SureCloud®

A White Paper That Unveils the Secrets of Taming the Monstrous Problem of Third-Party Risk

Alex Hollis,
GRC Solutions Director at SureCloud

WHITEPAPER

Overview

Data breaches are a growing problem; since 2005, over 10 billion consumer records have been compromised. For large enterprises, each data breach can result in lost revenue of £1.3m.

One of the main culprits of data breaches are third-parties that organizations engage to perform key functions within the business. It's the weaknesses within their infrastructure, and the services they provide, that can often leave you vulnerable.

During the last 12 years, we've helped over 400 customers, 10% of which are in the FTSE 100, with their risk management programs. We've discovered that organizations that implement a comprehensive 'Third-party Risk Management Program', which follows the following 7 best-practice models, experience the most success and tame the monstrous problem of third-party risk:

- Maintain a comprehensive list of all third parties, large and small.
- Complete a risk register that is regularly updated.
- Always take a risk-based approach.
- Maintain disciplined governance.
- Select integration into inertial GRC.
- Be proactive with continual assessment and monitoring.
- Leverage the power of technology.

Data breach:

> **“ An incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve payment card information, personal health information, personally identifiable information, trade secrets, or intellectual property.**
>
> TechTarget

Trusted by Companies around the world:

JUST EAT · Dixons Carphone · Everton 1878 NIL SATIS NISI OPTIMUM · TGI FRIDAYS · Thames Water · SHOP DIRECT

Overview

Once upon a time, hearing about a data breach would have been shocking, but unfortunately, in today's world they're commonplace in our headlines. Privacy Rights Clearinghouse is a not-for-profit organization that reports on data breaches impacting consumers. Back in 2005, when it started maintaining its chronology of information, 136 breaches, affecting 55,101,241 records were recorded; last year, this exploded to 7,934 breaches that have been made public, affecting 10,082,217,317 records.

Besides the negative press attention, data breaches can have a huge impact on your organization:

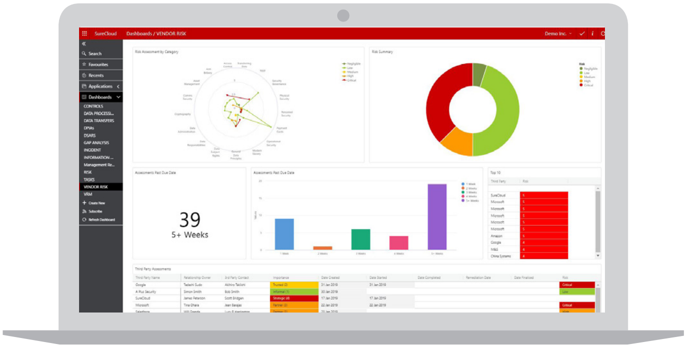
- 40% of organizations experiencing a breach lose customers.
- 29% lose revenue.
- 23% lose business opportunities.

According to PwC, more than a quarter of businesses (28%) don't know how many breaches they've experienced, and a third have no idea how they happened. It's worrying, yet understandable when you consider how heavily reliant we're becoming on engaging third-parties to perform key functions within our businesses; research suggests that third-parties now represent 60% of revenue.

The problem lies in vulnerabilities within a third-party's infrastructure and the services they provide. And the risks presented to both the organization and the end customer only mount with each additional party involved. The chains involved industries can stretch beyond the first, second, and third (customer, the organization, immediate suppliers) into fourth and fifth (suppliers of the suppliers of suppliers). It's no wonder that this mind-bending complexity becomes so easy for risks to permeate. Furthermore, with consumers' trust eroding more with every breach, it's forcing governments to tighten their regulatory control in making organizations more accountable.

> **“ Incidents affecting infrastructure hosted by third-parties, cost small businesses £106,000 on average, while large enterprises lose nearly £1.3m.**
>
> **Kaspersky Lab**

Sources
Cisco Security Survey, ITPRO, PWC, Deloitte



Third Party	Risk
SureCloud	5
Microsoft	5
Microsoft	5
Microsoft	5
Microsoft	5
Microsoft	5
Amazon	5
Google	4
M&S	4
China Systems	4

Third Party Name	Relationship Owner	3rd Party Contact	Importance	Date Created	Date Started	Date Completed	Remediation Date	Date Finalised	Risk
Google	Tadashi Sudo	Akihiro Takishi	Trusted (2)	31 Jan 2019	31 Jan 2019				Critical
A Plus Security	Simon Smith	Bob Smith	Informal (1)	30 Jan 2019					Low
SureCloud	James Peterson	Scott Bridgen	Strategic (4)	17 Jan 2019	17 Jan 2019				
Microsoft	Tina Ohara	Jean Barajas	Partner (3)	22 Jan 2019	22 Jan 2019				Critical

Implement a Third-party Risk Management Program

So what can you do to control your third-parties and protect your organization?

With a growing number of data breaches and increasing spotlight on third-party risk from regulatory bodies, there's never been a greater need for a 'Third-party Risk Management Program'.

By monitoring and managing interactions with your third-parties, you can increase visibility of their actions, deepen your understanding of their movements and implement robust processes to mitigate any risk. These third-parties may include contractual and non-contractual parties such as suppliers, vendors, contract manufacturers, business partners, affiliates, brokers, distributors, resellers and agents. And don't be fooled into thinking that the size of the organization matters; always keep in mind the activities, level of access to sensitive data or property, the maturity of compliance and risk programs, and accountability for fourth parties.

Target lost 40m records through its HVAC contractor:

Like many organizations, US retailer Target's heating, ventilation, and air conditioning (HVAC) system connects to the Internet, which allows it's HVAC contractor to carry out tasks like remotely monitoring energy consumption and temperatures at different outlets. By exploiting the vulnerability of this small third-party contractor, hackers were able to steal the login credentials and gain a foothold in Target's payment systems. The retailer lost data on 40 million credit and debit cards, as well as exposing the control systems for other companies that Target connects to.

Implement a Third-party Risk Management Program

1. Maintain a comprehensive list of all third-parties, large and small

Sounds easy, but what if you're working with 50,000 third-parties? It's rare to find an organization that maintains a complete list, which is unfortunate, because much of the risk tends to lie with those who are forgotten. The key to success is not thinking of this as a task that must be finished, but to view it as an ongoing process that becomes more accurate as you apply structured effort.

Start by agreeing the data that needs to be captured, so you maintain consistency in your records. For example:

- Name (full business name, avoiding product names or acronyms)
- Internal owner of the relationship
- Type – this will be an evolving categorization but should start off identifying upstream and downstream (suppliers / resellers)
- External contact(s)

Start with your suppliers (upstream). It's likely that your procurement or finance team will have existing lists you can build on. Then review open POs and investigate the outgoing payments for smaller suppliers who may be paid on a more ad hoc basis.

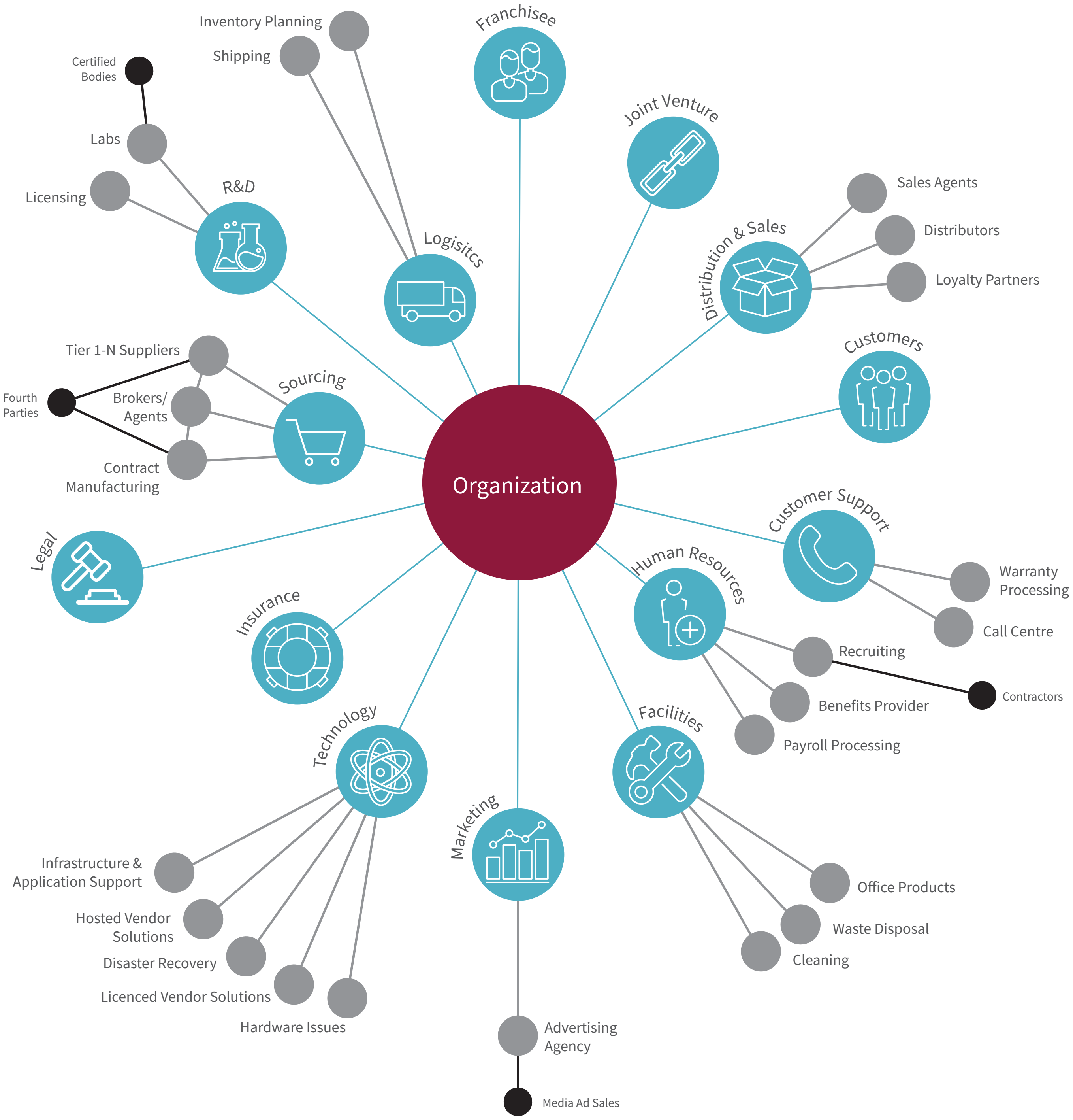
Next, speak to each department in your organization to understand if they have a dependency on any third-parties. Consider outsourced processes or functions, software, support, contractors or services.

Now consider your distributors, resellers and partners (downstream). If you have partner managers they should be able to provide a list to you, and again, leverage financial data or teams to identify large regular orders made to the organization.

Having a flat complete list of consistent data is a key maturity milestone and a good initial goal. For organizations who have already reached this stage the next step is to understand the deeper relationships.

Third-parties are rarely flat; often you will be engaging different departments from an organization for different purposes, for example, procuring software and services from an organization, which have been procured and negotiated separately. Noting these relationships is beneficial to understanding risk and compliance, but also when negotiating contractual renewals.

Beyond the complexity that exists within a single company, you then have to consider the suppliers of suppliers, or "fourth parties". Don't be naive and think you can ignore them as you don't deal with them directly; there are numerous examples of risk events and incidents occurring through fourth parties, where accidents or deliberate attacks have exploited vulnerabilities in smaller organizations to undermine the large enterprises. In addition, you may find that shared fourth parties undermine any diversification strategy, so as your program matures you should keep sight of the wider environment you operate in.


Organization
Franchisee
Joint Venture
Distribution & Sales
Sales Agents
Distributors
Loyalty Partners
Customers
Customer Support
Warranty Processing
Call Centre
Human Resources
Recruiting
Contractors
Benefits Provider
Payroll Processing
Facilities
Office Products
Waste Disposal
Cleaning
Marketing
Advertising Agency
Media Ad Sales
Technology
Infrastructure & Application Support
Hosted Vendor Solutions
Disaster Recovery
Licenced Vendor Solutions
Hardware Issues
Insurance
Legal
Sourcing
Tier 1-N Suppliers
Brokers/ Agents
Contract Manufacturing
Fourth Parties
R&D
Licensing
Labs
Certified Bodies
Logisitcs
Shipping
Inventory Planning

Implement a Third-party Risk Management Program

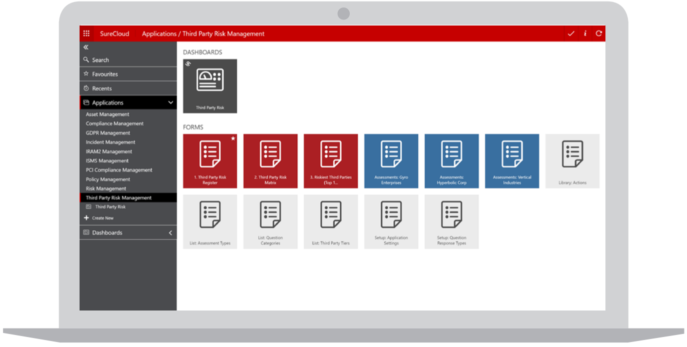
2. Maintain a risk register and updated regularly

A list of potential incidents that can impact your organization, the risk register exists to try and protect you. By assessing each risk, you can determine its impact, and if necessary, take appropriate action, such as implementing mitigating controls, transferring the risk to a third-party through outsourcing or insurance, or outright avoiding the risk.

As part of your management program, third-party risks should be added to the risk register as part of the business units' own risk and control assessments. Just because a third-party is being leveraged does not remove or affect the management of the risk.

Mitigating actions, such as controls and transfer, should not be ignored but rather identified and managed. Third-party risks may be mitigated by using a diversification strategy, which could mean accepting a secondary competitive party at a different price point or losing discounts of scale. The costs of diversification can be considered as the cost of control in mitigating the risk. Consider diversifying with additional risk factors, such as geographic location when choosing.

Furthermore, these risks should factor into the risk assessment sent to the third-party.


SureCloud
Applications / Third Party Risk Management
Search
Favourites
Recents
Applications
Asset Management
Compliance Management
GDPR Management
Incident Management
IRAM2 Management
ISMS Management
PCI Compliance Management
Policy Management
Risk Management
Third Party Risk Management
Third Party Risk
Create New
Dashboards
DASHBOARDS
Third Party Risk
FORMS
1. Third Party Risk Register
2. Third Party Risk Matrix
3. Riskiest Third Parties (Top 1...
Assessments: Gyro Enterprises
Assessments: Hyperbolic Corp
Assessments: Vertical Industries
Library: Actions
List: Assessment Types
List: Question Categories
List: Third Party Tiers
Setup: Application Settings
Setup: Question Response Types

The horsemeat scandal:

Possibly the biggest food fraud of the 21st century, 'The horsemeat scandal' in 2013 led to the withdrawal of tens of millions of burgers and beef products across Europe, from retail giants including Tesco, Burger King, Co-op and Aldi. During the ensuing investigations, the horrifying supply chain exposed drug and horse smuggling, animal welfare abuses and mislabelling; according to the Irish department of agriculture, the factory that supplied Tesco with its 'beef burgers' (containing 29% horsemeat), was using "multiple ingredients from some 40 suppliers in production batches, and the mixture could vary in every half-hour."

Implement a Third-party Risk Management Program

3. Always take a risk-based approach

There are broadly two approaches to performing a risk-based assessment:

- Score-based assessments ask questions in order to carry out diligence across all dimensions, which results in a score that can then be reviewed and understood.
- Scope-based assessments use a set of criteria, such as the financial scale of the relationship (income or expenditure), the nature of the services provided, strategic relevance, reputational impacts, appropriate regulations, and operating country, to create the scope. Determined by an internal owner, the resulting scope-based assessment can reduce the number of questions on the average assessment by 40-60% over pure score-based assessments.

'Assessment fatigue' is a term used in medicine to refer to the fatigue felt by patients who undergo numerous clinical tests. Within third-party assessments I have borrowed the term to describe the fatigue that third-parties feel from answering very large and often complex questionnaires. The attention of the person completing your assessment is finite. For each question asked, the level of attention, and detail given, is going to reduce. This 'assessment fatigue' can lead to a drop in the quality and detail of answers given, so assessments need to spend the level of attention wisely.

Once the data is gathered from the assessments, it should be reviewed based on the severity of the risks highlighted by the answers. You should establish a level at which you will accept assessments that do not highlight any risk. This could be for medium to low-risk third-party annual assessments. This automatically accepted list should include appropriate spot check or sampling method to provide diligence for any errors or omissions.

Implement a Third-party Risk Management Program

4. Maintain disciplined governance

As with any good process, it must be followed and those involved must be given the appropriate decision-making powers. On paper, most people within an organization will agree, however, when faced with the challenges of procuring new services and the costs of the various solutions, the detail of the third-party assessments is often an area that is easily overridden.

Giving authority and decision-making power to block or ban a particular third-party based on unacceptable exposure to risk, should be respected by all involved and not automatically overridden by any executive mandate.

This exercise should not be viewed as a purely hypothetical risk mitigation exercise.

Increasingly, the regulatory focus is on looking at how organizations manage their relationships with other agents. The regulator's goal is to ensure the consumer is protected and newer regulations, such as GDPR, are more focused on the rights and freedoms of the individual. New governance must ensure there is a consideration for the individual.

5. Choose an Integrated GRC Programme

Most organizations deal with each aspect of governance, risk and compliance in silos. Teams will use people, process and technology that is specific to their requirements, within their particular GRC niche. But while this serves the purposes of the team, it is short-sighted, and often causes those outside the function, the additional pain having to complete the same data multiple times or having to consume and update different outputs.

As an organization matures it becomes clear that there are advantages to be had in a connected approach. Each team can maintain some separation with data capture and workflow, but the overall aggregation and interrelation is consistent. For example, third-party risk details can be made available from risks when considering transferring, or outsourcing processes, to reduce exposure to risks. This information might lead a business owner to reconsider whether this form of mitigation is appropriate.

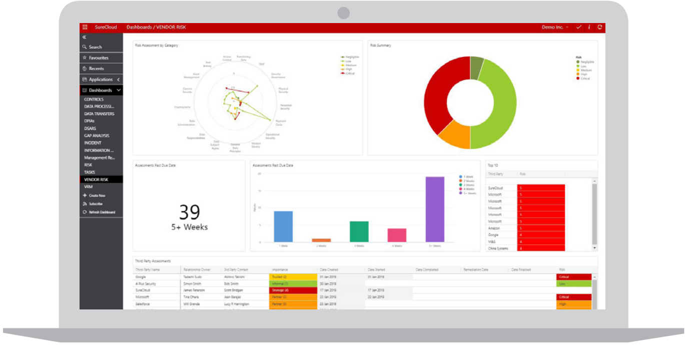
> **“ Research shows that there is an ROI of 4%-6% through competitive advantage for a properly implemented and controlled Third-party Risk Management Program.**
>
> Deloitte

Implement a Third-party Risk Management Program

6. Be proactive with continual assessment and monitoring

The annual, or six-monthly cycle has its place, and while sending and receiving a set of designed questions is useful, it will not catch everything. Successful Third-party Risk Management Programs contain:

- Regular assessments.
- Include out of cycle activities to monitor and review third-parties.
- Follow up on remedial actions to implement any mitigating controls.
- Review incident data, whether internal, third-party or external, to provide insight into potential weaknesses and highlight tasks and activities that need to be tracked.



Third Party	Risk
SureCloud	5
Microsoft	5
Microsoft	5
Microsoft	5
Microsoft	5
Microsoft	5
Amazon	5
Google	4
M&S	4
China Systems	4

Third Party Assessments

Third Party Name	Relationship Owner	3rd Party Contact	Importance	Date Created	Date Started	Date Completed	Remediation Date	Date Finalised	Risk
Google	Tadashi Sudo	Akihiro Takishi	Trusted (2)	31 Jan 2019	31 Jan 2019				Critical
A Plus Security	Simon Smith	Bob Smith	Informal (1)	30 Jan 2019					Low
SureCloud	James Peterson	Scott Bridgen	Strategic (4)	17 Jan 2019	17 Jan 2019				
Microsoft	Tina Chara	Jean Barajas	Partner (3)	22 Jan 2019	22 Jan 2019				Critical
Salesforce	Will Grenda	Lucy R Harrington	Partner (3)	23 Jan 2019					High

7. Leverage the power of technology

Once you have the right people and the right processes, you need the right technology to accelerate everything. Most organizations start by using Excel to model out their desired systems. This 40-year old technology is excellent for building a temporary model of the system, but often few make a plan to move from it. Instead as the system grows with multiple users, workflows and interdependencies, the more Excel shows that it is not the right tool for the job.

Third-party risk management has the added challenge of requiring external users to provide assessment data and updates to actions on an ongoing basis. In most organizations, this is achieved by sending Excel documents back and forth over email, which floods inboxes, and creates an auditing/versioning nightmare.

A better approach is to start early, reviewing GRC technologies to understand the common models. Even if you cannot prove a business case now, by incorporating some of these models and concepts into the Excel sheets that you create, you can set yourself up for a smoother transition in the future. If you have started to feel the pains of out-growing Excel spreadsheets, it's time to consider moving to a GRC technology. Most providers will have pricing models that allow you to scale the solution, gaining the benefits incrementally.

Introducing SureCloud Third-party Risk Manager

Designed to streamline third-party risk management, our cloud-based application automates, simplifies and puts you in control of your Third-party Risk Management Program. Over 400 companies worldwide trust SureCloud Third-party Risk Manager to:

- Gain control and certainty over their network of vendors.
- Eliminate risk-heavy processes by eliminating spreadsheet/ email-driven programs.
- Adopt best-in-class structure using best-practice risk-based methodologies.
- Get everyone on the same page by creating a single version of the truth.
- Be smarter and faster through real-time analytics.
- Create process templates and common controls, which are instantly available to third-parties.
- Implement a central structure with improved visibility of all assessments.
- Automated data aggregation across the entire program.
- Benefit from flexible reporting through pre-configured best-practice charts and tables.
- Automated task allocation for each assessment.

> **“ SureCloud’s real-time dashboard provides an instant view of where we are with data compliance. The responses given by our partners will determine which suppliers we should focus more on. And with a few clicks, we can produce reports such as our 10 most high-risk suppliers.**
>
> Shop Direct

Book your demo

If you’re ready to tame the monstrous problem of third-party risk by simplifying, automating and controlling your Third-party Risk Management Program, it’s time to book your demo of SureCloud Third-party Risk Manager:

Email: sales@surecloud.com

Start your Third Party project today.

SureCloud®

SureCloud is a provider of cloud-based, integrated Risk Management products and Cybersecurity services, which reinvent the way you manage risk. SureCloud is underpinned by a highly configurable technology platform, which is simple, intuitive and flexible. Unlike other GRC Platform providers, SureCloud is adaptable enough to fit your current business processes without forcing you to make concessions during implementation; meaning you get immediate and sustained value from the outset.

www.surecloud.com

Corporate Headquarters
SureCloud Limited.
10 Brick Street, Mayfair, London,
W1J 7DF UK +44 208-012-8544

SureCloud Inc.
6010 W Spring Creek Pkwy
Plano, TX 75024
United States of America

Phone: +1 (972) 996-6989

sales@surecloud.com