Risk Q

CYBER RISK & PRIVACY MANAGEMENT

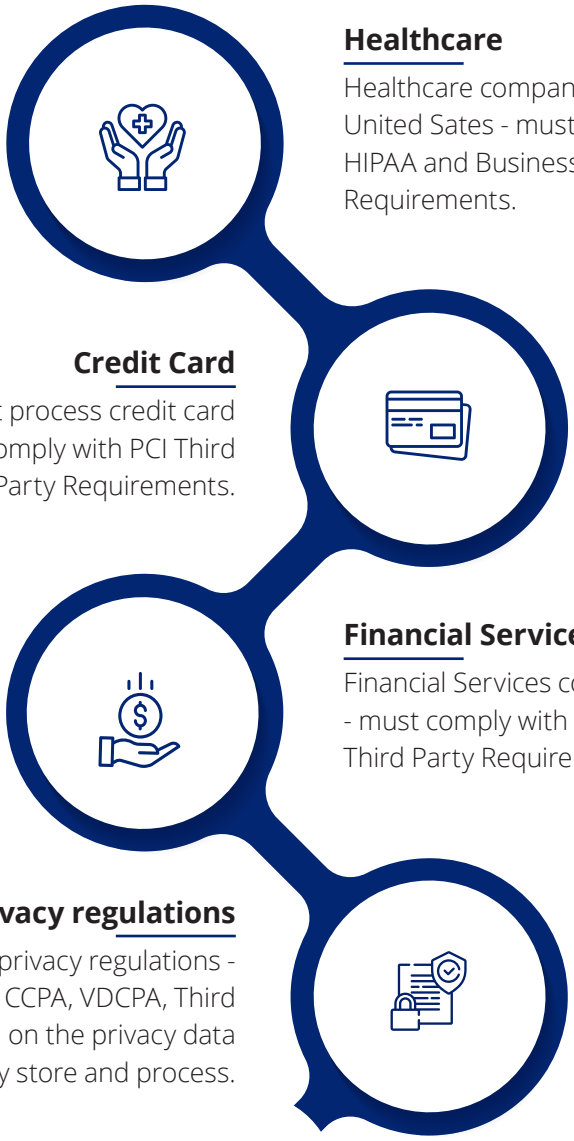
Highly Automated Third Party Cyber Risk Management (TPCRM) Compliance

www.risk-q.com

email
info@risk-q.com

Who does TPCRM affect?

Any business is expected to comply with a TPCRM program if they meet any of the following criteria below:



Healthcare

Healthcare companies in the United Sates - must comply with HIPAA and Business Associate Requirements.

Credit Card

Companies that process credit card data - must comply with PCI Third Party Requirements.

Financial Services

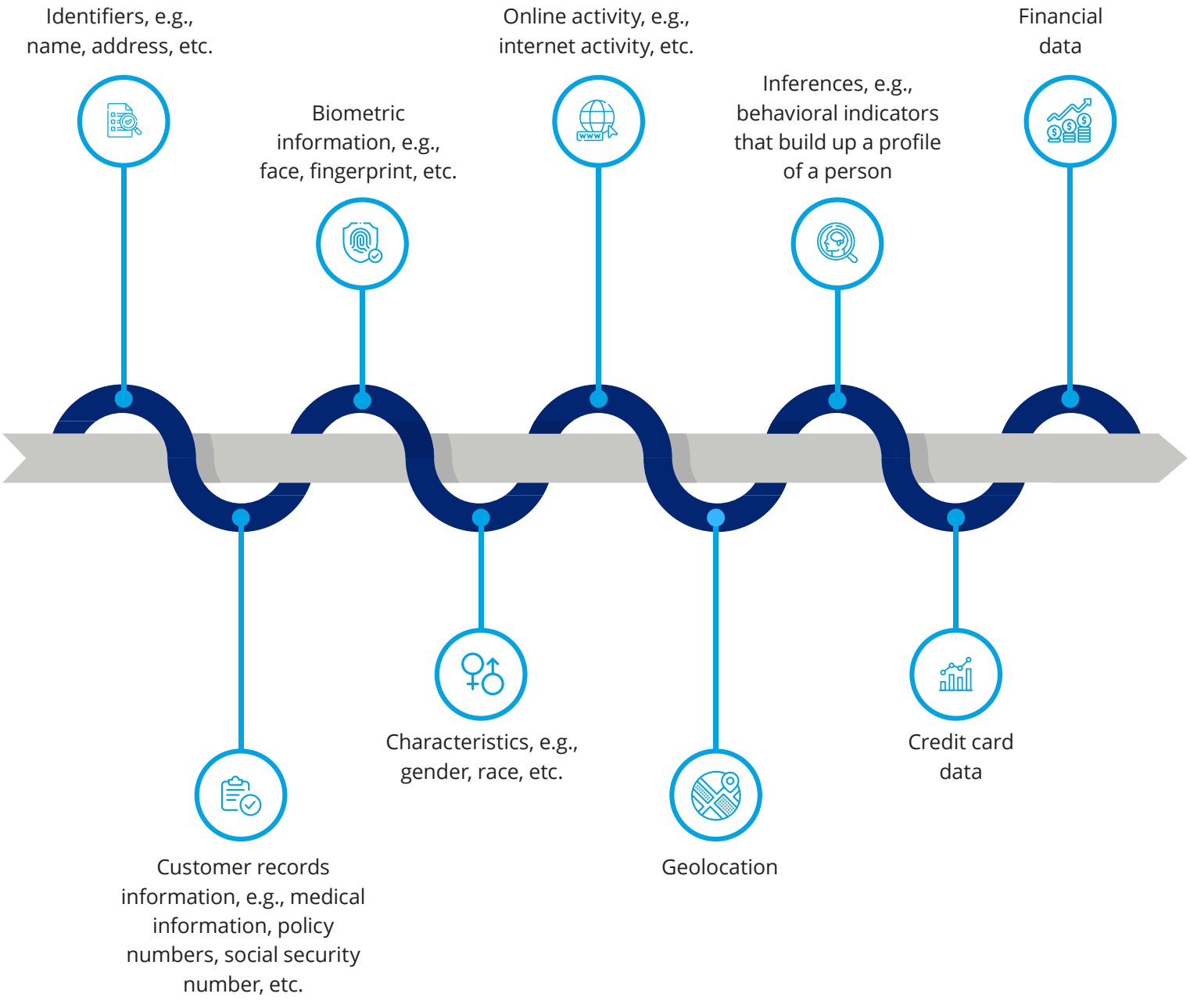
Financial Services companies in NYS - must comply with NYSDFS Part 500 Third Party Requirements.

Privacy regulations

Companies in scope for privacy regulations - must comply with GDPR, CCPA, VDCPA, Third Party Requirements based on the privacy data they store and process.

What types of data put you in scope for TPCRM?

The categories of personal information outlined in the CCPA are wide and include:



Our Automated TPCRM Software

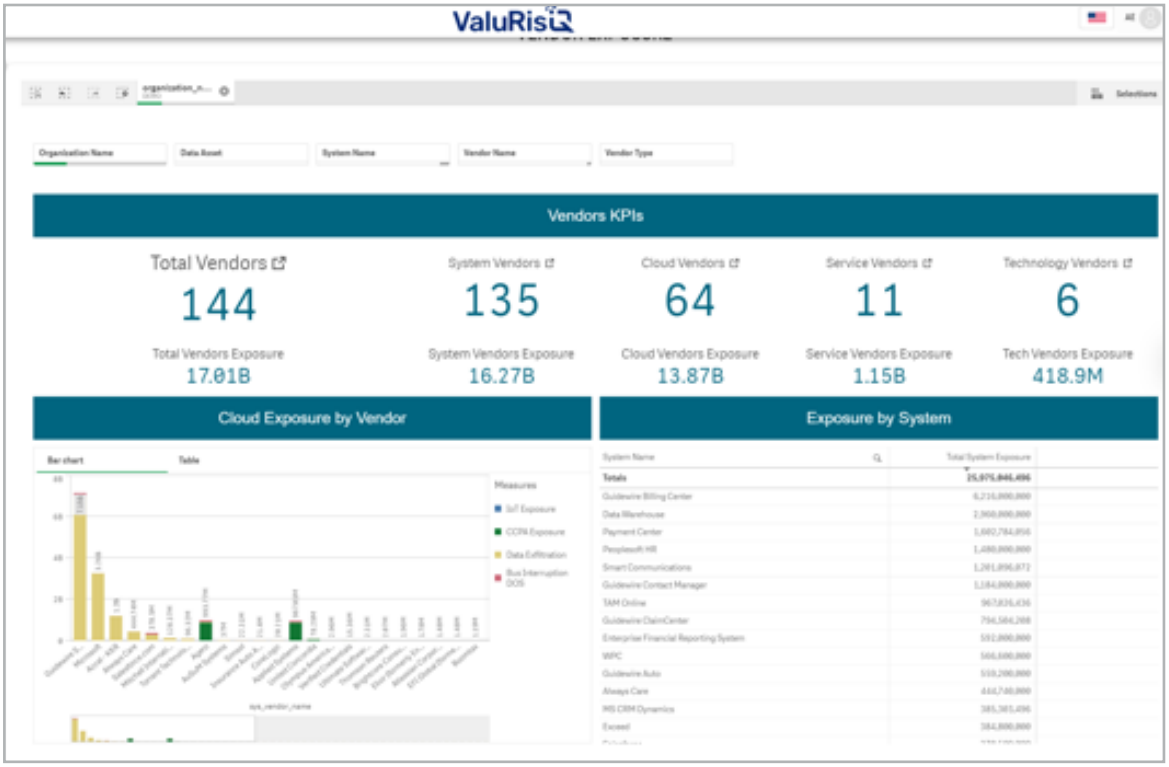
Our software provides an automated approach to

TPCRM Compliance Step 1: Determine the Scope, Quantify Third Party Cyber Exposure and Prioritize

Determine if you must comply, the # of vendors to be assessed and their priority based on financial exposures.

Fines

Assessment prioritization is based on fines. Fines range from $100 for each record lost up to 4% of annual revenue based on the regulatory scope. Our cyber risk engine provides financial quantifications of third party cyber exposures.



ValuRisQ Third Party Financial Exposures

It is also worth noting that consumers could also sue an organization for third party mismanagement and non-compliance and class-action lawsuits could be used.

TPCRM Compliance Step 2: Create your Vendor Requirements

Using cybersecurity frameworks and requirements aligned to vendor type, create the required evidence for each requirement using our out of the box frameworks.

Security Requirements

Risk assessments are required which use a set of cybersecurity control tests. We allow the company to choose any including but not limited to:

- NIST Cybersecurity Framework
- CIS Top 20 Framework
- ISO 27001 Framework
- Payment Card Industry Data Security Standard

TPCRM Compliance Step 3: Third Party Cyber Risk Assessments

Enable your vendors to provide evidence for the risk assessment based on vendor type and regulation requirements.

ValuRisQ Security Assessment & Vendor Risk Assessments

Third party contracts and the supply chain

The firm must consider their relationships as service providers with larger organizations and reflect the situation vis-à-vis regulatory requirements in their business contracts to help govern relationships with customers. It is vital to identify third parties involved in data processing, for example, payment processing vendors. These relationships must be defined within contracts.

TPCRM Compliance Step 4: Third Party Contract Review

RiskQ allows contracts to be uploaded and reviewed in an automated workflow for each vendor, procurement, legal and IT teams.

Knowing your vendor financial exposure is key. RiskQ shows you how much exposure each vendor has and identifies the gaps in their cybersecurity program.

Report, Communicate and Act – using our state of the art dashboards and workflows.

TPCRM Compliance Step 5: Report, Communicate and Act

Approve policies and procedures with our workflows, communicate risk in our dashboards and allow the vendor to provide you evidence with our state-of-the-at platform.

Automated TPCRM Compliance

We connect to your systems and technologies on AWS and automatically identify which systems are in scope for TPCRM. This saves our customers tens of thousands of dollars in resource time while providing a higher level of confidence about the data. Our risk models are based on five years' worth of research and are taught at Universities across the U.S.

Why RiskQ

RiskQ uses an automated digital asset approach to measure financial exposures and assess cyber risk. This provides clients with objective financial data and eliminates up to 90% of the manual work by untrained personnel to perform the assessment. Clients are provided regulatory requirements/scope, policies, procedures, and automated risk assessments to be compliant with all applicable cybersecurity and privacy regulations. Our platform provides an integrated solution that is powerful, easy to use and offers the lowest total cost of ownership. In 5 simple steps you can be complaint with any cybersecurity or privacy regulation.

1. Determine the Scope, Quantify Third Party Cyber Exposure and Prioritize
2. Create your Vendor Requirements
3. Third Party Cyber Risk Assessments
4. Third Party Contract Review
5. Report, Communicate and Act

About RiskQ

Based on five years of research with the Fortune 1000 and cyber insurance industry and from some of the sharpest cybersecurity and risk minds in Israel and the United States. RiskQ provides the ultimate in data loss prevention and risk management by identifying hidden exposures and making sure the attack surface is minimized and the digital assets have effective protection in place. RiskQ fundamentally alters the cybersecurity risk landscape with its digital asset approach and integrated risk platform. Get our book 'Enterprise Cybersecurity in Digital Business' free with your purchase of our TPCRM offering.

RiskQ

RiskQ
66 West Flagler Street - Suite 900, Miami, FL 33130
email: info@risk-q.com
www.risk-q.com