The DNA of Digital Trust: Data Protection and Privacy for the Intelligent Enterprise
Table of Contents

3 Data Security: Enabling Digital Trust – And Future Growth

4 Building Defenses for the Intelligent Enterprise

5 Seeking Help from Outside Experts

6 How SAP Can Help

About the Authors

Bruce Romney, Senior Director,
SAP SE
bruce.romney@sap.com | +1 972-408-7331

Bruce Romney is a senior director at SAP leading governance, risk, and compliance (GRC) and security global product marketing. He shares the vision and capabilities from SAP regarding GRC, security innovations, and transformational opportunities, especially as they relate to SAP S/4HANA®. Bruce has more than 15 years of experience in supporting clients with their SAP® offerings and other risk and compliance engagements and consulting initiatives.

Dr. Sandro Lovisa, Product Manager/Owner,
SAP SE
sandro.lovisa@sap.com | +49 6227 7-43070

Sandro Lovisa has more than 23 years of experience with SAP and has been part of the GRC product and development unit at SAP since its inception. In his role as product lead for the SAP Privacy Governance application, he currently concentrates on the various GRC aspects of privacy and data protection.

Ben Zimmerman, Principal,
Ernst & Young LLP
benjiman.zimmerman@ey.com | +1 612-341-4746

Ben Zimmerman is a principal in the advisory services practice of Ernst & Young LLP and a global agile business risk leader. He supports risk innovation and transformation efforts, focusing and leading risk transformation services for SAP in the Americas. Ben has more than 20 years of experience in supporting clients’ SAP offerings and digitally enhanced transformations. His experience includes strategy, organization development, project advising, quality assessment, project management, and risk analytics design and implementation. From an industry perspective, Ben has focused, over the last 10 years, in automotive and transportation, oil and gas, and technology.

Pavi Malhotra, Managing Director,
Ernst & Young LLP
pavi.malhotra@ey.com | +1 732-516-4468

Pavi Malhotra is a managing director in the advisory services practice of Ernst & Young LLP. He has more than 18 years of professional services experience helping large global companies transform their finance and risk functions to better manage and control risks across the enterprise. He possesses a well-integrated knowledge of business control automation and analytics as companies evolve into digital enterprises. His recent experience centers on digital co-innovation, leveraging SAP S/4HANA and SAP GRC solutions to solve business problems and supporting companies as they navigate complex changes to privacy regulation (such as GDPR, CCPA, and others).
Data Security: Enabling Digital Trust – And Future Growth

Data and connectivity are the enablers of the digital economy. Whether you are hiring, acquiring, manufacturing, selling, or building partnerships and ecosystems, information is being shared, stored, processed, and consumed. As everyone and everything become more connected, the ability to build and maintain digital trust around data becomes a key competitive differentiator. The question is, how trustworthy is your enterprise?

Digital trust means that your stakeholders are confident in how your company governs the use, monetization, and sharing of data – and that it does so without compromising on security, management, or compliance. They know you’ve built strong data security into the DNA of your systems and processes – especially around your most sensitive data, such as customer personal information, employee data, finance, and high-value intellectual property – and operate with a clear code of ethical conduct around it. And they see that you continuously test and optimize your security and risk management to protect against new threats, even as you innovate new, digitally enabled products and services.

Digital trust is hard to build and easily lost following a single data breach, report of unethical data use, or negative customer experience. And once this happens, you can quickly lose the loyalty of customers, partners, and suppliers as well as suffer irreparable brand and financial ramifications. The fact is, if your organization’s talk about data security is not matched by the right actions, it’s just a matter of time before a breach occurs. Cyber threats are evolving, intensifying, and increasingly successful at reaching sensitive data even at seemingly security-hardened companies. Breaches are also yielding increasingly larger volumes of sensitive data. At the same time, expectations of stakeholders and regulators regarding data security have changed drastically in recent years. The focus has shifted from the protection of financial accounts and identities (so they can’t be used to gain access to company assets and data) to the prevention of personal data breaches and unethical exploitation of this information.

So, is your organization’s approach to data security strong enough to build and sustain digital trust?
TRANSFORMING YOUR RISK LENS FOR FASTER, MORE COMPREHENSIVE RISK INTELLIGENCE

In today’s threat-intensive environment, earning digital trust – especially around sensitive data – is no small feat. Companies are undergoing rapid technology changes, innovating faster to meet new customer expectations (often through closer collaboration with new partners and ecosystems), and dealing with external factors such as intensifying global regulatory requirements, geopolitics, and trade. Rapid changes in these areas are bringing new challenges, risks, and threats to businesses, especially on the data security front.

Let’s take a closer look at why.

Expanding Government Regulations

Governments around the world are implementing regulations, many of which shift the focus of data privacy from the enterprise to the customer. These laws are bringing new standards, clear accountability, fines as high as 4% of revenues for breaches, and unprecedented consumer visibility and control over their personal data. Consider the EU General Data Protection Regulation (GDPR), which gives data subjects increased protection of and direct control over their personal data, including the right to access, correct, object to or limit processing, erase, and request an export of their personal data from companies. Companies (also referred to as “controllers and processors”) have vastly increased responsibilities around data protection and privacy, including systems, policies, processes, and personnel. Other countries around the world are following suit with similar laws. And the California Consumer Privacy Act (CCPA) is the first of many state laws that provide consumers with more control over their personal information and how it is collected, used, stored, and transferred by companies.

The challenge, of course, will be implementing current and future data privacy requirements across your entire personal data lifecycle to confirm compliance. At the highest level, this will require:

• A unified and integrated approach to tailoring leading practices of data privacy management to your unique company needs
• Solutions that reduce the cost, complexity, time, and resources required to comply with changing privacy demands and regulations
• Centralized visibility into the location and use of customer and employee data
• An integrated request management and data fulfillment lifecycle
• Automated production and maintenance of processing activity documentation
• An easy-to-use interface for auditors, and data subjects who request their rights (for example, under GDPR, the right to be sent a copy of all personal data a company has about them or to delete their data)
• Efficient, scalable, and accurate privacy policy operations and compliance management
• The ability to initiate and flow Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs)
Cloud Adoption
Moving data to the cloud adds a new layer of network complexity and increased exposure to threats such as misconfigured environments. While the cloud gives your business flexibility and unprecedented scale, it also broadens your organization’s attack surface, which increases risk and creates more data management and security work. Your risk lens must extend to the cloud now, as you need transparency and control of data in the cloud, as well as the ability to comply with geolocation requirements and considerations. In addition, critical data in the cloud must be inventoried, classified, prioritized, protected, and managed to confirm digital trust and compliance with complex regulations. This work requires skilled resources and a new set of tools optimized for the cloud.

Digital Transformation
Cloud adoption is often part of larger digital transformation initiatives, which enable the connectivity you need to become an agile, intelligent enterprise. But remember that the more your business depends on digital connections among people, partners, suppliers, and assets, the more data your business is collecting, storing, sharing, and moving. This makes it critical that the right data security be embedded into the very core of every digital transformation initiative. Simply “lifting and shifting” old approaches or trying to bolt security on after the fact will inadvertently lead to easily exploited gaps in data security.

Digital transformation requires security to be smarter, automated, and embedded. This means:

- **Security role design and governance** must be considered early on to minimize cross-system risk and insider threats
- **Interconnected systems and applications** must be monitored and maintained to minimize vulnerabilities and protect against data loss
- **Manual controls and checks** must be replaced with smarter, artificial intelligence–driven controls to identify anomalies and potential issues early on
- **Digital automation** must be implemented to provide more reliable and effective monitoring of transactions and processes as human intervention is minimized
Building Defenses for the Intelligent Enterprise

In light of these trends, how will you transform your risk lens to build digital trust? As explored in this paper, it requires embedding trust as a design principle into your entire business – and building digitalized, real-time risk intelligence into every product, service, and digital transformation initiative. Optimized, embedded risk processes and systems can provide faster, earlier risk intelligence, which in turn enables both better data protection and risk-informed business decisions.

Ernst & Young LLP (EY) refers to this approach to security as “trust by design,” which supports a risk optimization mind-set across the enterprise. Risk becomes less about avoidance and more about harnessing risk insights to make growth-oriented, strategic decisions about how to innovate new products and services and enter new markets to drive growth and business value – all while maintaining stakeholder trust. Protecting data is central, especially for the “crown jewels” of the enterprise such as customer and sensitive business data. You need to do so in a way that ensures key business decisions are not based solely on fear but also on real-time insights that help you navigate through risks with confidence – even when competitors can’t.

To get started, EY subject-matter resources and SAP professionals suggest you begin with the basics, which include:

- Inventorying, classifying, and prioritizing data
- Understanding how you collect, use, and share customer personal information
- Clarifying management responsibility for data security across the organization
- Protecting enterprise applications
- Making your defense approach sustainable
INVENTORYING, CLASSIFYING, AND PRIORITIZING YOUR DATA

As information security resources and funding are spread thin across a vast digital footprint, your data security approach needs to focus on protecting the data that matters most. This requires a detailed data inventory and classification of your sensitive data – for example, based on:

- What data sets are sensitive and to whom
- Which types of information would cause the most harm, if exposed
- Which data sets must be protected per regulatory requirements
- What could go wrong if the data were exposed
- Which customers, suppliers, or partners would be damaged if a breach occurred
- Who is most interested in acquiring this data and why

Carrying out a comprehensive data inventory helps you identify the data that matters most, which typically falls into three categories:

- Data that, if breached, would cause reputation damage, negatively impacting the brand, consumer and investor confidence, employee recruiting and retention, and key counterparty relationships
- Data that, if breached, would result in a compliance risk such as fines, loss of credibility with regulators, and industry ramifications
- Data that, if breached, would result in strategic business ramifications such as lost competitiveness, impaired strategy execution, significant business disruption, and loss of confidence among customers, investors, and partners

Based on this information, you can make data-driven decisions about where to prioritize data security investments.

New data is being created, captured, and stored continuously. To effectively protect it, you need a data inventory process that supports **consistent, sustainable data identification and classification** – whether it’s at rest, in use, or in motion.
UNDERSTANDING HOW YOU COLLECT, USE, AND SHARE CUSTOMER PERSONAL DATA
While understanding your sensitive data broadly is critical in prioritizing your resources, personal data for consumers carries special requirements that are rapidly evolving. Consumers’ expectations for transparency about how their data is used are increasing rapidly as a result of frequent breach reports in the news and expanding government privacy regulations. It is critical for consumer-facing organizations to mature their own understanding of how they use and share consumer data, particularly around:
• Why data is collected (for example, personally identifiable information, financial data, and health data)
• How consumers expect information will be used (for instance, whether it can be used to make hiring or credit decisions at a bank)
• Other purposes for which data is used
• Who data is shared with and for what purpose (for example, with other departments in your business or externally with partners)
• How data is protected within the enterprise and at third-party processors
• How long data can and should be retained to meet the needs of the organization and the privacy rights of the consumer

As a first step, organizations must understand the footprint of consumer personal information within the enterprise. This helps to scope and prioritize both operational privacy processes and protection efforts. It is imperative that consumer data is protected as strenuously as possible to protect both the consumers’ data and the reputation of the organization.
DEFINING CLEAR MANAGEMENT RESPONSIBILITY

Central to providing effective data security across the enterprise is defining clear roles and responsibilities at all levels of your organization. SAP recommends designing and implementing a three-level data security framework that is overseen by your executive management and board, which approves the overarching data security and privacy framework, leverages risk and privacy insights when making decisions, and evaluates business units on a risk-adjusted basis.

Under this oversight layer are three lines of defense:

- **First line – risk-taking business units**: Leaders of business units own data security risks. They oversee data management and privacy processes, identify and mitigate risk, design and implement controls, define technology requirements to protect data, set employee permissions, and execute day-to-day compliance tasks such as managing opt-in and opt-out consumer notices.

- **Second line – risk and compliance functions**: These leaders provide oversight and monitoring of risk and compliance activities across the enterprise, starting by designing and deploying the company’s overall data and privacy management framework, including governance and accountability. They monitor and test business unit compliance with policies and government regulations, compile exposures, escalate risk and control issues, and more.

- **Third line – internal or external audit function**: This function provides independent testing and verification of data and privacy security effectiveness within lines of business, validates the overall security framework, and identifies opportunities for continuous improvement.

The right technology can help by supporting an overall governance process for managing these various lines of defense.
PROTECTING THE ENTERPRISE
The advent of the digital age has brought tremendous opportunity for growth and innovation along with many difficult challenges. Many organizations are struggling to keep pace with the data protection implications associated with this business change and have become subject to increasing data-protection and privacy-related regulations.

To start, you need secure products – software with security built in from the bottom up that reflects the latest research on threats and vulnerabilities. SAP developers, for example, follow a mandatory secure software development lifecycle methodology that’s ISO 27034 compliant, so it covers all aspects of product security and links with operational security from the earliest design phases. And we perform validation tests – run from the customer perspective – to check for vulnerabilities and collect information on data protection and privacy.

You also need defendable applications – software with the ability to identify and prevent attacks from within the application itself. Runtime application self-protection, or RASP, technology, for example, can be built into applications, addressing security layers beyond the network perimeter and end-point security.

Protecting your enterprise also requires the ability to transmit, store, and process data while providing complete confidentiality. At SAP, we call this objective “zero knowledge.” So even when hackers gain access to infrastructures and systems, they run into structural, restricted access to data through principles such as encryption for data in transit, customer-managed keyword systems, homomorphic encryption for products and services, tokenization, and anonymization.

In addition, with more partners and suppliers plugging into supply chain systems from SAP – and you engaging with industry ecosystems – you also need a security-shielded ecosystem. This means aligning with partners and suppliers around security, exchanging security expectations, enforcing policy compliance, and facilitating a holistic approach to security up and down your supply chain and ecosystems. You also need to maintain an up-to-date inventory of services provided by third parties (especially cloud service providers), periodic security reviews, and use of free and open source security software all parties can agree to use. In addition, you will likely need more stringent controls and security for all communications and data sharing, training, threat simulations, and contractual updates.

Paramount for any organization is establishing trust with customers, partners, and employees by securing and protecting personal data. As noted earlier, not only is personally identifiable information a target for hackers, but complex regulations across the globe define the governance and management processes needed to protect and manage this data, as well as comply with these regulations. So, you need systems and processes that can support, document, and enable compliance.
To secure the growing numbers of devices and end points used by your mobile workforce, you also need a perceptive data shield, which can support application virtualization, microvirtualization, and zero-day protection or comprehensive endpoint protection. Next-gen cloud firewalls and domain name service–based malware can complement network protection.

In addition, you need to create a **security-first culture** that encompasses all employees, contractors, guests, customers, and partners. This involves training all employees and associates to increase security awareness and empowering them to respond to, resolve, and escalate potential threats – whether it’s a well-crafted phishing e-mail or socially engineered phone conversation – before it’s too late.

Finally, you need a way to manage the constant changes impacting data security and privacy. Your business and technology are constantly changing, as are regulations around data, so you need **privacy by design** built into the design, deployment, testing, and ongoing maintenance of your solutions and the processes they support. For example, you build safeguards for data into solutions from the start, alerts when security risks may be an issue, and application lifecycles that include data privacy reassessments.

**MAKING YOUR DEFENSE APPROACH SUSTAINABLE**

Given the constant changes impacting data security and privacy, it’s essential that your approach to data security be agile and sustainable – in other words, able to respond to change and be executed consistently. This requires alignment around people, processes, and technology.

**People**

Every new control and process requires downstream operational execution or oversight by people. Unless your people are educated about new threats, trained on how to respond to them, and held accountable for security failures, they will inadvertently be weak links in your enterprise firewall. Hence, adequate training and procedures for handling data with their obligations is critical to sustaining continuous compliance.

**Processes**

Every process must have trust by design built into it. Trust is now the competitive differentiator in this complex and evolving landscape. To embed a sustainable data security model, your organization must instill a risk mind-set and culture across the business, as well as embed security into both new product and services design and operations. This approach accelerates speed to market while sustaining trust.

**Technology**

Technology undergirds secure people and processes. Any shift in your IT infrastructure must be looked at from a risk perspective to determine whether it will create a new gap in your data security framework. Additionally, as privacy requirements related to data subject rights management increase the need for automation, you will need new technology that’s built for sustainable operations. Given the complexity of data protection, this will require an architectural strategy that controls the distribution of protected data inbound, outbound, and across your organization. This strategy must then be translated into a comprehensive data security framework that reflects a deep understanding of your IT environment, data assets, and data processing applications. To enable sustainable security compliance, you should consider employing tools that automate security compliance operations on an enterprise scale.
Seeking Help from Outside Experts

So how will you build trust by design into your organization?

Achieving and sustaining trust by design is a huge endeavor – and an increasingly complex one. That’s why so many organizations choose to engage third parties such as EY that can support the process at critical points and provide insights and recommendations that enable sustainable success. For example, consider the following EY services designed to support critical steps in your organization’s journey.

ASSESSING YOUR CURRENT SECURITY PROFILE

EY Cyber Risk Management services can help your organization tackle the many security challenges it faces on a day-to-day basis – including supporting risk-based decisions and improved cybersecurity, reducing costs related to managing security risk, and improving your company’s overall cybersecurity posture.

To manage cyber risk and enable business outcomes, your organization needs to conduct regular qualitative and quantitative data-driven cyber program assessments to better understand the effectiveness of its capabilities from a people, process, and technology perspective. These assessments provide an objective understanding based on an analysis of how information security shapes and fits into your overall risk management structure and enables business objectives.

By performing routine assessments, you can:
• Maintain a pulse on your risk exposure
• Assess the maturity of your current cybersecurity program and identify areas for improvement
• Develop a prioritized road map for project investments and organizational change initiatives
• Compare your business with other organizations
• Validate whether security investments have improved your security posture
CAPTURING THE UPSIDE OF RISK WHILE MANAGING DOWNSIDE RISK

Most current risk programs are reactive, meaning they are designed to manage and prevent downside risks, such as having sensitive data stolen. When you build trust by design, you can adopt a security approach that digitalizes risk intelligence so you can also balance upside risk (what must go right, such as the potential for innovative ideas to grow consumer bases), downside risk (what could go wrong, such as regulatory noncompliance), and outside risk (what could surprise you, such as geopolitical risk and megatrends). This allows you to confidently embrace disruption, seize new opportunities, and expand into unpredictable markets – all while managing negative outcomes and building stakeholder trust.

The key to capturing upside risk is to transform digital data into corporate value – including consumer data – in a compliant way while managing the potential downside risks of holding that data. This is the key to smarter business decisions that help you navigate through risk to capture upside. For example, providing upside risk insights to operations and product teams will inform your organization’s strategy. Integration into the first line of defense (the risk-taking business units) will be critical; this enables you to create a nimble, efficient risk operations model that keeps pace with the business landscape while maintaining strong risk oversight.

Simultaneously, of course, your business needs to manage downside risks such as fraud, compliance failures, brand and stock value damage, and fines. EY services are available to help you identify high-value information assets, protect the data that matters most, and comply with data privacy regulations.

EY services can help you capture upside risk by helping you:
- Evaluate risks across multiple dimensions to monitor what must go right (upside risk), what could go wrong (downside risk), and what could surprise you (outside risk)
- Embed risk into the agile development lifecycle to design and sustain trust along the customer journey
- Digitalize risk intelligence to enable predictive and real-time reporting to drive agile decision-making – from the executive board to line managers – that’s aligned with your strategic priorities so everyone focuses on what matters most
- Transform your organization to design a business and risk strategy that is more customer centric and relationship driven
ASSESSING YOUR RESILIENCE TO THREATS
Even after your organization has implemented a data security program, your work is not done. Threats are constantly evolving and becoming more sophisticated. That’s why EY provides services that help you continuously assess your organization’s resilience to threats on the data front. For example, EY teams offer:

• Cyber simulations – which are realistic cyber-security incident scenarios that challenge your business, operations, and decision-making processes. This is critical today, as regulators worldwide increasingly expect organizations to test their cyber resilience through crisis management exercises as part of basic corporate risk management. Rehearsing through cyber simulation exercises is the best way to achieve this. We work closely with you to plan, design, and execute a realistic incident scenario and simulation, assess how your response teams react, and provide feedback and summarize findings in a report.

• Isolated recoveries – which address extreme data destruction incidents for which traditional methodology may not be sufficient. EY secures point-in-time copies of vital enterprise data in a vaulted environment that is typically isolated from the main production network. The vault is connected to the production environment on a periodic basis, through restricted connections.
How SAP Can Help

Deploying the right technology in the right places will be critical to securing your data across the enterprise. To this end, SAP can help you:
- Build security into the very foundation of your digital enterprise
- Deliver efficiencies in required regulatory activities
- Enable real-time risk intelligence for the organization so executives have insight, balance, and perspective as they develop and execute strategies

As summarized in Figure 1, SAP® governance, risk, and compliance (GRC) solutions can help you do all this and more across six pillars of cybersecurity and data protection. When all these pillars are aligned, the result is confident, risk-informed decision-making that enables growth, increases business value, and helps you maintain stakeholder trust.

Figure 1: Pillars of Data Security for the Intelligent Enterprise

<table>
<thead>
<tr>
<th>Cyber risk and governance</th>
<th>Application security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity and access management</td>
<td>Data protection and privacy</td>
</tr>
<tr>
<td>Cloud transparency and control</td>
<td>Continuous insight</td>
</tr>
</tbody>
</table>
**CYBER RISK AND GOVERNANCE**

SAP solutions for cybersecurity and data protection help you manage risk and provide governance for your compliance processes by identifying and managing risks, regulations, and policies to minimize potential business impact. SAP offerings such as the SAP Risk Management, SAP Privacy Governance, and SAP Process Control applications enable you to:

- Document and monitor security risks and regulatory compliance as part of the enterprise risk management program
- Align risk management and controls with business objectives and security best practices
- Establish security policies and test adherence and understanding
- Document and test a response and recovery plan
- Audit the security program to provide independent assurance
- Report and manage at the board level to ensure awareness and status

**APPLICATION SECURITY**

SAP GRC solutions are designed to help secure the core applications that run your business. This includes helping you identify risks and vulnerabilities within your applications so you can deploy the right security technologies – including free security features and capabilities that SAP builds into each application. Together, SAP offerings such as the SAP Enterprise Threat Detection application, the SAP Business Integrity Screening application, and the SAP Code Vulnerability Analyzer tool enable you to:

- Monitor business applications for anomalies and attacks
- Analyze business transactions for fraud and unusual activity
- Correlate insights from security and business alerts
- Apply security patches and updates
- Focus on custom code and find and fix vulnerabilities
- Continuously monitor critical security configuration

**IDENTITY AND ACCESS MANAGEMENT**

SAP GRC solutions are designed to help you optimize digital identities across the enterprise. This includes enabling identity and access management to manage system accounts and provide the correct authorization assignments. Using offerings such as the SAP Access Control application, the SAP Identity Management component, the SAP Single Sign-On application, SAP Cloud Identity Access Governance software, the SAP Access Violation Management application by Greenlight, and the SAP Dynamic Authorization Management application by NextLabs, you can:

- Reduce costs and improve security with identity management and automated provisioning
- Manage access for enterprise applications – in the cloud or on premise – with role- and attribute-based controls
- Enable greater user productivity by eliminating excessive logins with single sign-on
- Reduce audit costs by quantifying the financial impact of access risk violations
- Support superuser account access with monitoring and integrated log review workflow
DATA PROTECTION AND PRIVACY
SAP GRC solutions are designed to help protect your company's reputation and intellectual property and improve compliance and reporting for specific regulations. This includes addressing data protection and privacy concerns and regulations. For example, solutions such as the SAP Privacy Governance application, the SAP Enterprise Digital Rights Management application by NextLabs, the UI data protection masking package, SAP Customer Data Cloud solutions from Gigya, and the SAP Privacy Management application by BigID help you:

• Secure files and data using transportable policies and encryption
• Add layers of granularity for access decisions based on a variety of attributes
• Enable data masking in sensitive data fields
• Manage personal and sensitive data across landscapes and geographies
• Manage customer consent, preferences, and rights requests
• Use logging features (in case of potential breach) to identify and stop sources of potential data leaks
• Decrease the probability and magnitude of data leaks

These solutions support granular data management capabilities needed to comply with regulations such as GDPR – and give employees a single point of entry for handling privacy matters. For example, when you deploy SAP Privacy Governance with SAP Privacy Management by BigID, users can:

• Manage records of data protection- and privacy-relevant processes using questionnaires that are auto-delivered to process owners
• Define centralized regulations and requirements using built-in policy management and dissemination functionality
• Monitor daily compliance with policies
• Manage data protection impact assessments for at-risk personal data and flows
• Manage the security business impact analysis within an IT security framework
• Automate compliance, risk, and controls reporting
• Run data subject rights access requests
• Have an accurate, data-driven analysis of data profiles and flows

With these integrated capabilities, your business benefits from:

• Centralized management and documentation of all Record of Data Processing Activities (ROPA), Data Privacy Impact Assessment (DPIA), and Security Breach Information Act (SBIA) activities
• Full transparency into GDPR-relevant process ownership and compliance levels
• Fast, accurate compliance reporting and insights
• Risk-driven data protection and privacy compliance based on real-time data analysis

PUBLIC CLOUD TRANSPARENCY AND CONTROL
SAP GRC solutions are designed to deliver multi-cloud data transparency and control for organizations hosting data in a public cloud. For example, SAP solutions such as the SAP Data Custodian solution help you:

• Create and enforce public-cloud data access, location, movement, and processing policies
• Monitor and report on data access, storage, movement, processing, and location in the public cloud
• Configure public-cloud data location, movement, processing, and access policies
• Enforce geolocation controls for data access, storage, processing, and movement
• Prevent unlawful transfer of business data
CONTINUOUS INSIGHT

Using solutions and services from SAP and EY, you can provide upside risk insights to executives, operations, and product teams to inform strategy. The offerings help you turn risk-related data into real-time insights so you can accelerate innovation and speed to market. For example, SAP Digital Boardroom helps you manage risk from the top down by providing C-level executives one view of risk across all enterprise risks tied to business objectives. And EY Risk Navigator combines the trusted EY risk and controls experience with the industry-leading SAP HANA® Cloud data platform, all in a single tested and supported service.

Figure 2: SAP and EY Solutions and Services Supporting the Five Pillars of Cybersecurity and Data Protection
LEARN MORE
As explored in this paper, paramount for any organization today is establishing digital trust with customers, partners, and employees around how personal and other sensitive data is secured and protected. Not only is data a target for hackers, but there are government and industry regulations around the world defining its governance and management. Failure to comply is not an option.

EY and SAP are complementary collaborators with the products and services to help you achieve sustainable digital trust. Figure 2 summarizes the key offerings of both companies around the six pillars of cybersecurity and data management.

Specifically, SAP offers a best-in-class, integrated portfolio of solutions that helps secure applications and day-to-day interactions – both those inside and outside your organization. These solutions deliver the visibility, control, and insights you need to achieve sustainable compliance, build digital trust, and realize the upside of risk.

Integration of risk insights into the first line of defense – the risk-taking line-of-business units – will also be critical to creating a nimble, efficient risk operations model that keeps pace with the business landscape while maintaining strong risk oversight.

EY consulting services help you build digital trust early into the foundation of digital transformation initiatives. They can assess your current environment in light of the latest regulations, identify gaps, provide recommendations, define a technology road map with SAP products, and help you develop a strategy for capturing the upside of risk. EY professionals’ vast industry experience also means you benefit from leading practices, key learnings from other industries, and more.

To learn more, visit:
- ey.com/trustbydesign
- ey.com/cybersecurity
- sap.com/grc
- sap.com/about/trust-center.html
- sap.com/products/crm/customer-data-management.html

© 2020 SAP SE or an SAP affiliate company. All rights reserved.