February 2019

TruOps Powered by SDG

Delivering Agility & Intuitiveness to IT GRC

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

©2019 GRC 20/20 Research, LLC. All Rights Reserved.

No part of this publication may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of GRC 20/20 Research, LLC. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines established in client contract.

The information contained in this publication is believed to be accurate and has been obtained from sources believed to be reliable but cannot be guaranteed and is subject to change. GRC 20/20 accepts no liability whatever for actions taken based on information that may subsequently prove to be incorrect or errors in analysis. This research contains opinions of GRC 20/20 analysts and should not be construed as statements of fact. GRC 20/20 disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. Although GRC 20/20 may include a discussion of related legal issues, GRC 20/20 does not provide legal advice or services and its research should not be construed or used as such.

Table of Contents

Complexities of IT GRC Challenge Organizations 4

TruOps Powered by SDG 6
- Delivering Agility & Intuitiveness to IT GRC 6
- What TruOps Does 7
  - *TruOps Enables IT GRC Management Processes 8*
- Benefits Organizations Have Received with TruOps 10
- Considerations in Context of TruOps 11

About GRC 20/20 Research, LLC 12

Research Methodology 12

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

©2019 GRC 20/20 Research, LLC; Redistribution Rights Granted to SDG Corp

TruOps Powered by SDG

Delivering Agility & Intuitiveness to IT GRC

Complexities of IT GRC Challenge Organizations

Organizations operate in a complex environment of risk, compliance requirements, and vulnerabilities that interweave through departments, functions, processes, technologies, roles, and relationships. What may seem as an insignificant information or technology risk in one area can have profound, cascading, and exponential impact on other risks and significant compliance ramifications. The dependency of organizations on information and technology exacerbates this problem with the interconnectedness of third parties and the Internet of Things (IoT) causing more points of exposure. Understanding and managing IT governance, risk management, and compliance (IT GRC) in today's environment requires a new paradigm in managing these interconnections and relationships of information and technology risk management.

Information security departments are scrambling to keep up with multiple initiatives that demand greater oversight of risk and compliance across the IT infrastructure, identities, processes, relationships, devices, and information. Most organizations approach these issues reactively — putting out information security fires wherever the flames are hottest. It is time for information security to step back and think strategically; to figure out how to streamline resources and use technology efficiently, effectively, and agilely to manage and monitor IT GRC across the interconnectedness of information and technology in modern business. As these pressures mount, IT often fails to think strategically as it is too busy reacting to issues and putting out fires. What gets attention is where the pain is the greatest. A reactive approach to IT risk is not only unsustainable in an environment of growing pressures, but is also a recipe for disaster, and leads to:

- Higher cost, from . . .
  - *Wasted and/or inefficient use of resources.* Silos of IT lead to wasted resources. Instead of leveraging controls and resources to meet a range of risks and compliance requirements, controls are developed haphazardly to address specific pain with no thought for leverage across risks. Organizations often try to relieve the symptoms instead of thinking how to address the root cause. IT ends up with too many different internal processes, systems, controls, and technologies 'in play' to meet individual risk and compliance needs.
  - *Unnecessary complexity.* Multiple IT risk and compliance approaches introduce complexity. With complexity comes an increase of inherent risk. Controls are impossible to streamline and manage consistently,

©2019 GRC 20/20 Research, LLC; Redistribution Rights Granted to SDG Corp

introducing more opportunities for controls to fail or go unmonitored. Inconsistent controls also produce inconsistent documentation, which further confuses IT, stakeholders, regulators, and the line of business.

- Inability to align with the business, resulting in . . .

  - *Lack of agility.* Complexity drives inflexibility. IT GRC becomes so wrapped up in spinning individual risk and compliance plates that support of the business is degraded. IT staff along, with the business, is bewildered by a maze of varying methodologies and control requirements that are not designed with any consistency or logic.

  - *Vulnerability and exposure.* A reactive approach leads to more exposure and vulnerability. Complexity means departments are focused on their own silo of risk, and no one sees the big picture. No one looks at IT GRC holistically or contextually, with regard for what is good for the business in the long run. Varying and independent efforts around IT GRC lead to difficulty demonstrating control, resulting in confusion in audits and assessments.

Not only does a reactive approach to IT GRC lead to greater vulnerability and exposure, it also means higher costs for the business. Addressing IT GRC across a series of disconnected projects and assessments leads to inefficiency in IT management and operations, wasted spending on redundant approaches, and a greater burden to the business.

IT GRC, and broader enterprise GRC management processes, have often been designed in an ivory tower, while neglecting the human factor and the conflicting priorities within groups and organizations. Organizations need to recognize that the underlying goals of protecting digital and physical assets, understanding and influencing the factors of uncertainty in desired outcomes, as well as defining, agreeing, and adhering to sensible group rules cannot be achieved in purely technocratic ways. Organizations need to look to technology that focuses on people's everyday behavior and decisions, as this has the most significant impact on achieving these goals.

The bottom line: When organizations approach IT GRC in scattered silos of documents and disconnected solutions and processes there is no possibility to be intelligent about IT GRC decisions that impact the broader organizations and its operations. Organizations need an integrated IT GRC architecture that delivers 360° contextual intelligence on IT security, risk, and compliance that provides an integrated foundation to expand and build enterprise GRC capabilities across departments.

©2019 GRC 20/20 Research, LLC; Redistribution Rights Granted to SDG Corp

TruOps Powered by SDG

Delivering Agility & Intuitiveness to IT GRC

SDG TruOps is a GRC solution that GRC 20/20 has researched, evaluated, and reviewed with organizations that are using the TruOps platform in complex, distributed, and dynamic business environments. TruOps delivers a new breed of an intuitive IT GRC solution that delivers significant business value that brings a contextual understanding of IT risk and controls within organizations.

SDG is headquartered in Norwalk, Connecticut in the United States and has over 500 employees around the world. They are an integrated IT GRC firm delivering technology, content/intelligence, and professional services to clients around the world. It is this combination of offerings that position them as high value to their clients that GRC 20/20 has interviewed. A core strength of theirs is the combination of providing professional services led by industry experts with a highly intuitive and easy to use IT GRC software solution that is cost effective to acquire and implement.

GRC 20/20's evaluation, research, and interactions with TruOps clients has determined the following:

- **Before TruOps:** Clients of TruOps typically are replacing manual processes that are encumbered by documents, spreadsheets, and emails, or outdated GRC solutions that are difficult to implement, hard to use, and did not meet the breadth of capabilities needed in the organization. Some even built their own in-house solution that did not work for them and was too costly to maintain. Such approaches can be very manual, time-consuming, and prone to errors, particularly in aggregation and reporting on data that involves hundreds to thousands of documents and spreadsheets.

- **Why TruOps:** Organizations choose TruOps as they are looking for a single integrated information and process architecture for IT GRC that is intuitive and easy to use by the front office of the organization, as well as IT security, risk, and compliance professionals in the back office. They are looking for a single information and process architecture that can handle a complex taxonomy of risks, controls, and objectives mapped to business processes and objectives. A primary reason clients choose TruOps is the solution's agile and rapid implementation timeframe over their competitors in the market. Clients state they found the solution to be rich in features, intuitive with a modern interface, easy to use, with a short implemention timeframe when compared to its' competitors and value for money. In addition, clients also stated that the people at SDG are extremely knowledgeable, consultative and easy to work with.

- **How TruOps is used:** As a new breed of GRC software that is intuitive with a modern user interface and SaaS implementation, the diversity of use cases for TruOps continues to grow. Typical use cases for TruOps clients, that GRC 20/20 has encountered, include:

©2019 GRC 20/20 Research, LLC; Redistribution Rights Granted to SDG Corp

- IT compliance and control management
- IT security management and assessments
- Cyber risk management
- Risk management
- Risk exceptions and acceptance
- IT operations
- Issue reporting and management
- Vendor risk management

- **Where TruOps has excelled:** Organizations consistently state that TruOps has improved the quality of their GRC related information and their ability to engage, interact, and report on that information. The solution is highly agile to work with in an organizations existing processes, instead of having to redo those processes to fit to the solution. This improves the organization's overall visibility into IT GRC, while eliminating the overhead of managing manual processes encumbered by hundreds to thousands of spreadsheets, documents, and emails. Clients find that the solution is flexible to adapt to their organization's management needs, has all the core capabilities needed, and provides them the ability to grow and mature their program over time to other areas of IT GRC. Overall, users find the solution intuitive and easy to use, fast to deploy, and agile to meet diverse organization and process requirements. The greatest strengths clients report of the TruOps platform are:

  - Single interface to manage policies, controls, risks, assessments and deficiencies
  - Better visibility into compliance posture by automated and real time data aggregation, analysis, reporting and dashboards
  - Ability to respond faster to internal & external threats - automated risk-based actions

What TruOps Does

GRC 20/20 has evaluated the features and capabilities of the TruOps solution set and finds that it delivers an integrated and harmonized IT GRC information and technology architecture. TruOps is a new breed of IT GRC software that is intuitive and easy to use. TruOps is a SaaS/cloud-based platform that centralizes all IT GRC data in one place that enables the organization to collaborate, manage, analyze, and report on critical controls, risks, and compliance data in real time.

In context of researching TruOps, GRC 20/20 has interviewed several TruOps clients, and finds that the solution has helped these organizations be efficient, effective, and agile in managing IT security, compliance, controls, and risks in complex and dynamic environments. It enables organizations of all industries and sizes to mature their cyber security, risk management, and compliance capabilities, and cost effectively measure maturity across the organization. TruOps helps the organization know their IT compliance requirements and to assess IT risk.

The business problem the TruOps solution addresses is the lack of automation when managing IT GRC related activities. Most organizations manage their IT risks and controls in manual processes using spreadsheets, documents, and shared folders, or with large GRC solutions that are costly to implement and maintain. This environment is inefficient and difficult to manage. Manual updates are time-consuming and complicated to manage as well. TruOps addresses this by centralizing all risk and control data within a single platform, allowing it to be managed from one central location. The TruOps information architecture allows for flexibility in reporting and provides real-time feedback in the form of dashboards and notifications tailored for management.

TruOps Enables IT GRC Management Processes

GRC 20/20 finds that TruOps is a solution that can grow and expand with the organization and adapt as the organization and its environments change. It can be easily implemented to meet simplistic IT risk and control management requirements for organizations just beginning an IT GRC management journey or implemented as the information and technology architecture core for established IT GRC management processes in the organization. It has a particularly adept way of managing the organizations structure and assets and can map authority documents and controls that are assessed through an intuitive and engaging survey engine.

TruOps is designed to make IT GRC management processes efficient, effective, and agile in a dynamic business environment. To achieve this, the core IT GRC management processes that TruOps automates and manages are:

- **IT Security Management.** TruOps allows the organization to define, model, manage, and monitor IT security to the organizations processes and assets. The integration with an organization's IT security ecosystem brings real time visibility into cybersecurity threats & vulnerability, and continuous control monitoring significantly reduces manual effort of control assessments.

- **IT Compliance Management.** TruOps allows organizations to manage and monitor IT compliance to obligations (e.g., regulations) through control registers, assessments, metrics/indicators, reporting, checklists, and surveys/questionnaires. This includes pre-built controls & assessment templates (PCI, ISO 27001, GDPR and more).

- **IT Risk Management.** TruOps allows organizations to manage IT risk within context of IT objectives, processes, and assets, as well as manage corresponding risk appetite, metrics/indicators, risk registers, assessments, reporting, and scenarios.

©2019 GRC 20/20 Research, LLC; Redistribution Rights Granted to SDG Corp

- **IT Issue Reporting & Incident/Case Management.** TruOps enables the organization to provide an enterprise view of IT incidents and issues with detailed information on operational loss, near risk events, root cause analysis, and metrics/indicators.

- **Vendor/Third Party Risk Management.** TruOps enables the management and ongoing security due-diligence in and across an organizations third party relationships to ensure that these relationships mitigate exposure and vulnerability to the organizations systems and data.

TruOps ability to manage IT GRC across areas and organizational contexts is delivered through the capabilities in the solution's technology architecture. These core capabilities include:

- **Organization management.** TruOps defines, models, and interconnects organizational processes, assets, and IT GRC object libraries to represent organizational realities to simulate incidents, risks, and impacts.

- **IT Risk and control libraries.** TruOps has a robust information architecture that details IT risk and control libraries and allows objects to be cross-referenced to each other to provide contextual insight and awareness. TruOps further provides content for these libraries that organizations can leverage, adapt, and expand for their own specific requirements through their relationship with UCF.

- **Workflow and task management.** TruOps manages workflow and related tasks, and ensures things are completed when they need to be completed. It has built-in escalation capabilities when milestones are near or missed.

- **Dashboards and reporting.** TruOps delivers pre-built granular and high-level reports and dashboards, as well as the ability to support ad hoc reporting and customization.

- **Assessments.** TruOps has full survey and scalable assessment functionality to build questionnaires and assessments, as well as to gather information to assess risk, internal controls, and conduct audits.

- **System of record.** TruOps traces and records all actions and activities across the solution, so an organization has a complete system of record and audit trail of what was done, by whom, and when. This provides the ability to defend the organization and deliver evidence of compliance and control through complete traceability of actions.

- **Mobility.** TruOps has a modern and responsive interface design that allows it to be used on any device with a modern web browser interface.

- **Configurability.** TruOps is configurable and adaptable to meet an organization's specific requirements. No coding or programming is needed and therefore supports fast deployment and speed to value. The solution can be modified by

the customer to meet the needs of the variety of IT GRC management functions within an organization.

Being an agile SaaS/cloud platform, TruOps is continually adding new functionality. In early 2019 they expect to have IT policy management available to facilitate the management, communication, acceptance, and maintenance of the breadth of an organizations IT policies and procedures.

Benefits Organizations Have Received with TruOps

Most TruOps clients that GRC 20/20 has researched and interviewed moved to the solution because they found their manual document-centric approaches consumed too many management resources, and they found things were slipping through cracks in the continuous barrage of IT GRC management - as well as regulatory and business change. Others move to the solution as they found their previous solution was too cumbersome and expensive to maintain and own. Across these clients, there is consistent praise for the value of TruOps in context of the ongoing cost of ownership, the speed of deployment, return on investment, improved effectiveness, and agility to reliably achieve objectives while reducing uncertainty and risk.

Specific benefits that clients of TruOps have told GRC 20/20 they have achieved in their implementations are:

- *360° visibility into IT risk and control* where all information is in one place and gives complete situational and contextual awareness of risk and controls in context of objectives and processes.
- *Elimination of hundreds to thousands of documents, spreadsheets, and emails,* and the time needed to monitor, gather, and report on them to manage related activities and processes.
- *Significant efficiencies in time through automation* of workflow and tasks as well as reporting. Specifically, the time it took to build reports from hundreds to thousands of documents and spreadsheets now is just a matter of seconds.
- *Less things slipping through cracks* as there are established tasks, notifications, and escalation when things are approaching or are past due.
- *Time efficiency in streamlining processes* through identification of requirements, accountability, tracking, getting things done.
- *Greater granularity and ability to report* on specific IT risk and control details that could not be done in spreadsheets.
- *Increased awareness and accountability* of risk and controls by business owners who are informed on risk and controls in context of their role.

©2019 GRC 20/20 Research, LLC; Redistribution Rights Granted to SDG Corp

- *Consistency and accuracy of information* as the organization conforms to consistent processes and information structures. It has increased quality of IT GRC related information that is more reliable and improves decision making.

- *Accountability with full audit trails* of who did what and when; this particularly has delivered value in fewer things slipping through the cracks.

- *Reduction in time needed to govern and manage IT GRC* that are freed from manual processes; these resources can then focus on value added activities. One organization reported that their assessment process went down from four weeks to less than one, while another went from twelve weeks to six.

- *Increased agility in context of change* that enables the organization to be proactive, and not just reactive, leading to less exposure and being caught off-guard.

Considerations in Context of TruOps

Every solution has its strengths and weaknesses and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of TruOps to enable organizations to achieve consistent IT GRC processes, readers should not see this as a complete and unquestionable endorsement of SDG or the TruOps platform.

GRC 20/20, in interacting with current TruOps clients, finds that the solution continues to exceed expectations, and the company has met upgrade and enhancement promises they have committed to. Clients find TruOps to be extraordinarily responsive to issues and requests, as well as comprehensive in addressing them. They particularly enjoy the SaaS architecture which eases implementation and maintenance updates.

An area in which TruOps clients have reported they would like to see the solution improved is to enable a stronger workflow capability, and separate the risk and issue management into separate, but still related, modules. Clients would also like to see improvement on TruOps ability to export data to business intelligence tools for further analytics and reporting.

Overall, clients have shown a high degree of satisfaction with their use and implementation of TruOps and find the organization to be agile and responsive to their issues and needs. Clients praise TruOps for the ease of use and intuitiveness of the solution. They find that the solution is agile by allowing distributed management and business functions to get what they need when they need it.

©2019 GRC 20/20 Research, LLC; Redistribution Rights Granted to SDG Corp

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com