



GRC SOLUTION BRIEF

# Enterprise Governance, Risk, and Compliance for PeopleSoft

## Abstract

As data regulations expand in scope and cyber threats become more sophisticated (and aggressive), organizations need to upgrade their security posture to control risk factors and comply with new regulations. Risk management and regulatory compliance are two critical components of an organization's security posture, but if not well established, can lead to devastating data breaches, crippling monetary penalties, legal implications and more. While breaches and cybercrime are at an all-time high, new data privacy regulations like GDPR have introduced stringent mandates on the processing and use of sensitive data.

In case of legacy ERP applications, developing a robust GRC posture can be especially difficult. Out-of-the-box, most legacy ERP systems lack the granular visibility and security controls needed to effectively address compliance requirements and manage risk. To fill these gaps, organizations are left with expensive, time-consuming customizations or must rely on piecing together disparate 3rd party solutions that can prove to be complex and expensive to maintain.

An effective GRC strategy must take a holistic approach to ensure proper policies are implemented, appropriate security controls are used, and that all related components can work in unison to fulfil compliance requirements. In this Solution Brief, we will first cover the fundamental parameters necessary to develop an effective security posture to manage modern threat vectors and navigate complex compliance regulations. In following, we'll explore the GRC challenges unique to PeopleSoft and how Appian Security Platform can enhance security to meet today's compliance requirements.

## The Prerequisites of an Effective Risk Management and Regulatory Compliance Strategy

### Ensure organizational preparedness

- **Maintain Identity-Based Authentication & Authorization Controls** – In today's security environments governed by mobile devices, remote connectivity, and web-facing applications, identity has become the new network perimeter. As opposed to the traditional physical network perimeters, sensitive data is now accessible from anywhere in the world. As a result, **layered identity-based controls** need to be assessed, deployed, and strengthened.

- **Understand Business & Regulatory Drivers** – Every business domain has its unique operating procedures and governing regulations that play a significant role in the decision-making process. Therefore, it is essential that these factors are documented and accounted for before making any additions, upgrades, or eliminations to an enterprise's technology architecture or business processes. Changes must be thoroughly evaluated, as compromises on existing components are likely to increase loopholes in the security posture.
- **Ensure Support & Participation of Appropriate Stakeholders** – Awareness and accountability are of paramount importance. To manage risk, organizations cannot afford to leave out any details that internal teams can provide - including requirements, expectations, historical incidents and more. It is important to include every stakeholder in the decision-making process to reduce the possibility of errors and to ensure technical/functional accountability.

## Manage your data

Before you can effectively manage your data, you need to know where you have it, the volume of data you are handling, and put in place the basic security measures.

- **Discover & Catalog Your Sensitive Data** – To protect data, organizations must first identify and categorize it based on the level of sensitivity, importance, and usage. Adequate classification of data also simplifies reporting and helps in prioritization when routine or compliance audits are requested.
- **Encrypt Sensitive Data-At-Rest & Data-In-Motion** – Sharing data is critical to several business processes. However, whether in storage or as it travels among employees, third-parties, partners, vendors, etc. sensitive data that is susceptible to compromise and misuse must be properly encrypted.



## Improve activity monitoring, tracking, and access control

Gather as many details as you can about how data is used, shared and transferred within your systems and ensure that the integrity of data is maintained throughout its lifecycle, no exceptions!

- **Implement Granular Application & Database Access Controls & Monitoring** – Traditional logging is not enough to fulfill today's complex threat detection and regulatory requirements. As a result, organizations need to employ measures that record user activity on a granular level, so that risk factors can be identified and mitigated faster.
- **Protect Sensitive Data in ALL Environments** – More often than not, protection of sensitive data is a matter concentrated on non-production (development, testing, QA, etc.) environments only. However, data assets are still at risk of exposure in production environments. To mitigate the risk of accidental or even intentional data leakage, it is important that sensitive data is located and protected in all stages alike.

## Stay prepared for incident response and remediation

Breaches are inevitable. Hold your guard up at all times and keep a remediation strategy ready to minimize the impact of security incidents as they occur.

- **Implement a Security Info & Event Management (SIEM) Platform** – Implementing systems to aggregate security data for better visibility is key to establishing risk and compliance management measures. This is necessary for SOC teams to spot threats early and quickly implement appropriate remediation efforts.
- **Implement Intrusion Detection & Response Capabilities** – Compliance is not just about knowing that you've been breached and reporting it. It is about knowing how to handle and mitigate the implications of the breach while strategizing adequate incident responses. Therefore, organizations need to have robust detection and response systems in place.

## Why is PeopleSoft an Important Part of Your GRC Strategy?

Your PeopleSoft applications are your organization's hub for business-critical transactions and the core of your organization's financial, personnel, and corporate data. The amount of sensitive data across these applications makes them a crucial part of your organization's governance, risk, and compliance strategy. With evolving threats, the security stature of PeopleSoft applications needs to evolve too. However, despite robust security features, out-of-the-box most ERP applications are not prepared to tackle modern security threats and regulatory compliance requirements.

## GRC Challenges with PeopleSoft

### Lack of Visibility

#### PeopleSoft Offers Limited User Activity Data via Logging

Like legacy ERP systems, the default logging in PeopleSoft is high-level and only records application usage data required for trouble shooting and debugging. Due to system performance considerations many organizations choose to turn off data logging and limit it to recording login and logout instances only. Native logs are mostly system-focused, bulky, and unstructured and pose the following limitations:

- Key pieces of information are missing
- Insufficient actionable data to identify or investigate a breach
- Audits need to be done manually with limited data
- Lack of data for regulatory reporting puts organizations at-risk of non-compliance

#### Lack of Actionable Analytics

Tracking a specific event in detailed logs is time-consuming. Traditional security audits performed manually on excel sheets can take weeks or even months. With data protection regulations mandating that a data breach should be reported a stipulated amount of time (for example, within 72 hours under GDPR), organizations need to have instant access to real-time transaction data that helps security teams identify, investigate, report and remediate data breaches quickly.





## Limited Security Controls

### Lacks of Support for SAML-based Single Sign-On

Organizations rely on their respective identity providers (AD, ADFS, Okta and more) to build and enforce centralized password governance policies. Since PeopleSoft applications lack native support for SAML, the widely accepted identity federation standard, those governance policies cannot be applied to them - leading to application isolation and a higher risk of password-based threats.

To make usual off-the-shelf SSO solutions work with PeopleSoft, organizations would typically have to build an extensive framework of additional customizations and potentially additional hardware in order to simulate communication between the application and their respective identity provider. Once complete, the custom solution would work, but will often be fragile and could adversely impact the ability to upgrade PeopleSoft components.

### Limitations of Traditional Multi-Factor Authentication

Conventional MFA solutions are predominantly implemented at the login screen to prevent malicious outsider access. However, once a user passes an MFA challenge at login, the data inside the application remains vulnerable to insider threats via privilege misuse, unintentional data leakage, data exfiltration and more. To protect specific data assets (i.e. SSN, direct deposit info), authentication measures must be expanded beyond the perimeter and into the application.

### Lack of Dynamic Access and Privilege Management

Access controls within PeopleSoft are governed by rigid rulesets such as static user roles and permission lists. As a result, everyone in a privileged user group or permission list can access sensitive data freely – regardless of where they are accessing it from or the data's sensitivity-level. To ensure robust security, organizations need to establish dynamic access controls based on the context of access, such as location or device, nature of data, user activity and more.

### Sensitive Data Exposure

Controlling the exposure of sensitive information is a fundamental best practice for data management. As a key tactic to control exposure, data masking protects sensitive information from intentional or accidental data leakage and significantly minimizes threats by ensuring that only authorized users who need to see data can see it, as well as only when they should.

PeopleSoft has released data masking functionality, but the delivered masking rules cover only the basic security and compliance needs, posing certain limitations:

- Masking/Redaction is governed by static roles; therefore, certain users can view all of the sensitive data while others cannot view it at all.
- One-way field masking is used. Even if a data field is masked, the field is not locked, and malicious users/ hackers can still change it.
- Masking is implemented at the UI-level only. Queries can still be used to gain access to otherwise masked data.

## Solution

Appsian Security Platform (ASP) is uniquely designed for PeopleSoft and provides layered security features that are contextually aware of both the user requesting access and the sensitive nature of the data/transaction being accessed. ASP enhances the security and visibility of your PeopleSoft environment without impacting user experience – ensuring that your data stays safe, your users stay productive, and your organization's reputation remains intact.

### Actionable Insights

#### [Granular PeopleSoft Logging and Activity Monitoring](#)

With the goal of helping customers minimize the impacts of breaches and avoid regulatory violations, ASP's detailed logging features enable direct visibility into user activity within PeopleSoft. The security logs record all user transactions on a granular level, providing the level of detail needed to comply with data protection regulations, fulfill audit reporting, and to investigate and respond to breaches efficiently. Logs include detailed information on who is accessing the data, what information is being accessed, where it is being accessed from, user ids, IP address involved and more.

#### [Visualized Analytics for Expedited Detection and Response](#)

Appsian's Security Analytics software integrates with PeopleSoft to seamlessly access the essential data needed to identify suspicious activity and mitigate issues. Advanced visual dashboards equip security professionals with real-time snapshots of data usage and enhance data discovery and exploration capabilities to expedite breach detection and response efforts.



## Modernized Access Control

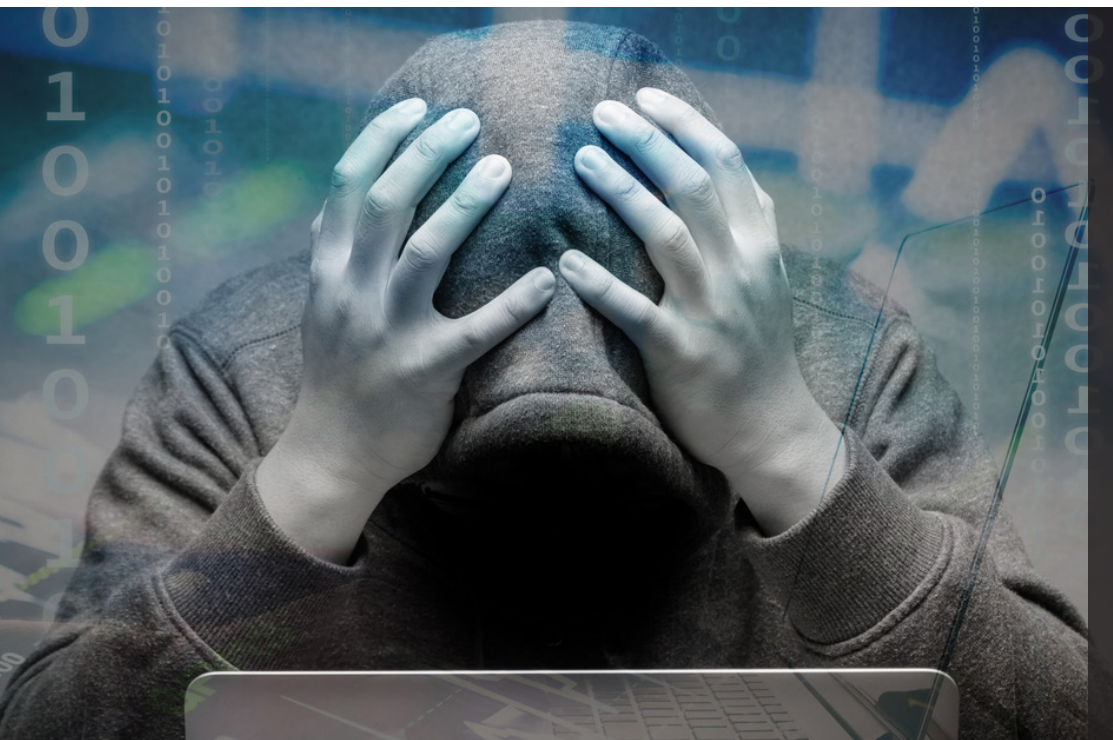
### [Native SAML Integration to Enable Single Sign-On](#)

AppSIan's Single Sign-On solution enables seamless, secure access to PeopleSoft for organizations leveraging SAML based Identity Providers. It enables centralized ID management by supporting identity federation through the implementation of related rules capable of responding to assertions/claims from SAML providers.

By using existing identity providers with PeopleSoft, organizations can simplify the login process to improve user engagement and productivity, allowing users to switch between applications seamlessly and reducing password-related downtime. Additionally, strong password governance policies set forth by identity providers can be used to improve security, and the removal of manual logins will reduce the likelihood of compromised credentials.

### [Multi-Factor Authentication Inside PeopleSoft](#)

AppSIan's MFA allows organizations to expand MFA functionality to the field, page, and component levels within PeopleSoft. Unlike conventional MFA solutions that only protect the front door, AppSIan's MFA can leverage all existing PeopleSoft artifacts to challenge users with MFA at login, and also in scenarios such as when trying to access their direct deposit information from an unrecognized location (off your secure network) – or have high-privilege users challenged if they are attempting to access specific PII or execute a transaction deemed highly sensitive.





## Contextual Security

### Location-Based Security & Least Privilege Access

ASP regulates user access based on the user's location of access. Aimed at controlling the misuse of PII from stolen credentials to high privilege accounts or privilege misuse by insiders, ASP applies conditional access by leveraging the context of where access is coming from. Considering whether users are accessing PeopleSoft from a secure network or the open internet, organizations can apply rules for what users can view and what transactions they can execute.

### Dynamic Data Masking/Redaction

ASP allows organizations to partially or fully mask any data field(s) to prevent unsolicited divulgence of sensitive information. Using ASP's data masking rules, organizations can configure which fields to mask, apply conditional access rules for end users to view masked data, and track the access to sensitive data by tagging it with corresponding user ids. Features like click-to-view masking allow organizations to minimize exposure without obstructing users.

## Conclusion


Risk management and compliance have evolved from being IT centric issues to impacting enterprise-wide business functions like legal, HR, supply chain, finance and more. Data protection mandates such as GDPR have increased the pressure on security teams to better manage sensitive data and the risks surrounding it. The key to success lies in understanding the needs of your organization's unique IT and business structure and incorporating prevention and remediation features throughout.

When it comes to PeopleSoft applications that've been in action for decades, layering prevention, visibility, as well as remediation features within your applications, on a granular level, can ensure that you are prepared to minimize if not eliminate potential risk to sensitive data. Monitoring user activity, establishing access controls, and eliminating unnecessary privilege can help propagate compliance as an organizational culture rather than being an obligatory operational burden.



8111 Lyndon B Johnson Fwy. Dallas, TX 75251

© AppSIAN 2019

 +1 (469) 906-2100

 [info@appsian.com](mailto:info@appsian.com)