committing resources to building business cases, attempting to capture and define requirements, or conducting costly feasibility studies.

1. **Business Unit(s)** – Which business unit(s) are requesting (R2L) the initiative or will be impacted (L2R) by the initiative? What are the lines of business are you supporting? What is their role in the enterprise's overall strategy?
2. **Business Driver(s)** – What is behind the initiative being proposed?
3. **Business Value(s) & Benefit(s)** – What is expected to be gained? What is the gain that will be provided by implementing the initiative? What need are you satisfying by delivering this initiative?
4. **Financials** – What investments will need to be made and what risks may exist that may influence the outcome?
5. **Business Enablement & IT Alignment** – How will the initiative further enable the business? Does the initiative align with the goals and objectives of the business?
6. **Enterprise Information Security Alignment** – How will the initiative influence the various dimensions of information security?
7. **Key Activities** – What are some of the key activities that will need to be performed as part of the initiative?
8. **Resources Required** – What are some of the key resources which would be needed to ensure success of the initiative?
9. **Culture** – What elements of the enterprise ethos could be impacted or need to adapt/modify to ensure success of the initiative?

The Model

The left-hand side of the model considers elements affecting various elements of IT Operations and the right side of the model considers the business unit.

Culture – This element is comprised of not only the tone from the top, but also must consider the sub-elements of people, processes and technologies within the environment, those aspects that enable the success of Digital Trust.

Framework Components:

- Ethics
- Non-invasive practices

People – How will the initiative affect customers, stakeholders, and users? Will users need to be trained? Will skills need to be assessed? Will new staff be required? Will we gain additional customers? Will stakeholder confidence be increased?

Framework Components:

- Education & Training
- Security Measures
- Compliance & Accountability

Processes – How will the initiative affect existing processes? Will updates need to be made? New processes designed and implemented?

Framework Components:

- Privacy Protection
- Compliance & Accountability

Supporting functions:

- *Security Operations*

Technology – How will the initiative affect existing technology? Will hardware/software be needed or retired? Are changes required? Are any secondary or ancillary systems impacted by the initiative? Is a configuration change required?

Framework Components:

- Security Measures
- Privacy Protection
- Compliance & Accountability

Key Activities – At a high-level, what key activities are required for the initiative? This may include, but not limited to, activities such as:

- Architectural review and approval,
- Conducting research,
- Change request submission and approval,
- Detailed project planning,
- Developing a proof of concept,
- Gathering requirements,
- Performing cost-benefit analysis,
- Performing site surveys, or
- System security testing.

Framework Components:
Regular Auditing & Reporting
Education & Training

Resources Required – At a high-level, what resources are required for the initiative? This may include, but not limited to, resources such as:

- Application Developers
- Audit & Assurance Department
- Database Administrators
- Enterprise Security Architect
- General/External Legal Counsel
- Network engineers
- Product Owners
- Risk/Control Owner
- Security Operations
- Solutions Architect
- Systems Administrators
- Third-Party Provider

Framework Components:
Security Measures
Privacy Protection
Compliance & Accountability

Supporting functions:
Third-parties

Enterprise Information Security Alignment – This is how an initiative may impact or otherwise influence the Enterprise's Information Security posture. It is inclusive of nine sub-elements listed as follows:

Confidentiality – Ensuring the preservation of authorized restrictions and permissions on the access and disclosure, including the means for protecting data and information.

Framework Components:
Security Measures
Privacy Protection

Integrity – Ensuring the proper fidelity of data and information; protecting against improper modification or destruction, to include ensuring the nonrepudiation and authenticity of data and information.

Framework Components:
- Ethical Behavior
- Security Measures

Availability – Ensuring timely and reliable appropriate access to and use of data and information.

Framework Components:
- Security Measures
- Compliance & Accountability

Privacy – Ensuring the rights of an individual who has entrusted to the enterprise will appropriately and respectfully use, store, share and dispose of their personal and sensitive information within the context, and according to the purposes for which it was collected or derived.

Framework Components:
- Privacy Protection
- Non-invasive Practices

Compliance – Ensuring the ability to show the enterprises adherence to statutory and regulatory requirements, as well as voluntary requirements arising from contractual obligations and internally defined policies.

Framework Components:
- Ethics
- Compliance & Accountability

Supporting functions:
- Operations

Audit – Ensuring the ability to reliably and confidently undergo the formal inspection and verification to determine the level of completeness a defined standard is being followed, that evidence accurately reflects the environment, or efficiency and effectiveness targets are consistently being met.

Framework Components:
- Regular Auditing & Reporting

Environmental – Ensuring that the area in which the organization operates does not introduce any threats to the existing natural resources, human health or wildlife.

Framework Components:
- Security Measures
- Compliance & Accountability

Social – Ensuring the active and consistent engagement with the community, our customers we serve, the suppliers and vendors we rely on, and our employees; providing the appropriate level of transparency into our operations which demonstrate our commitment to the social fabric.

Framework Components:
- Security Measures
- Privacy Protection

Safety – Ensuring the protection from harm, for both our customers and employees. This is inclusive of logical and physical environments and the convergence of the two.

Framework Components:
- Security Measures
- Privacy Protection

Business Value & Benefit – Will the initiative enable us to achieve our enterprise strategy, goals and objectives? Will the initiative provide sufficient return on investment for lifecycle of the initiative? Will the initiative increase or decrease productivity, brand recognition, competitive advantage, and/or enhance growth potential? Will the initiative increase efficiencies or effectiveness of impacted processes, technologies and/or controls?

From a Digital Trust perspective, we also want to consider the following:

- Brand Loyalty
- Consumer Confidence
- Customer Retention
- Stakeholder Confidence
- Regulatory Approval
- Public Trust

Business Unit(s) – What are the various lines of business that the initiative would impact? These can be primary stakeholders and champions, as well as secondary business units which may be impacted (changing standard operations, processes, or workflows as a result) or benefit from the initiative.

From a Digital Trust perspective, we also want to consider the following:

- Human Resources
- Sales
- Marketing
- eCommerce

Business Driver(s) – Why is the initiative being proposed and considered? What business need is being fulfilled and satisfied by the initiative? Drivers can be internal or external in nature, understanding what is behind the change in operations can arise from any number of areas, such as changes to:

- The enterprise's strategy
- The consumer market
- Credit/Cash flow
- Operating budget
- Operating environment
- Compliance requirements

From a Digital Trust perspective, we want to consider the following:

- Security Measures
- Privacy Protection
- Non-invasive Practices
- Compliance

The bottom row of the model contains four common management elements, from left to right, included:

Enablement – How will initiative further enhance business operations and/or support the delivery on enterprise goals/objectives? The operational enablement for achieving the respective practices areas defined within the Framework.

- Security Managed
- Privacy Protected
- Ethical Behavior
- Non-Invasive Practices
- Compliance & Accountability
- Education & Training
- Regular Audit & Reporting

Alignment – Does the initiative align with our enterprise strategies (Business, IT, Cyber, Digital Trust), goals and target objectives?

Investments – What resources (e.g., time, staff, and budget) is needed for the initiative to be successful? In context of Digital Trust, what component(s) is most likely to require additional investments.

Risks – What are the threats, obstacles and challenges need to account for that may prevent the initiative from being successful? In context of Digital Trust, what outcomes may be experienced that are beyond the defined thresholds, for example costs of non-compliance, penalties/fines associated with privacy violations, or data breach & incident response costs.

Practical Use of the Model

Each element, and supporting sub-element, should be populated with sufficient detail to identify how an initiative may impact the enterprise's Digital Trust posture, whether it's from business, technology or security perspective.

To this end, we will want to look at the model as if it were a blank canvas, with each cell waiting for an index card or post-it note providing the proper attributes or narratives being placed in each cell.

With the appropriate, knowledgeable subject matter expert representatives from the business, information technology and security providing sufficient detail regarding their respective sections for each of the cells.

The Canvas Model should facilitate the initial conversations and engagement, with the ability to rationalize the information provided by both parties to ensure that sufficient details are collected which fairly and accurate represent the Business and Information Technology positions.

This practical use of the model can be used from either being initiated by the Business (that is moving from right to left within the model), providing the high-level narrative of what needs to be accomplished and capturing sufficient details as to how that translates into the various elements of Information Technology to allow proper planning, budgeting, resource allocation and alignment with the enterprise strategy.

Conversely, when initiated by Information Technology (moving left to right across the model), the narrative outlines and captures how an initiative will impact, across multiple elements, the organization. This is to allow for proper planning and execution by Information Technology, while ensuring that the relevant business stakeholders are kept informed and to prevent a condition which may expose the enterprise to unnecessary risk or exposure.

Regardless of where an initiative originates, the centerline element of the enterprise's overall Digital Security posture is captured. Sufficient information provided by both the Business and Information Technology groups is reviewed, with the impacts to the core security posture of the enterprise being identifying. This should then allow the initiative's stakeholder(s) to make well informed decisions around the initiative and plan accordingly, understanding the potential impacts faced by the enterprise.

Business Unit Representatives

Authoritative business representatives should be engaged to complete the right side of the model. These can be those stakeholders who can speak on behalf of the business and who have identified a need or gap within the enterprise which needs to be addressed.

1. Starting in the top right corner of the model with the **Business Unit(s)** cell, capture the business unit who is proposing and considering the initiative. Additionally identify any downstream or upstream secondary's business units who are either impacted or will benefit from the initiative.

2. Moving down one cell to the **Business Driver(s)** cell, capture what is driving this initiative. Is it to meet customer needs, comply with regulatory or contractual requirements, or reduce risks to the enterprise?

3. Next move to the left into the **Business Value and Benefit** cell, have the business define what they perceive as the value to be gained and what benefits need to be realized in order for the initiative to be considered a success.

4. Moving down to the **Financials** element to the *Investments* cell, have the business identify what investments they are willing to make (e.g., time, staff, budget) to successfully complete the initiative.

5. Moving right within the **Financials** element to the *Risks* cell, have the business identify what their perceived risks which might result by NOT undertaking this initiative. For example, the business unit may view not successfully completing the initiative to result in not achieving their goals or objectives, missing a market opportunity, impaired growth, diminished brand reputation, fines and/or penalties.

6. Moving left into in the bottom left hand corner of the model is the **Business Support** cell, starting with the *Enablement* cell, identify and capture what the business believes the initiative will provide to their customers, their users and ultimately their business unit. Enablement is something (tangible or intangible) that will assists in realization of their goals and objectives. Examples of enablers are provided in the Appendix.

7. Finally moving right into the *Alignment* cell, we will identify how the initiative aligns with the defined goals and objectives of the business unit. This can be best summarized by asking "What will this initiative provide back to the business?" Examples are listed in the Appendix.

IT Subject Matter Experts

Information Technology Subject Matter Experts (SMEs) should be engaged to complete the left side of the model ("**Operations**"). These are those SME's who are familiar and can provide sufficient information on what activities, resources and culture changes are needed and the subsequent impacts the initiative will have in order to successfully deliver the initiative to the enterprise.

1. Starting in the top left corner of the model with the **Culture** cells, capture how the initiative may impact the following sub-elements, consider the following questions:
    a. Starting in the ***People*** cell, capture people who will be impacted by and benefit from this initiative. Does this impact IT only, a department or the entire enterprise? Will this make the customer experience better or degrade it? Will additional resources be needed to staff the initiative? What skills or training are required for this initiative? Will the initiative impact the entire enterprise or just a single business unit?
    b. Next move down to the ***Process*** cell, identify and capture what process may be impacted or required to be created or revised as a result of the initiative. Will the initiative require changes to existing process? Will new processes need to be created? Will the initiative impact processes upstream or downstream?
    c. Finally move down to the ***Technology*** cell, identify and document what the primary and supporting technologies that are required for the initiative to succeed. These could be uplift and replacement firewalls from the same vendor to a complete transition from one cloud service provider to another. Understand and document the major and supporting system components are such as: network engineering, data storage, identity & access management, account provisioning.

2. Upon completing the sub-elements, you will need to consider those sub-elements in context of the relationship between enterprise culture and desired Digital Trust posture.

3. Moving right to the **Key Activities** cell, identify what the key activities that must be performed to ensure the success of the initiative. These can be anything from developing a formal project plan, submitting a change request, gathering system requirements or securing commitment for funding.

4. Next, move down to the **Resources Required** cell, identify and capture what resources are required to ensure success of the initiative. This could be the need for specific team members, commodity or specialized hardware, increase in application licensing, approval from the business architecture team. Is technology going to be acquired from a supplier or does it need to be internally developed?

5. Moving down to the **Business Support** cell, complete the two sub-element cells:
    a. Starting in the *Enablement* cell, identify and capture how this initiative will improve business operations and allow the business unit to meet their objectives. Additionally, document how the initiative may impact the IT department's ability to meet their target objectives.

    b. Moving to the right, into the *Alignment* cell, identify and capture how this initiative will align with the business' goals, as well as documenting if the initiative aligns with the goals established for the IT department.

Information/Cyber Security Professional

While the Information Security Professional should be engaged throughout this process, it rests with the InfoSec Professional to complete the centerline of the model, specifically the **Enterprise Security Alignment ("Security")** cells.

Review the details provided by both the Business Representatives and Information Technology SMEs, once sufficient information have been provided, and identify shifts in the respective Information Security areas.

1. *Confidentiality* – How will the initiative affect confidentiality of sensitive or regulated data and information? Will the initiative unintentionally expose data or arbitrarily restrict existing access to data and information?

2. *Integrity* – How will the initiative affect sensitive or regulated data and information? Will the initiative inadvertently change the fidelity or quality of data or information needed by the enterprise?

3. *Availability* – Will the initiative affect authorized accessibility to systems, data or information; will the initiative interrupt business transactions or operations? Will the initiative increase or diminish accessibility? Will the initiative increase or decrease capacity requirements? Will systems, data and information be obtainable to authorized and approved consumers of those systems, data and information? Will the initiative require an outage?

4. *Privacy* – Will the initiative expose or restrict access to customer data and information? Will privacy be modified, enhanced, or diminished in any way?

5. *Compliance* – Will the initiative have any impact on our existing compliance obligations? Will the initiative address outstanding compliance concerns? Does the initiative create compliance issues or gaps?

6. *Audit* – Will the initiative change, improve or diminish our ability to sufficiently evidence audit requirements?

7. *Environmental* – Will the initiative demonstrate our commitment to safeguard the environments in which we operate in? Will the initiative require we file any exceptions to our current environmental policies? Will the initiative enhance, obscure or reduce transparency of our compliance with environmental regulations?

8. *Social* – Will the initiative improve or degrade our reputation and image with the local community? Will the initiative improve or degrade our relationships with our employees, suppliers, customers and the communities where we operate in? Will the initiative enhance the local community? Will the initiative demonstrate and promote our positive ethics?

9. *Safety* – Will the initiative increase or decrease safety measures designed to protect and safeguard our customers and employees?

Appendix

General Business Values & Benefits

- Agility
- Avoid fines and penalties
- Better informed risk decisions and risk awareness
- Better integration of information security across the enterprise
- Better management and optimization of costs related to information security
- Better support for innovation and competitiveness
- Better understanding of information security by stakeholders
- Brand Image
- Brand Recognition
- Business Resilience
- Compliance
- Corporate Culture
- Cost Avoidance
- Cost Reduction
- Creative Output
- Customer Attrition (Reduction)
- Customer Engagement
- Customer Experience
- Customer Relationships
- Customer Satisfaction
- Customer satisfaction
- Diversification of Revenue
- Employee Engagement
- Employee Retention
- Employee satisfaction
- Enhance data management capabilities
- Higher stakeholder satisfaction with information security outcomes
- Improve growth opportunity
- Improvements in prevention, detection and recovery
- Issue/Problem Resolution
- Market Penetration
- Market Share
- Overhead Cost (Reduction)
- Process Efficiency
- Product Quality
- Productivity
- Protect business reputation
- Reduced risk
- Reduction of complexity and increased cost-effectiveness through improved and easier integration and alignment of information security standards, good practices and/or sector-specific guidelines
- Reduction (*in terms of both impact and probability*) of information security incidents
- Reputation
- Return on Investment
- Revenue
- Revenue Per Employee
- Risk Avoidance
- Risk Reduction
- Sales Volume
- Service Quality
- Social Responsibility
- Stakeholder Relationships
- Sustainability
- Talent/Competencies
- Tax Efficiency
- Technology integration
- Time to Market
- Unit Cost Reduction
- Work Quality
- Work Throughput

Example Enablers:

- Applications
- Behavior
- Budget
- Capabilities
- Consultants
- Contractors
- Culture
- Ethics
- Frameworks
- Information
- Infrastructure – Facilities
- Infrastructure – IT
- Organizational structure
- People (individuals)
- People (staff level)
- Policies
- Principles
- Procedures
- Processes
- Service Providers
- Services
- Staff competencies
- Staff skills
- Standards

Example Alignment Statements

- Agility to turn business requirements into operational solutions
- Competent and motivated staff with mutual understanding of technology and business
- Compliance and support for compliance with external laws and regulations
- Compliance with internal policies
- Delivering programs on time, on budget and meeting requirements and quality standards
- Delivery of services in line with business requirements
- Enabling and supporting key business functions using appropriate technology
- Knowledge, expertise and initiatives for business innovation
- Manage risks
- Quality of financial information
- Quality of management information
- Realize benefits from investments and services portfolio
- Security of information, processing infrastructure and applications, and privacy