MAY 2020

Safepost Quarterly

Great Stuff for Cyber Security and Risk Management Buffs.

A message from SafePaaS CTO

Hennie Vermeulen

First and foremost, I'd like to thank you all for continuing to put your trust in SafePaaS during these challenging times. At a time like this, our company has a responsibility to continue protecting your critical business systems to help you maintain business continuity. Our product management and support services teams are working around the clock to make sure that all our platform is available to meet your risk management needs.

Furthermore, as businesses impacted by COVID-19 are under pressure to respond to emerging technology risks, streamline ERP access controls for the remote workforce, and maintain effective controls over significant processes such as Procure-to-Pay, Order- to-Cash, and Financial Record-to-Report, we have introduced a number of new enhancements to rapidly deploy automated controls to continuously monitor business performance. We are committed to our innovation plans for 2020 to enable our customers adopt essential new cloud services and continue forward with clarity, collaboration and confidence.

WHAT'S INSIDE THIS ISSUE?

- A message from SafePaaS CTO
- Business Continuity Management
- Enhanced self-service Access Management for remote workers and managers
- FireFighter ID™ for emergency access
- Access Monitor™
- Control Monitors
- Enhanced DataProbe™
- Customer Success
- SafePaaS Events
- Partner Spotlight

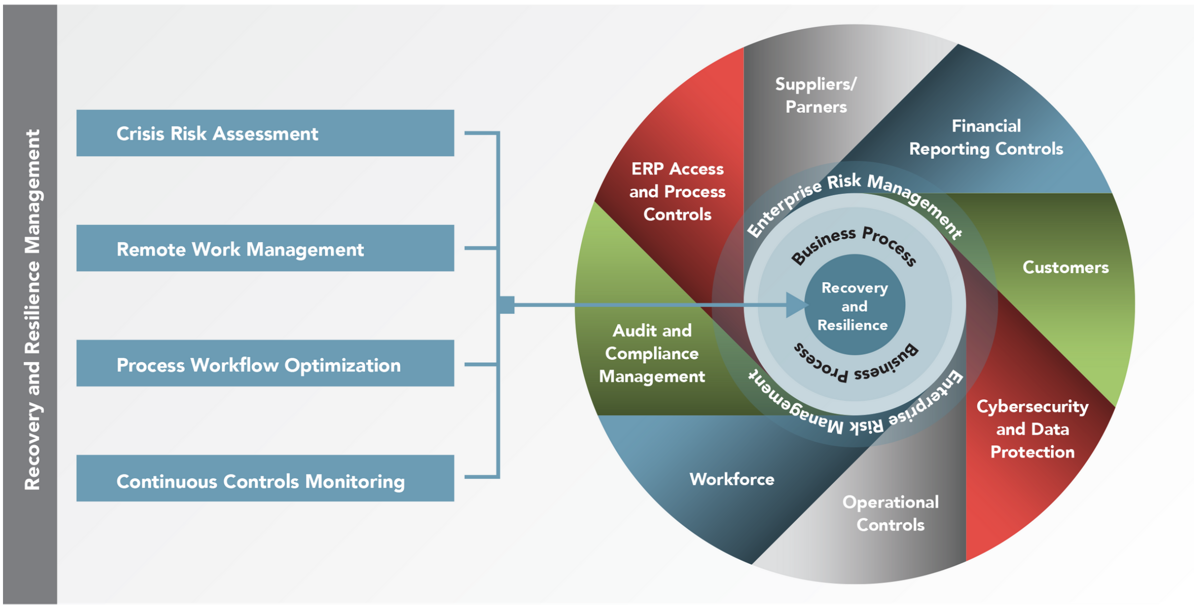
Strengthen your Business Continuity Management Program with SafePaaS.

SafePaaS Business Continuity Program enables businesses to adopt a structured framework to assess risks, implement continuous controls monitoring to build resilience for what's next, and help reform your future for what comes beyond the pandemic.

We are offering a Business Recovery and Resilience program to businesses affected by the pandemic, which includes five Key Risk Indicators for supply chain, finance and customer service. The subscription and service assistance is free until September 30 2020. You can gain immediate access to easy-to-use apps, content and best practices to support all phases of Business Continuity Management (BCM) Lifecycle which will help you assess risks, manage remote work collaboration, detect process bottlenecks and monitor operations enabled by ERP systems.

Organizations that adopt a structured framework to execute resilient strategies, operate fluidly and adapt quickly to threats and disruptions, can continue on their strategic path, beat competitors to market, launch new products and services with calculated efficiencies, and avoid major issues that affect operations, reputation and the bottom line.

Business Continuity Management


Recovery and Resilience Management
Crisis Risk Assessment
Remote Work Management
Process Workflow Optimization
Continuous Controls Monitoring
Suppliers/ Parners
Financial Reporting Controls
ERP Access and Process Controls
Customers
Audit and Compliance Management
Cybersecurity and Data Protection
Workforce
Operational Controls
Enterprise Risk Management
Business Process
Recovery and Resilience
Business Process
Enterprise Risk Management

Enhanced Self-Service Access Management for remote workers and managers.

Remote workers need secure access to their authorized job functions in ERP systems to perform their daily work as they navigate the new challenges of working from home. SafePaaS iAccess™ keeps employees securely connected to business-critical ERP systems and their work groups to maintain a productive daily work schedule, as they juggle personal commitments.

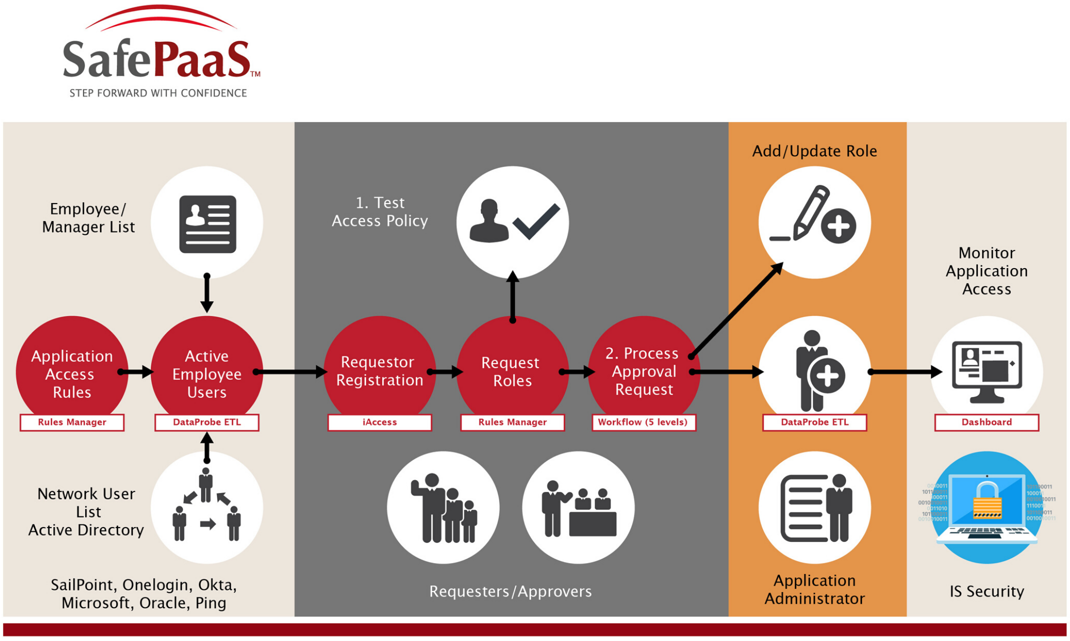
iAccess™ enables self-service application access request management. It ensures that each provisioning request is checked against access policies before allowing privileges to be granted. Exceptions that require management approval are processed via workflow notifications to obtain electronic approval from authorized supervisors.

The latest iAccess™ capabilities include:

- **More Flexible Self-Service Workflow:** We have improved iAccess™ Self-Service Access Management Workflow that enables you to set up up to five levels of approval with backups and conditions to meet the changing access requirements of remote workers and managers.

- **Fully-Automated Privilege Change Management:** Managers and Security Administrators can now easily change user roles and privileges as well as de-provision ERP inactive users within SafePaaS. This advanced privilege change management capability can help organizations monitor ERP dormant user accounts, reduce the cost of unused licenses, mitigate access risks in security configuration changes to prevent "privilege creep" as remote work is ramped-up.

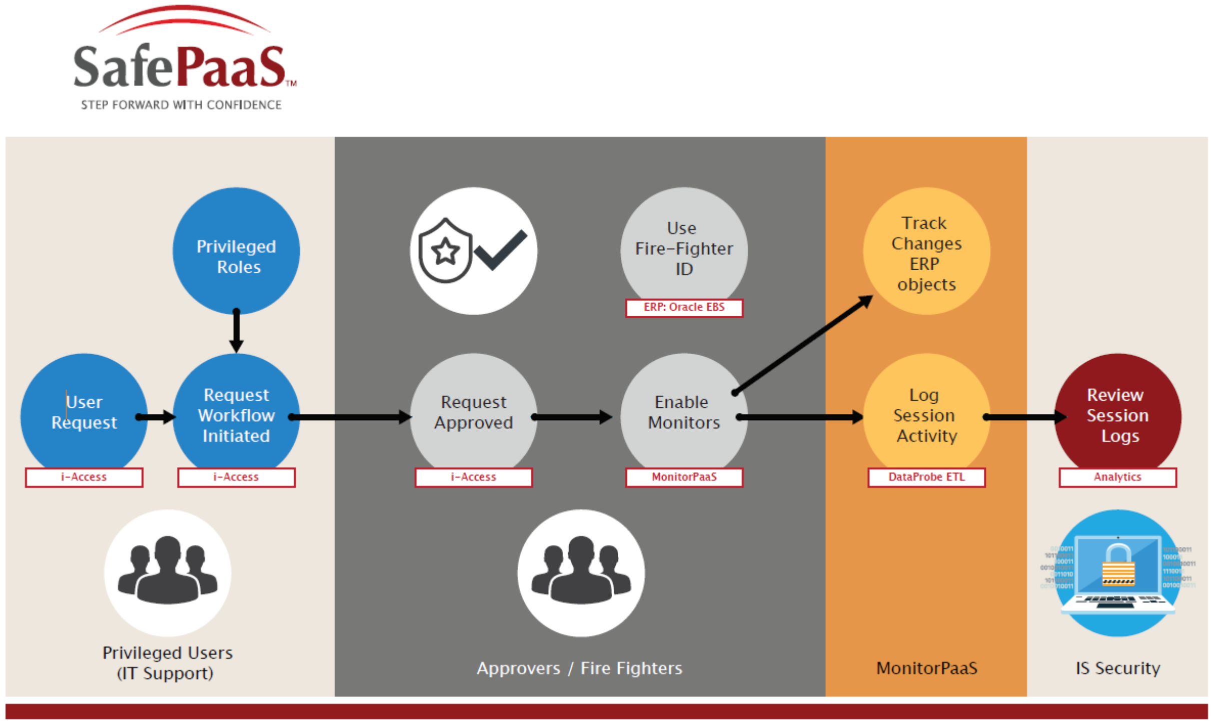
- **Improved Privilege Authorization API Services for Fine-Grained Identity Management to control access to business-critical systems:** Identity Governance has become a key catalyst to enable digital transformation and modernize the IT environment. However, many organizations are struggling to implement fine-grained identity and access management controls that prevent growing cyberthreats to ERP systems and mitigate access control risks as hundreds of users add, change, delete requests and processes every day through inconsistent, ad-hoc and manual processes across disparate provisioning tools and workflows. SafePaaS Fine-Grained Identity Access Management (IAM) services enable ERP customers to check each access request by invoking SafePaaS API services from many different request management systems such as ServcieNow, OneLogin, Okta, Azure, SailPoint, Oracle, etc.



FireFighter rapid request manager and audit trail streamlined for emergency access.

FireFighter is a secure process for controlling super-user access across multiple systems with an independent system of record to prevent audit-trail manipulation. SafePaaS enables pre-authorized users to request temporary access to elevated privileges to business-critical applications.

The enhanced Firefighter request processing enables SafePaaS Administrators to grant immediate access to pre-approved users with assigned fire fighter access to be able to get immediate access without any bottlenecks. The elevated access is logged for management review.



Risk and Group filters now available for enterprise-wide, Periodic User Access Certification.

Access Monitor automates the Periodic User Access Review and Verification process with notifications to each department manager, application owner and process owner to review active users and privileges assigned to those users. You can detect and prevent any unauthorized user access rights and quickly correct any conflicts.

The enhanced capability enables the SafePaaS Administrators to categorize user roles by risk levels e.g. High, Medium, Low and assign access groups such as business units, departments, locations, etc. Once the Roles are categorized, the administrator can filter the user roles by risk and access group to send certification requests. This improvement, combined with Dataprobe ETL enhancements, can enable organizations to implement effective access controls in all business-critical applications as well network identity privileges stored in Active Directory, or IDM systems.

Control Monitors enhanced to detect emerging risks, ensure compliance and mitigate operational disruptions.

The Rules Logic is enhanced to detect materialized risk: This improvement will help you evaluate the emerging risks of newer operating models and business practices so you can redirect your attention to the most time-sensitive risks.

You can use the latest capabilities in Rules Logic to "look-back" transactions in multiple data sources and objects to detect materialized risks. For example, if a Segregation of Duties (SOD) risk reports users with access to Enter/Update Supplier and Pay Supplier, you can identify if any of those users actually performed the two conflicting transactions, which may lead to a Fraud Risk. This capability can reduce errors, waste and cash-leaks if remote workers are granted emergency access to security policy waivers during the pandemic.

Compare Results with Control Monitors to ensure compliance: Companies are facing many compliance and reporting challenges depending on where they are in the fiscal year. These challenges come in the form of practical considerations, like the ability to "close the books," apply complex and judgment-based accounting concepts, reconcile accounts, meet regulatory expectations and filing deadlines.

You can use the latest Compare Results Set feature to streamline your financial close process that can automate financial close tasks such as account reconciliation, variance analysis and changes of key risk indicators of financial condition, and operating performance.

Use the latest Control Monitors capabilities to detect and correct risk in your ramped-up provisioning process.

Companies drastically increased remote access to business applications capacity to meet the needs of business need of "Connectivity First". In this rush, many companies compressed or ignored their risk and change management processes. While understandably given the speed the business demanded, those policies exist to protect the business from bad actors (internal and external).

Now you can deploy control monitors to answer an important audit question: “What business-critical application privileges my remote users can access vs. what access was last approved in your provisioning system whether it's manually processed or enabled by any of the leading user request management systems such as ServiceNow, Azure, Okta or SailPoint?” Without effective access request analysis, security breaches could be occurring right now and remain undiscovered for months.

Screen third party risks with Watchlist Monitor™ to avoid operational disruptions: Streamline your screening processes with powerful customization and control, and a range of time-saving features for single users or large teams. Our unified controls monitoring platform provides 360 degree visibility to support your due diligence needs in the fight against financial crime, bribery, and corruption. Integration services are available to pair with data from the world's leading sources of intelligent information including Thomson Reuters World-Check One, and Dow Jones anti-money laundering (AML), as well as the Office of Foreign Assets Control (OFAC), a financial intelligence and enforcement agency of the U.S. Treasury Department.

Dataprobe™ enhanced data governance capabilities improve data protection and compliance with CCPA, GDPR and other data privacy regulations.

At-home work due to the COVID-19 pandemic is leading to a spike in data breaches that's greater than anticipated, according to the International Association of IT Asset Managers (IATAM).

Many users of business-critical applications may have been granted permissions to sensitive data to perform their jobs remotely, without management oversight. The risk of unpatched applications, databases and servers is increasing as IT support staff is overloaded with remote support. Unprotected business computers can allow hackers to load malicious files with admin privileges.

The latest updates to Dataprobe enhance the data governance capabilities to protect sensitive data access from business-critical applications by providing the SafePaaS administrator the ability to grant access only to pre-authorized business objects. Encrypted data transfer from the datasource to SafePaaS can also have an added level of network security by a point-to-point private tunnel to ensure intended use only within a private network in such a way that the routing nodes in the public network are unaware of the transmission. Additionally, Dataprobe logs a history of all data snapshots retrieved from the datasource. Advanced options are available to create a mask or encrypt data in SafeObjects™ - user defined Dataprobe objects that extract and store data using a wide range of methods such as JDBC connection to application database, CSV import from a spreadsheet, JSON and Web-Service API.

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 and IT Modernisation. You can keep up-to-date with all our events on our event page.

In February, as part of our monthly webinar series we hosted **"Protect your critical business applications against emerging cybersecurity threats"** Learn to protect your enterprise applications against emerging cybersecurity threats with Fine-Grained Identity Governance. You can find the webinar here.

In March, we hosted a webinar **"Ramp up remote work to safeguard your organization"** Learn how to gain visibility with data and analytics to manage and monitor your organisation effectively. This webinar can be found here.

In April, we co-hosted a panel discussion with our UK partners Searchlight. We invited a small, cross-industry panel of leaders to explore how the increasing trend towards hybrid technology landscapes, with multiple cloud business applications working together with legacy, on-premise systems, compounds the ability to effectively monitor process execution and manage risk and data. You can find the recording of **"Ensure Risk and Compliance isn't the missing piece of your Cloud or Digital Transformation"** here.

In April, SafePaaS was preparing to exhibit at COLLABORATE 2020 in Las Vegas, but unfortunately, like many of the events we had planned on attending this year it was cancelled. Two hundred of the five hundred educational sessions planned for COLLABORATE were "lifted and shifted" to this new online event. SafePaaS was honoured to have our presentation **"Data Breaches are the New Normal"** selected. In the session we shared data governance best practices to assess, protect, remediate and respond to data breaches. We provided real-world examples, based on client case studies, to continuously monitor data privacy policies.

Customer Success Stories

We are grateful to all our customers that trust SafePaaS to protect their business. Here are a few recent success stories from the first quarter of 2020.

Japanese Automotive Leader chooses SafePaaS for Access Governance.

With companies looking to protect their business applications from ever-emerging cybersecurity threats, we are thrilled to have been chosen by an automotive global market leader, listed on the Tokyo Stock Exchange with 6,000 + employees to manage access controls and mitigate risk in Oracle ERP. By using AccessPaaS the company can improve productivity and reduce costs by enforcing access policies before violations get introduced into the ERP environment controlling sensitive business information to potential cyber threats. MonitorPaaS will allow the organisation to continuously monitor business activities within enterprise applications.

A leading US Bank established in 1898 with more than 500 branches all over the US chooses SafePaaS to help reduce segregation of duties risk in PeopleSoft.

SafePaaS will allow them to detect, prevent and remediate Segregation of Duties as well as improve assessment and documentation for SOD. The bank will be able to provide comprehensive, easy-to-read reports to their auditors. Jump start their top down risk-based SOD analysis with hundreds of SOD Rules based on thousands of application functions included in the SafePaaS rules repository. Rapidly reduce SOD risk with workflow-enabled collaboration among process owners, application managers, IS security and auditors and pull reports from one unified, trustworthy source.

World-class developer and manufacturer of Aerospace and Defence Systems selects SafePaaS to ensure effective GRC controls.

We are delighted to have been chosen by an American rocket and missile propulsion manufacturer headquartered in California to ensure effective controls in an Oracle EBS Upgrade and Migration project.

UK-based Consumer goods company selects SafePaaS to prevent access risks in Netsuite.

A multinational consumer goods company headquartered in London, UK with 155,00 employees worldwide extends SafePaaS to three new subsidiaries to help with an automated, repeatable Segregation of Duties solution to improve their monitoring of user access risks in Netsuite. The company will use policy-based centralised orchestration of user identity management and access control to mitigate risk.

The leading, global auto loan financing organisation renews SafePaaS Services to control risks in Oracle E-Business Suite.

A global provider of auto finance, with operations in the Americas, Europe, and Asia renews agreement to continue with SafePaaS ERP controls and trust their business-critical systems for Oracle EBS. SafePaaS, through a technology partner provides sensitive access and segregation of duty controls to detect and mitigate risks in key business processes such as order-to-cash, procure-to-pay, record-to-report.

A global audit firm selects SafePaaS to test Segregation of Duty controls in Workday.

One of the major, global audit and professional services firms with over 270,000 employees worldwide, in 150 countries selects SafePaaS for testing sensitive access and segregation of duties controls in Workday Human Capital Management (HCM) and Financials Management to provide assurances over financial statements for publicly-held companies.

Partner Spotlight

Partners are a key part of our ecosystem here at SafePaaS. In the last few months we are delighted to have welcomed onboard:

Searchlight Consulting - United Kingdom- Searchlight are independent specialists in technology-enabled change architecture, design and implementation, helping clients to align enterprise technologies, business applications and digital strategies. Searchlight partners with client organisations to shape digital transformation programmes and deliver change; enabling companies to grow, develop new capabilities and future proof their business. It has over 340 senior-level associates who bring high-quality experience of technology-enabled change, across a range of business areas and a multitude of industries; including retail, travel, leisure, financial services, manufacturing, wholesale and distribution sectors.

Appssurance - USA- Appssurance excited to partner with SafePaas to expand our capabilities delivering industry leading risk advisory solutions to our global clients. The comprehensive and integrated cross-platform solutions from SafePaaS will undoubtedly help our clients proactively manage and mitigate risks while reducing their overall cost of compliance.

For over 16 years Appssurance has been delivering risk advisory and continuous controls monitoring solutions to organizations around the world. Appssurance specializes in delivering risk advisory solutions to organizations running Oracle EBS, Oracle ERP Cloud, PeopleSoft, JD Edwards, Workday and Coupa. Appssurance resources average over 20 years of experience working previously at the Big Four audit firms, Oracle Corporation and multiple Fortune 500 companies. Appssurance has headquarters in Tampa, Florida.

The SafePaaS Team