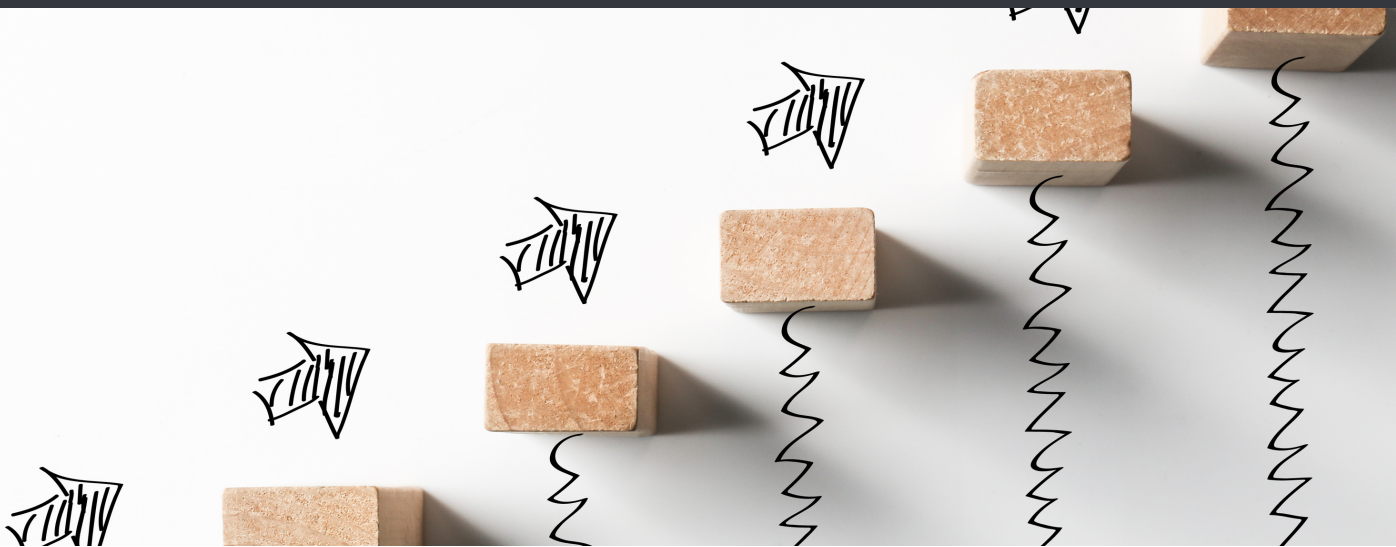


Safepost Quarterly

Great Stuff for Cyber Security
and Risk Management Buffs.



A message from SafePaaS CTO

Hennie Vermeulen

We continue to enhance our platform to meet the growing demand for Identity Governance and Administration (IGA) by releasing over 25 enhancements to our flagship **AccessPaaS™** product suite over the last quarter. IGA demand is on the rise due to cyber threats and data breaches growing at an alarming rate in 2020 with the dramatic and persistent shift in the workplace towards remote work.

As organizations continue to offer remote work options, they are facing an increasing need to identify their users, control whatever they can access, and further audit their activities for security of information. Apart from this, since we also provide continuous controls monitoring capabilities, including process and data management, the business leaders across industries are rapidly adopting our latest enhancements to the **MonitorPaaS™** platform that enables sustainable remote work, agile business processes and lower IT costs.

WHAT'S INSIDE THIS ISSUE?

- A message from SafePaaS CTO
- Customer Success Program – RiskRewards™
- API Services Enhancements in AccessPaaS™
- MonitorPaaS™ enhancements
- Mitigate Business Risks with Spreadsheet Controls
- Implementation Partners now enabled to Safeguard your Enterprise Data assure GDPR and CCPA Compliance.
- Forward foresight events
- Customer success

SafePaaS introduces RiskRewards™ – Continuous Customer Success Program



We appreciate the continued loyalty of all our customers who trust SafePaaS to protect their business by monitoring GRC controls to mitigate risks in their critical enterprise system.

For more than a decade, our customers, across a wide range of industries and territories, have partnered with us to successfully advance their strategic objectives by deploying and tailoring our products that control financial, operational and IT risks.

We are proud to have been able to reward our customers, in return, by delivering hundreds of innovative features throughout the years. With our multitenant, metadata-driven platform, we have provided customers with seamless, automatic release updates, delivered in real time, with no downtime or costs.

Just a few notable customer examples include:

An American manufacturer based in Minnesota, established in 1897 deployed our first SaaS product in 2007 to ensure SOX compliance by monitoring Segregation of Duties risks in Oracle E-Business Suite 11.5.8 and upgrade to 12.1.

A leading Latin American Bank founded in 1960 has been using SafePaaS since 2009 to ensure compliance with global banking regulations.

A US Department of Energy entity located in Colorado has been using SafePaaS for 10+ years to remain compliant with OMB Circular A-123.

As we continue to grow our customer-base at a higher pace each quarter, with the last quarter growing over 120% compared to the same quarter last year, we are introducing the RiskRewards™ program to ensure that our customers can count on the rewards from SafePaaS by mitigating risk in their business in the future.

For RiskRewards™ program details, please visit our [RiskRewards™](#) page on our website.

API Services enhancements in AccessPaaS™ mitigate cyberthreats with advanced Identity Governance and Administration.

Our latest Application Programming Interface (API) Services enhancements now offer AccessPaaS™ customers a wider range of options to integrate advanced access controls to mitigate cyberthreats that make their way inside to attack the heart of the enterprise. CISOs can now deploy advanced application access controls to prevent cyberthreats and ensure that user access to enterprise data and process complies with company policies and regulatory mandates. Advanced application access controls can manage user access requests, roles design, and entitlement configurations by detecting as well as preventing access risks based on fine-grained rules logic. Fine-grained access rules can be configured in SafePaaS that supports meta-data for the enterprise-wide application security model.

API Services adoption is growing rapidly, driven by digital transformations, cloud migrations, and data privacy regulations. IT security must ensure that every connected mobile app, every website that tracks users or provides a rich user experience, and every application deployed on a cloud service uses API connection points between the identity management platform and application ecosystems.

There are several options available to enable access controls for Identity Governance and Administration (IGA) based on the web-services supported by enterprise applications, IDM and ITSM systems. Customers can deploy the optimal solution that enables real-time fine-grained violation analysis to prevent user security risks in centralized authentication, single sign-on (SSO), session management and privilege authorization for enterprise applications.

Download our latest e-book for more details.

CISO's Guide to Enterprise Application Access Governance



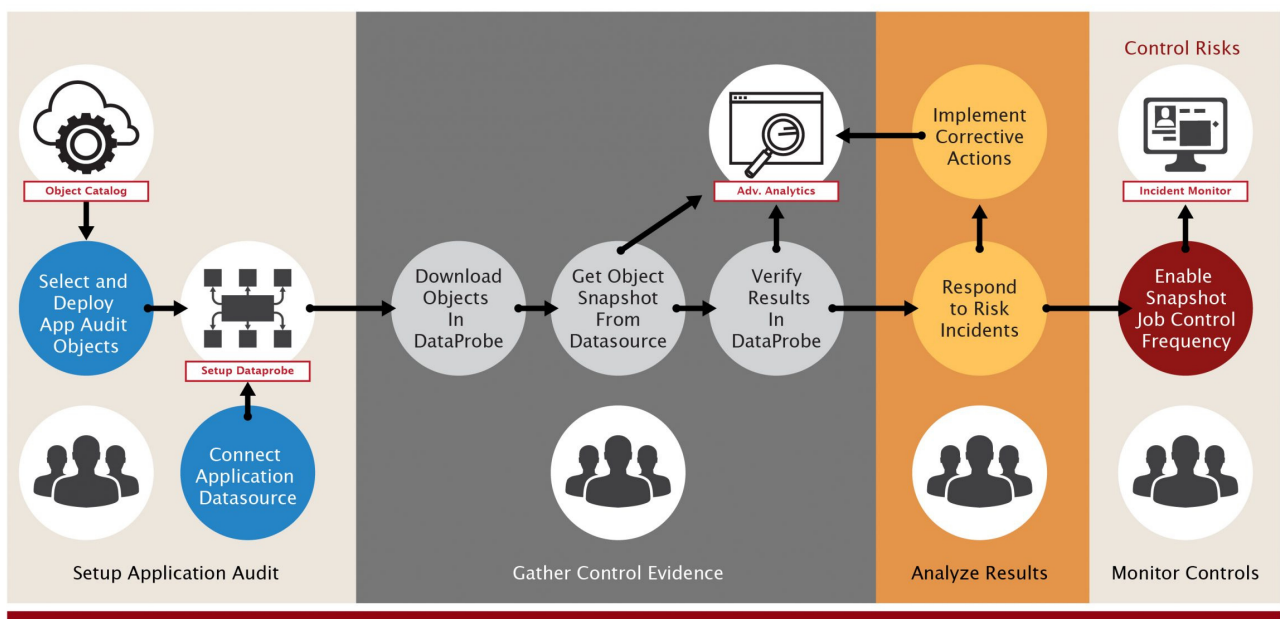
All product names, logos, and brands are property of their respective owners. Use of these names, logos, and brands does not imply affiliation.

MonitorPaaS™ enhancements enable sustainable remote work, business process agility and lower IT costs.

Business Process Owners, Controls Operators, and IT Managers can setup alerts based on thresholds using the latest enhancement to Monitor Rules Logic to receive workflow notifications that require timely response to prevent process workflow bottlenecks.

Enhancements to the Monitor Results Set template enables users to format the sequence and display fields based on reporting needs using a configurable template to define the display attributes and sequence. Change tracking records now auto-populate tracking fields, like who, when, where, based on the monitor type.

Enhancements to the auto-generated business object code enables agile business processes by optimizing business process activities aligned with rapidly changing operating environment. The capability also accelerates monitor deployment across Dev/Test/Prod instances. Enhancements to the Log Report provide advanced debug information to diagnose datasources mapping and object snapshot errors.



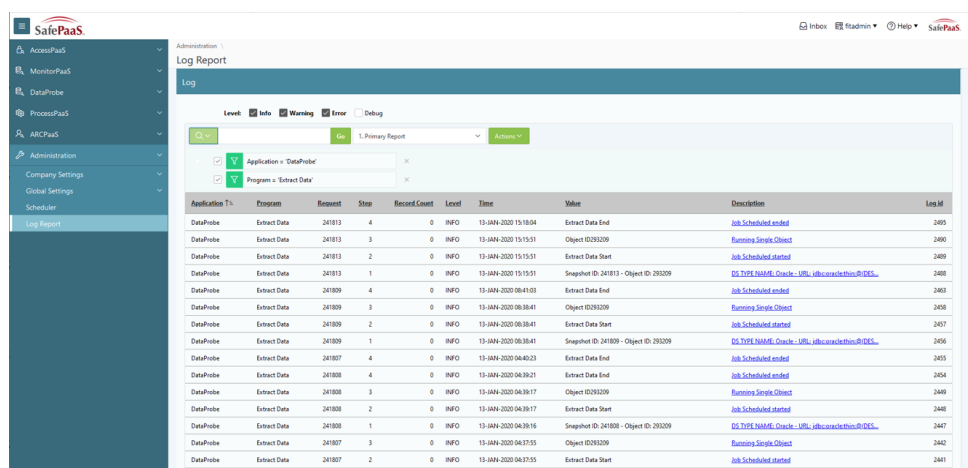
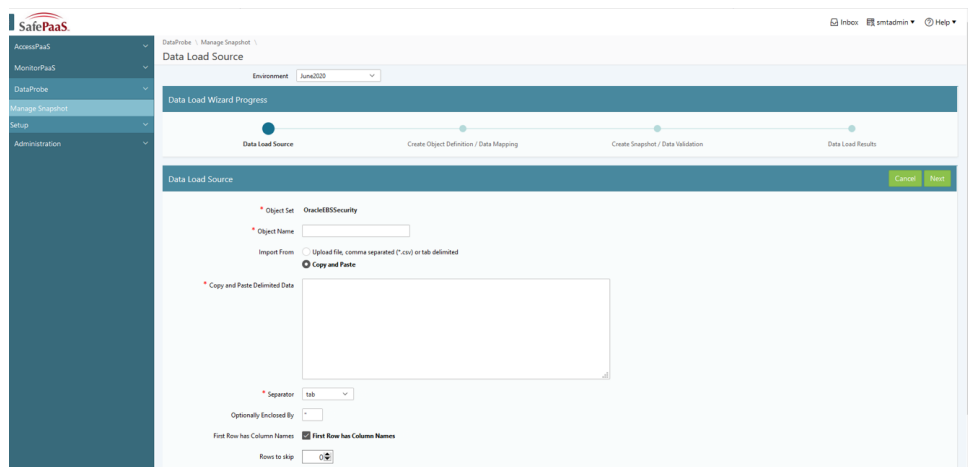
Mitigate Business Risks with Spreadsheet Controls

Spreadsheet use is growing as organizations continue to offer remote work options to the employees that support crucial business management and reporting functions. Spreadsheets are being used to fill in the gaps in ERP applications by extracting financial, operational and employee data, computing results and creating summary reports and charts for management to support critical decisions. However, the power and flexibility available to individual spreadsheet users is increasing enterprise-wide risks, combined with work-from-home distractions and fallibilities. In a recent survey, 90 percent of spreadsheets contained errors – indicating inherent risk that is far too great for management to tolerate.

ExcelGuard™ is our newest data protection functionality that allows you to simply cut and paste or upload data from a spreadsheet into SafePaaS, creating an auditable snapshot of the spreadsheet with data access controls. Furthermore, the snapshot transfer to SafePaaS objects is tracked in an audit log with the option to scramble and mask sensitive data. You can use ExcelGuard™ to ensure compliance with data privacy policies and regulatory mandates such as GDPR, CCPA, HIPPA, PCI, etc as well as streamline Provided by Client (PBC) requests for information and supporting documents to complete SOX audits.

Any changes to the spreadsheet data snapshot can be monitored using change tracking and comparison controls in MonitorPaaS™ with closed-loop approval workflow.

For more information, you can view our latest webinar [“Mitigate Business Risks with Spreadsheet Controls”](#)



Our Implementation Partners now enabled to Safeguard your Enterprise Data assure GDPR and CCPA Compliance.

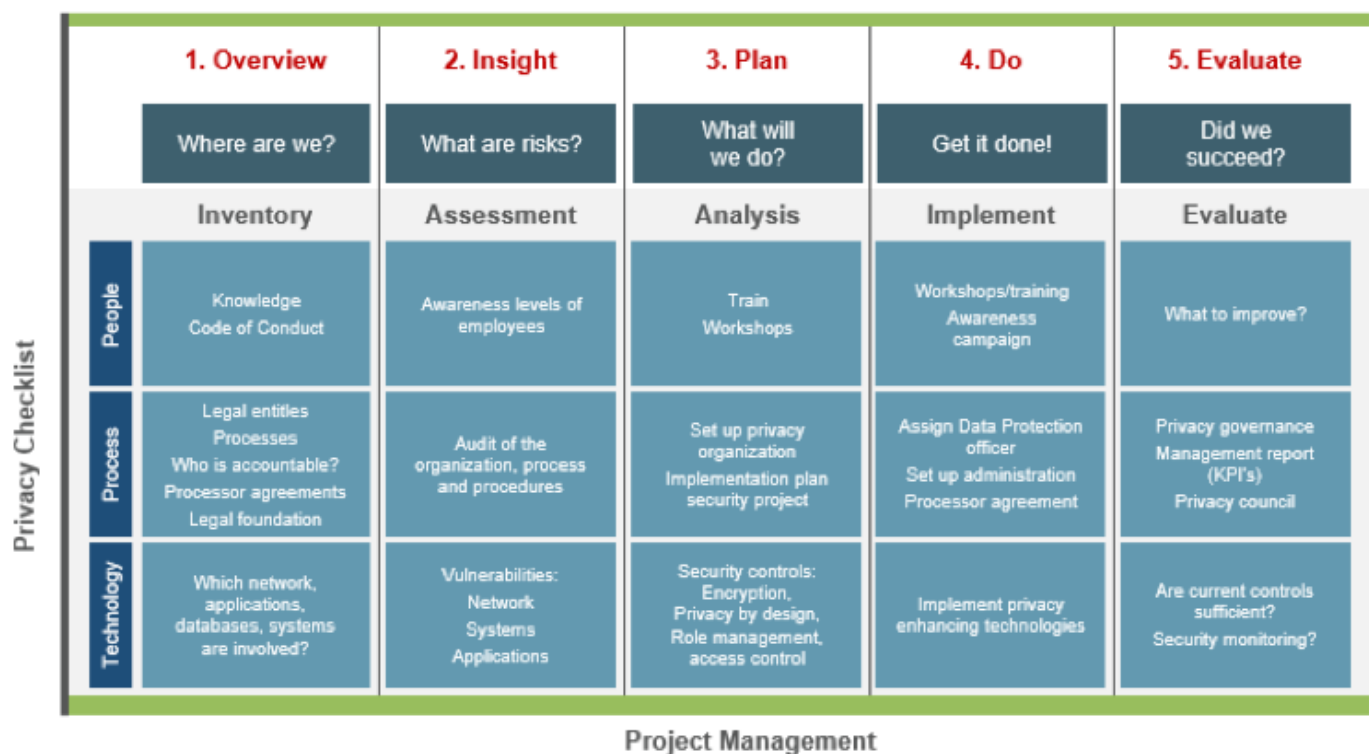
Continued enhancements to Dataprobe™ can help you detect, remediate, and prevent data breaches in your ERP system.

The majority of sensitive data such as customer credit details, supplier bank information and employee national ID's are stored in ERP systems. However, the fine-grained security measures required to protect this data has been overlooked for many years. As organizations have exposed ERP systems to the internet that provides continuous online access, the data stored in ERP systems has become vulnerable to cyber-attacks.

Our certified partners can implement SafePaaS with built-in Data Governance Best Practices to help you address enhanced data protection requirements by automating data discovery and mapping. The data protection controls span the life cycle activities over enterprise data processing. You can mitigate data privacy risks in operations, infrastructure, and customer-facing web-services, that are continuously monitored by SafePaaS.

SafeMethod™ implementation approach for enterprise data protection, followed by our services partners, ensures collaboration and sustainability. Our data protection solution supports built-in digital data discovery, data inventory, DPIA / PIA and assessment templates. You can deploy SafePaaS to facilitate ongoing periodic audits, that reflect business changes, enabled by workflows, and analytics that will automate and streamline the data protection process and serve as the central repository of compliance evidence.

The following chart shows a high-level SafeMethod™ data protection approach that can help you develop a sustainable data governance program:



Read our white paper, "[Data Breaches are the New Normal – Detect, Remediate and prevent Data Breaches.](#)"

SafePaaS Forward Foresight Events – Risk Knowledge that removes obstacles to propel your business forward.

SafePaaS has a series of events that explore key topics around risk management, digital transformation, cyber security and IT Modernisation. You can keep up-to-date with all our events on our event page.

In May, we presented “Understanding the New Technology and Security Risks as You Respond to COVID-19” with Dan Miller from Altum Strategy Group. In this webinar, we covered new risks that have emerged due to the COVID-19 pandemic and how we can to assess those risks. These included: Financial Risks, Operational Risks, Customer & Supply Chain Risks, Enterprise Data Risks and Remote Work Risks.

In June, we co-hosted a webinar as part of our monthly series with leading Oracle GRC expert Brian O’Neil from Appssurance. We invited Brian to explore how organisations gain actionable business insight with Continuous Controls Monitoring. The on-demand version is available on our website and can be accessed [here](#). Oracle GRC is on very limited support and with many customers realising the technology risks associated with using legacy software, Appssurance and SafePaaS are working together to upgrade customers to a more flexible, agile platform. You can read about the top technology risks of using outdated GRC software [here](#).

In July, we invited Dr Saif Abed from The AbedGraham Group and Chuck Scheller, Business Systems Consultant with 18+ years-experience in the healthcare industry to discuss how cyber security solutions can help protect patients at scale. SafePaaS’ diverse range of risk management capabilities can now be enriched by the power of The AbedGraham Group’s physician- developed clinical security analytics to identify patient safety and clinical workflow disruption risks to guide security control strategies.

How cybersecurity solutions can help protect patients at scale?

Wednesday July 22 12 Noon EDT (on-demand to registrants)



Dr Saif Abed
AbedGraham
Partner and Director of
Cybersecurity Services





Chuck Scheller
Business Systems Consultant
18+ years in Leading
US Healthcare Organization



Adil Khan
SafePaaS
Information Risk Management
CEO



August saw us present “How to Mitigate Business Risks with Spreadsheet Controls.” A recent survey reported that 90 percent of spreadsheets contained errors – indicating inherent risk that is far too great for management to tolerate. This webinar explored easy-to-use techniques to simplify the complexity of managing large spreadsheets, prevent mistakes in formulas, and maintain audit trail to control data access and mitigate the risk to potentially serious damage to your business reputation and bottom-line. To view the webinar click [here](#).

September sees the launch of our latest event, “[Oracle Governance, Risk and Compliance: Dead Product or Brave New World?](#)” This is a 4-part event to help Oracle GRC customers understand their options so that they can prepare for the future. All details about this event can be found [here](#). We start the event off with a panel discussion where we’ll be joined by Oracle GRC veterans Nigel King, Jannie Wentzel and Brian O’Neil from Appssurance “Why Advanced Controls Are Needed for ERP systems. Everything Oracle Customers need to know about the evolution of software that manages and automates Governance, Risk and Compliance controls.”

There will be a special session on November 11 for all SafePaaS customers entitled, “How SafePaaS Customers can Extend GRC Controls to the Enterprise – 12-month plan to leverage SafePaaS software throughout the organization.”



We will provide detailed information into the following topics:

- Review/Overview of the software capabilities
- How to integrate SafePaaS within your Security Architecture
- How to leverage SafePaaS Across multiple ERP Platforms
- Update from Product Development – What’s Next?
- Best practices from the field – lessons from our customers
- Building a Strategy and a Plan for Enterprise Controls
- SafePaaS Customer Success – New for 2021



Some of our recent customer success stories include:

A Global Telecommunications Organisation **goes live with iAccess™** for 500+ users.

iAccess™ will allow self-service application access request management and will ensure that each provisioning request is checked against access policies before allowing privileges to be granted. SafePaaS iAccess Provisioning Software Service will enable the organisation to ensure that all user provisioning requests proceed according to their Segregation of Duties and Restrictive Access policies.

US government agency that ensures the safety and security, as well as the reliability of a nuclear arsenal to protect the US selects **iAccess™** to improve User Provisioning.

American energy company based in Oklahoma chooses SafePaaS to prevent access risks in **Oracle ERP Cloud and Workday**. The organisation has chosen Enterprise Access Monitor and Roles Manager to remediate ERP security and control violations by addressing the root cause of the problem.

Global organisation in the food industry chooses SafePaaS for a Proof of Concept to automate fine-grained segregation of duties controls monitoring in **Oracle E-Business Suite** as well as streamline and self-service user access audit process in iAccess for ServiceNow.

An American manufacturer of programmable logic devices will use Access Policy Monitor™ and DataProbe™ Objects for Oracle E-Business Suite to ensure compliance and mitigate fraud.

The SafePaaS Team