SafePaaS

Risk Pro Solutions, LLC

The Essential Guide to GRC Technology

Co-authored by SafePaaS and Risk Pro Solutions

Table of Contents

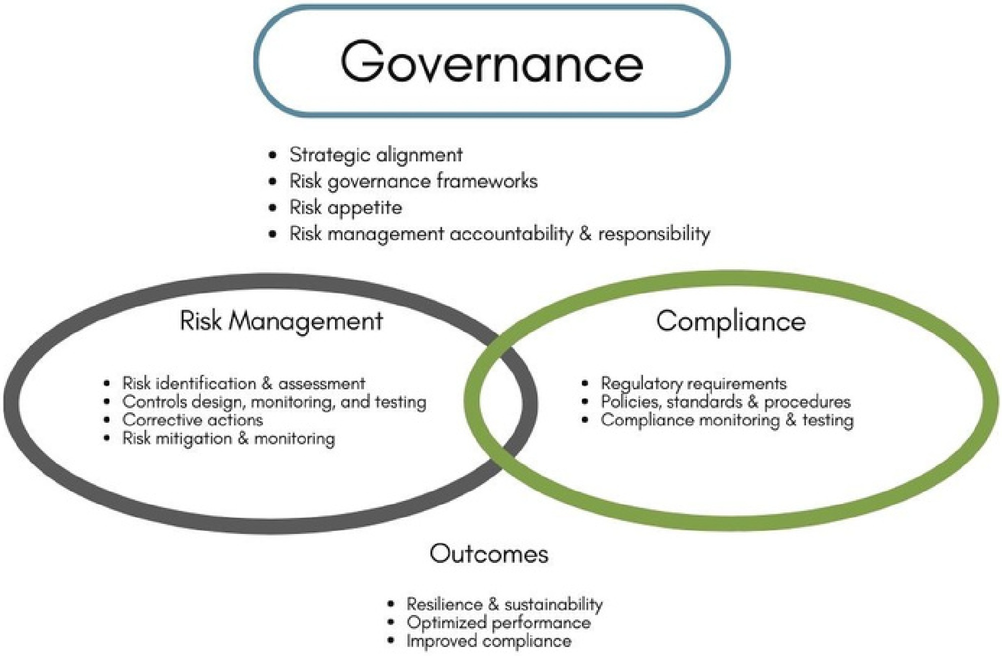
This e-Book provides an overview of the emergence of GRC solutions and describes functional capabilities found in a true integrated GRC ecosystem. It then goes on to discuss the considerations for continued investments in GRC and evaluating the benefits of updating GRC technology solutions.

When and why should you consider updating GRC technology?

It has been 20 years since the Sarbanes-Oxley Act was passed into law, marking an important chapter of corporate history where financial transparency and accountability became front and center of every public company's existence. Burdened with regulatory scrutiny, many companies were at a loss on how to demonstrate sound internal controls over financial reporting to auditors and regulatory bodies. In the last 20 years, companies have learned to juggle the art of managing risk and compliance while maintaining performance and profitability. One of the realizations that has come through this journey is that performance and risk management are not mutually exclusive, and one does not necessarily achieve one without the other. On the other hand, the risk landscape has progressively become more complex with higher standards of regulatory scrutiny, heightened cyber and insider threats, and higher fraud, supply chain and environmental risks. The risk management technology market is flooded with point solutions for risk and compliance management. Not surprisingly, companies are managing risk and compliance with cobbled-together solutions, although such a strategy may not be sustainable in the longer run. Today's integrated risk management solutions are expensive to implement and maintain, and still purportedly have challenges with integration, usability, and reporting.

The situation makes us wonder whether it is time to go back to the basics to relook at the principles of Governance, Risk and Compliance (GRC), understand what they really mean, and how to apply them in the modernization of risk technology systems.

What is GRC?


Governance
Strategic alignment
Risk governance frameworks
Risk appetite
Risk management accountability & responsibility
Risk Management
Risk identification & assessment
Controls design, monitoring, and testing
Corrective actions
Risk mitigation & monitoring
Compliance
Regulatory requirements
Policies, standards & procedures
Compliance monitoring & testing
Outcomes
Resilience & sustainability
Optimized performance
Improved compliance

The term GRC refers to a coordinated and integrated collection of capabilities necessary to support principled performance at every level of the organization. (Source: OCEG GRC Capability Model). Although GRC is often equated to technology tools only, it really means a program to enable an organization to develop, mature, and sustain risk management capabilities, make it more resilient and adaptive to business environment changes, and remain compliant with regulatory requirements. GRC refers to a holistic capability incorporating people, processes, data, and technology.

These capabilities include the work of various groups:

- Internal audit, compliance, risk, legal, finance, IT, HR
- Lines of business, the executive suite, the board, and
- Outsourced work conducted by external stakeholders

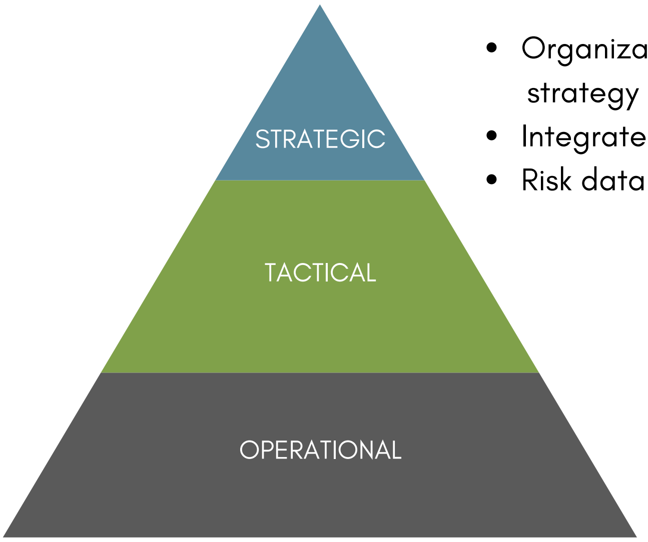
The role of technology within GRC

Technology is a key enabler that supports the automation of key activities and governance of risk and compliance data. A high-level overview of the key activities that GRC solutions help to support, is shown below:

- Standardization of risk and compliance management activities
- Increasing collaboration across risk and control teams
- Enhanced communication and reporting amongst peers and management
- Integrated risk assessments and registers across multiple organizational units
- Risk monitoring and mitigation action planning
- Key controls monitoring and testing
- End-to-end issue management
- Compliance dashboards across multiple regulatory frameworks
- Data visualization
- Audit planning, execution, and management

What do GRC systems do?

There are multiple areas where technology can be applied for the automation of GRC. To understand this better, we need to look at GRC technology capabilities across the distinct levels of the organization. GRC Technology solutions provide can be broadly classified into the following three tiers. Example capabilities include:



- Organization alignment of risk management activities with mission, strategy and values
- Integrated reporting and analytics
- Risk data visualization

- Automation of risk and control assessments
- Risk mitigation / remediation management
- Compliance framework management

- Continuous monitoring and auditing
- Automated controls testing
- Automated preventive and detective controls

Many leading GRC technology solutions offer integrated capabilities across the above tiers. Other solutions offer niche capabilities around specific areas, e.g., access controls management, policy compliance monitoring, etc.

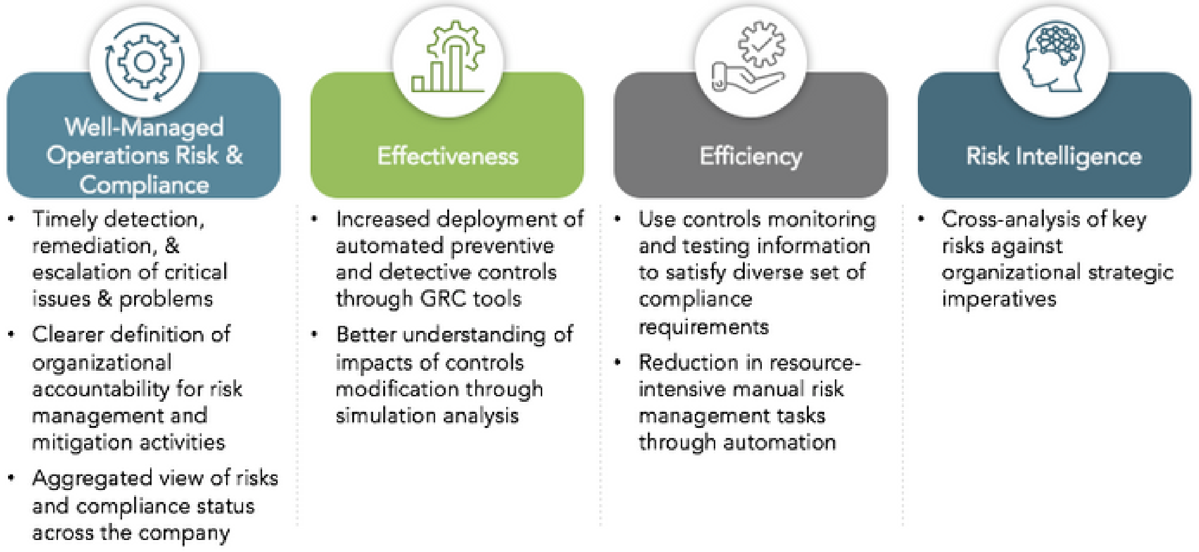
Strategic: At the highest level, GRC technology enables the alignment of risk and compliance with the overall strategy, mission, and objectives of the organization. GRC tools enable this through the establishment of a common risk data model, taxonomy organizational context, along with data aggregation, analysis and visualization, and data capabilities.

Tactical: The tactical level is the heart of the GRC ecosystem. GRC technology tools help define and maintain process, risk, and control registers, automate risk and control assessments, manage issues and corrective actions, and track compliance against regulatory requirements.

Operational: At this level, GRC tools are embedded within processes or systems for the continuous execution of automated controls and the monitoring of controls or key indicators (i.e., KRI/KPI) based on risk and compliance management requirements.

Even while considering a limited-scope solution for a niche area, it is always beneficial to have a broader automation perspective as part of the automation strategy. This will enable better scalability of the technology and integration with other GRC solutions when the need arises.

Why is continued investment in GRC technology necessary?



Well-Managed Operations Risk & Compliance

- Timely detection, remediation, & escalation of critical issues & problems
- Clearer definition of organizational accountability for risk management and mitigation activities
- Aggregated view of risks and compliance status across the company

Effectiveness

- Increased deployment of automated preventive and detective controls through GRC tools
- Better understanding of impacts of controls modification through simulation analysis

Efficiency

- Use controls monitoring and testing information to satisfy diverse set of compliance requirements
- Reduction in resource-intensive manual risk management tasks through automation

Risk Intelligence

- Cross-analysis of key risks against organizational strategic imperatives

There are many benefits to investing in GRC technology, but the answer comes primarily from the objectives the organization is looking to accomplish with a GRC solution. In general, the main reasons why companies should continue to invest in GRC technology are as follows:

- Enable the business to realize the full benefits of technology enhancements in tool
- Ensure alignment of technology capabilities with risk and compliance management requirements
- Improve the agility of GRC tools to respond to regulatory changes efficiently and effectively
- Maintain quality, integrity, and reliability of GRC data
- Enhance security, auditability, and controls within GRC tools
- Prevent degradation of tool performance over time
- Enable an optimized user experience

The Evolution of GRC technology

The GRC software market emerged in the early 2000s after the fall of Enron. First-generation GRC software such as OpenPages, Paisley and Oracle ICM were the first to emerge with functionality to support automated repository for risk and control matrices, risk assessments, controls testing and monitoring all of which enabled companies to provide assurance on the effectiveness of internal controls over financial reporting for SOX compliance. At the same time, the market saw the emergence of tools like Approva, Logical Apps (which later became Oracle GRC) and Versa (which later became SAP GRC) which offered capabilities to perform automated monitoring as well as implement automated controls within financial systems.

As the GRC tools landscape started maturing towards the mid-2000s, the need for aggregated risk and compliance reporting and advanced analytics led technology solutions to incorporate business intelligence (BI) capabilities. In addition to integrated BI tools such as Oracle BI, SAP Business Objects, and IBM Cognos, we also see standalone analytics solutions that are heavily leveraged, such as Tableau, Qlikview, MicroStrategy etc.

In the last decade, organizations have become more aware of the need to integrate GRC onto a single platform. GRC software vendors like MetricStream and BWise created a modular approach to various GRC functional needs that served various GRC-related departments like risk management, compliance, legal, finance, audit, and security. However, the GRC tools market is still very fragmented with most tools having niche offerings. The responsibility for the integration of the different tool capabilities often falls on organizations.

With the growth of emerging technologies such as Robotic Process Automation (RPA) and Artificial Intelligence (AI), in the late 2010s and into the 2020s, another dimension of capabilities has been added to GRC tools. Tools like UI Path and IBM Watson are expected to be significant enablers for further GRC automation in the days to come. The growth of emerging technologies within the GRC space presents both an opportunity as well as complexity for companies to consider for GRC automation.

While these GRC solutions served the needs of the market at the time, they do not live up to the demands of the current technology landscape or the demands of auditors.

Modern-day GRC capabilities accelerate your business

Organizations that continue to use outdated GRC software face many risks, however, modern GRC solutions provide capabilities to address the challenges dynamic digital enterprises come up against allowing them to accelerate and remain competitive.

Modern GRC solutions provide rich capabilities such as:

Lower cost of ownership and scalability

SaaS solutions eliminate costs related to installing and maintaining infrastructure significantly lowering initial costs and spreading costs over time.

Improved performance

Performance issues are commonly seen with GRC software that is old and outdated specifically with respect to response and latency. Consequently, it takes longer for tasks to be completed and creates an adverse user experience. Some of the legacy GRC applications are not enabled for mobile platforms and therefore, cannot be accessed using a smartphone or tablet. Modern GRC systems, on the other hand, have much improved performances and can be securely accessed from any device, including mobile or handheld devices, which improves user adoption.

Improved usability

As time passes, there may only be a handful of employees who know how the software works, making knowledge retention more time-consuming and costly.

User productivity takes a hit as new employees do not have the expertise to use the outdated GRC software. As professionals with this know-how retire or move on, finding a fresh talent pool with this legacy knowledge is more challenging and costly. Using outdated technology fails to meet user experience expectations for new employees.

Improved integrations

Outdated GRC software frequently doesn't communicate with modern systems that require the latest integration API protocols such as JSON and SAML. Many organizations run hybrid environments. If legacy software doesn't integrate well with your identity management system to support single sign-on or data exchange to automate control evidence management from critical business systems you're missing out on the strategic advantage of modern audit practices. Internal controls over business processes need to be flexible and agile, which legacy systems can jeopardize.

Continuous enhancement and support

As GRC software vendors discontinue or downgrade support, businesses begin to experience more significant downtimes. More downtime results in a slower response to critical bugs, which cause missed audit deadlines, regulatory penalties, and operating losses from unmitigated risks.

When the vendor no longer supports GRC software, it becomes unmaintained. This means that any new bugs found aren't addressed and, in a worst-case scenario, can lead to disruptions and data loss. Businesses are under pressure to maintain continuous controls over significant business processes. If the GRC software impedes control effectiveness, a lack of trust can escalate into reputational risks. As technology increases in age, downtimes increase and become more frequent, leading to a lack of management visibility. Human malice can exploit security weaknesses with no further bug fixes, leaving your systems vulnerable to cybercriminals.

The lack of enhancements and innovations creates bottlenecks in governance, risk, and compliance processes. As businesses respond to market opportunities such as online customer relations management and remote work, legacy technologies can't be easily reconfigured to the new workflows. And this creates obstacles to valuable business drivers. The lack of enhancements to GRC software can result in missed opportunities and hidden risks that can escalate control defects, increase audit costs and result in regulatory penalties.

Advanced automation capabilities

RPA capabilities can ensure continuous monitoring and auditing of GRC operations for ongoing compliance and ensure company policies are up to date.

Considerations for GRC Technology

The first step in choosing a GRC solution for your organization is to look at the tools you are currently using. Next, you need to evaluate what your precise GRC requirements are. What do you need to achieve, and what are your overall objectives? And lastly, you need to consider your budget. Once determined you should look for the following emerging technologies in a solution.

In recent years, companies have heavily leveraged emerging technologies like RPA and ML to further improve the efficiency and effectiveness of their GRC activities. However, instead of having emerging technology solutions bolted on with GRC tools, a well-integrated solution would be more effective. Therefore, while considering GRC technology solutions, companies should also evaluate the extent to which these solutions already leverage such emerging technologies, or have the necessary integration capabilities to do so with third-party products.

Risk intelligence utilizing Machine Learning and Artificial Intelligence capabilities

Risk intelligence in GRC solutions can provide your organization with a state of the union in terms of operational and financial risks. Risk intelligence solutions help companies mine vast amounts of data and provide a cross-analysis of key risks against organizational strategic imperatives.

Automation of manual repetitive activities utilizing Robotic Process Automation (RPA

The use of RPA solutions layered on top of your GRC technologies to ramp up your business's ability to automate repetitive manual activities. These activities include controls testing, workflow capabilities, end to end, to not only have the collection of data within your technology, but also the ability to talk to other solutions this is particularly important when your organization has a mix of different systems in play. And ensuring that you have seamless data transfer between those systems. For example, the ability to coordinate notification of relevant parties. For example, if you have a late controls test, that needs to be performed, notify your testers that the issue needs to be closed by a certain time.

Workflow capabilities for seamless coordination and notification of GRC activities

Many technology vendors would say they have workflow coordination and notification capabilities. However, creating a workflow notification system is more of an art than a science. For example, having workflow capabilities is one thing, but it depends on how you define them because it could lead to an overabundance of e-mail notifications or text message alerts. It's important to get the right number of notifications.

Integration capabilities of other GRC solutions through APIs

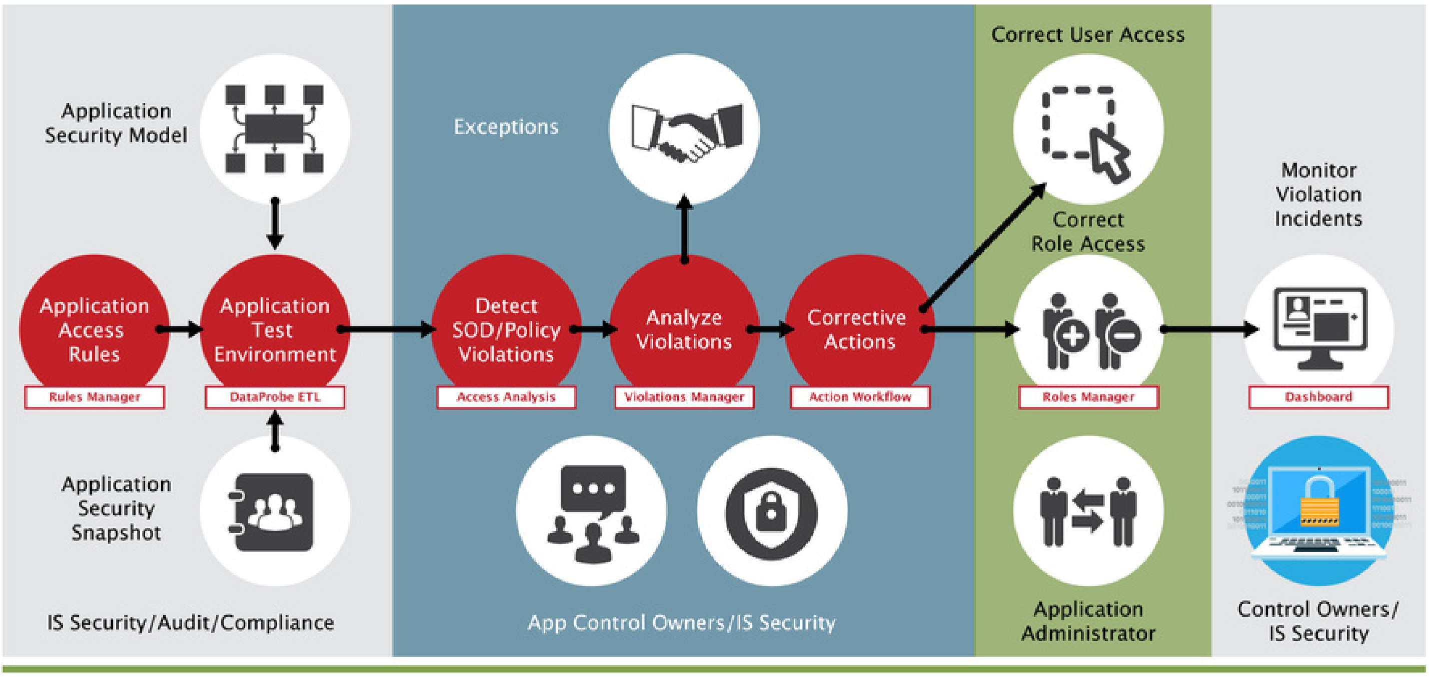
Solutions with API integration capabilities are important because they can integrate with existing and future technologies in your GRC framework. APIs provide seamless integrations into applications and can configure and extract security information. This is particularly important if your business has existing GRC applications that are fragmented across the workflow.

Extensibility of solution to adapt to different organizational needs without extensive customization

The extensibility of the solution is its ability to adapt to the different needs of the organization. For example, you can have an out-of-the-box solution that monitors your Oracle ERP for risk and controls, but what if you have a third party or custom software? Will your solution enable monitoring? A good solution will have an extensible adapter that goes into that solution and can perform the monitoring of the necessary control. The extensibility of solutions will really come into play as businesses operate in the increasingly hybrid environments of financial and operational systems.

Aggregation and analysis of risk and control data across multiple dimensions (i.e., organizational units, business processes, regulatory frameworks, risk taxonomy, etc.)

Then finally, being able to collate and aggregate data across multiple dimensions - this means organizational units and business processes. And then also your regulatory frameworks and your risk taxonomies. The ability to enable that alignment is a key capability of the GRC technology solutions to drive integrated risk and compliance management.


Application Security Model
Application Access Rules
Rules Manager
Application Test Environment
DataProbe ETL
Application Security Snapshot
IS Security/Audit/Compliance
Exceptions
Detect SOD/Policy Violations
Access Analysis
Analyze Violations
Violations Manager
Corrective Actions
Action Workflow
App Control Owners/IS Security
Correct User Access
Correct Role Access
Roles Manager
Application Administrator
Monitor Violation Incidents
Dashboard
Control Owners/ IS Security

SafePaaS makes GRC technology fully aligned with an organization's strategy by providing the agility and scalability to connect all the risks exposed to applications, whether they're in the cloud, or on-premise applications.

SafePaaS is a fully integrated GRC platform. The workflow capability (as seen here) provides a thorough configurable application security model which enables SafePaaS to support top-tier applications such as Oracle E-Business Suite, PeopleSoft, J.D. Edwards, Oracle ERP Cloud, and SAP (and others) out of the box with seamless integrations. APIs allow SafePaaS to configure (using DataProbe™ technology) and extract all the security information.

SafePaaS is a **policy-based access controls management platform** that provides a central global repository for all policy controls. In today's fast-moving business environments, looking at a report and telling someone to fix the issues is not sufficient. SafePaaS allows organizations to create a workflow that notifies approvers so they take action. The action is recorded creating a closed-loop workflow, as opposed to a simple notification.

It's not sufficient for a process owner to remove an employee's access. What auditors look for is the evidence that access is taken away. That's what can be seen here in the infographic above - where SafePaaS executes corrective actions directly in the ERP. This allows businesses to demonstrate not only what the control owner or process owner approved but the workflow can execute that in the ERP.

Contact Us

While there are many GRC solutions, the importance of having a well-defined GRC strategy and roadmap along with well-articulated business requirements cannot be undermined. To do so, many companies turn towards partnerships with trusted advisors that understand the risk and compliance domain.

RiskPro Solutions is a **trusted partner** to help your business with a solid GRC technology strategy. Leveraging extensive experience in risk and compliance management allows clients to define the optimum scope of technology implementation, set realistic milestones, and create a solution design that adds the most value.

SafePaaS is a SOC-certified cloud platform for enterprise risk management solutions, recognized by leading IT analysts and recommended by major audit firms. SafePaaS delivers a single source of truth for all Audit, Risk, and Compliance needs. **It is the single most utilized policy-based access control platform for detecting and controlling risk in enterprise applications with over 5.7 million ERP users on a single most reliable, secure, scalable platform.** The platform offers control applications, API services, and content to detect, remediate, mitigate and prevent risks to the digital enterprise. Application suites on SafePaaS include AccessPaaS™ for audit-ready reporting, access request management, privileged access monitoring, automated fulfillment, identity analytics, and workflow orchestration; MonitorPaaS™ for Configuration controls, Master Data tracking, and Transaction monitoring in ERP systems; ProcessPaaS™ to embed preventive controls in business processes; and, ARCPaaS™ to automate Audit, Risks, and Compliance Management.

Risk Pro Solutions, LLC

https://riskprosolutionsllc.com/
https://www.safepaas.com/

SafePaaS™