VIRTUAL GUARDIAN

Third Party Risk Assessment

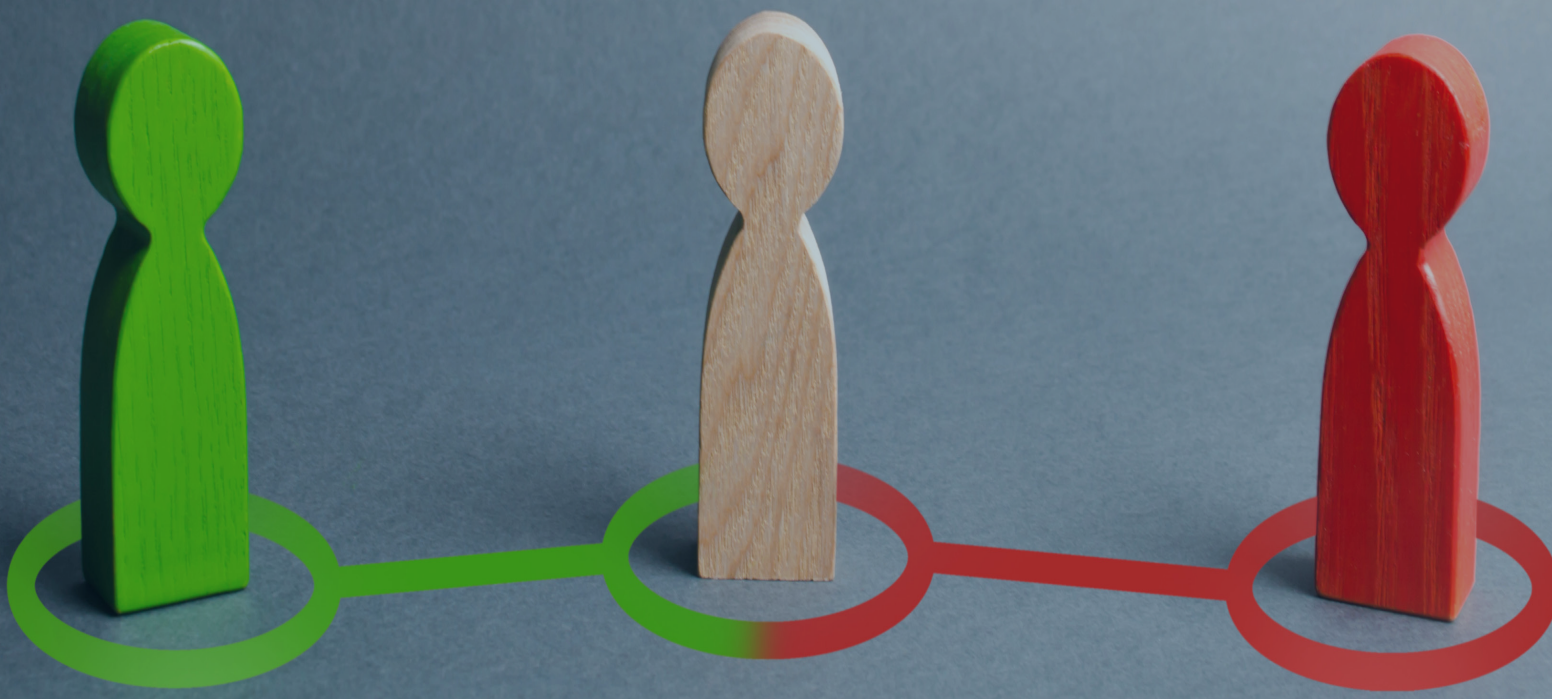
3rd Party Risk.

Is your attack surface expanding?

Third-party risk management is increasingly crucial in today's cybersecurity landscape due to the expanding reliance on external vendors and service providers, amplifying the potential for data loss and security vulnerabilities. With organizations outsourcing various functions to third parties, the attack surface widens, exposing them to diverse risks.

The protection of your sensitive data and business continuity are our prime concerns, as third parties often handle or have access to valuable information or critical processes. Moreover, regulations like the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), among others, heighten the stakes for organizations. Non-compliance with these regulations not only incurs legal repercussions but also jeopardizes the trust and privacy of stakeholders.

As the number of providers grows, so does the complexity of managing these relationships, making it challenging to ensure uniform security standards across the supply chain. The Virtual Guardian TPRM assessment service provides a tailored offering to your organization's vendor risk management needs.



TPRM assessment at your service.

Our data-driven approach helps you identify and manage third-party risks efficiently, ensuring compliance with industry standards and regulations. We understand the importance of freeing up your employees' time. We will handle the busy work of the assessment process, allowing your team to focus on core tasks. Our goal is to become your trusted partner in managing risks, ensuring confidence and strengthening your organization's security.

Virtual Guardian TPRM Assessment Steps

- **Initiation** - Client provides assessment request to Virtual Guardian which includes vendor(s) to be assessed

- **Response Tracking** - Track Vendor responses. Virtual Guardian will follow up with any non-responsive Vendors using a defined escalation process.

- **Evaluation**

  Analyze responses and additional attachments if requested
  Follow up on inadequate vendor responses
  Analyze SecurityScorecard Atlas information with assessment responses
  Validate quality of policies
  Document potential vendor findings for review with Client

- **Collaboration** - Pre-call email and post call confirmation email
- **Reporting** - Report with executive summary, relevant findings, recommended actions

Find out how easy it can be to identify and manage your risk.

VIRTUAL GUARDIAN

287 6th Street E,
Suite 500,
St. Paul, MN 55101

1550 Metcalfe Street,
Suite 1100,
Montréal, Québec
H3A 1X6

130 Adelaide St. W.,
Oxford Tower
Suite No. 2202
Toronto, ON M5H 3P5

1255 Lebourgneuf Blvd,
Suite 270
Québec (Québec) G2K 0M6

+1 -800-401-TECH (8324) www.virtualguardian.com www.gardienvirtuel.ca