5 KEY THINGS Your Annual Third Party Risk Assessment ISN'T Telling You

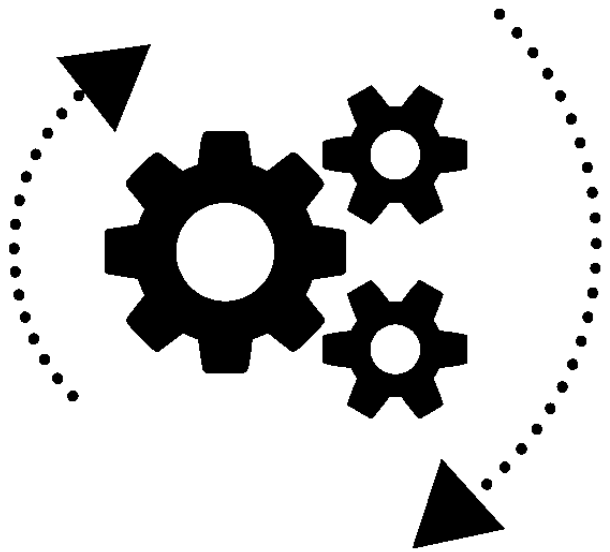
63% of companies don't have plans to update their Third Party risk assessments on an ongoing basis*

If you rely only on one-time assessments you **risk missing critical information** about your suppliers that can affect the security of your systems and data

So, **what's not covered** in a one-time annual third party supplier risk assessment?

* 2017 Ponemon Cost of Data Breach Survey

1 Operational Supplier Business Activity



Mergers and acquisitions,

Expansions,

Divestitures,

Contractions,

Redundancies, and

Senior Management changes…

all place stress on your suppliers and Third Party partners, their people controls and processes – which increases information security risk!

2 Legal Threats and Regulatory Action

You deserve to know if your supplier or Third Party partners is undergoing:

Group litigation proceedings,

IP cases,

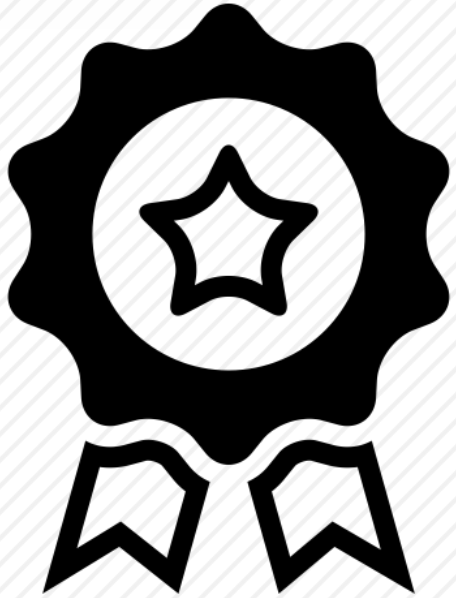
Sanctions,

Regulatory investigations, or

Other legal actions...

as this will affect how and whether or not you choose to do business with them.

3 Brand and Reputation Issues



Employee morale is stressed when a supplier confronts brand and reputational challenges, hurting operational effectiveness and security awareness..

which increases the probability of successful phishing and breach activity.

4 Data and Security Events

If your suppliers and Third Parties experience a data breach or security incident, they could experience business interruptions that affect your operations.

Or worse, their hackers could become your hackers - gaining access to your systems and sensitive data.

5 Financial Stability

Missing financial goals, capital changes, and bankruptcies can all be signs of deteriorating long-term viability of a supplier's business.

This can also signal decreasing investment in information security resources and controls to combat today's rapidly evolving threats.

"How can I keep track of these potential threats to my security posture between annual risk assessments?"

Get the complete picture - Continuous Threat Monitoring

Continuous Threat Monitoring provides a holistic view of the ongoing internal and external events that can affect the security postures of your suppliers… and you!

- ✓ Fills the intelligence gap between periodic assessments
- ✓ Holistic view of potential risks across 5 key areas

  Operational | Financial | Regulatory | Brand | Data
- ✓ Potential risk events constantly surfaced, scored and delivered
- ✓ Intelligent filtering of risk events and feeds
- ✓ The only monitoring service offering insight into each supplier's investments in IT security products

Welcome to DVV Solutions

Founded in 1999 | Headquartered in Cheshire, UK

- Experts in Third Party Risk and IT Security
- Shared Assessments member – only UK-based Assessment Firm
- Prevalent EMEA Channel Partner – only EMEA-based Partner
- Certified Third Party Risk Professional accredited Risk Assessors
- Clients across legal, banking, insurance, retail, and public sectors
- SupplierAssess™ managed service - unique TPRM-as-a-service offering outsourced risk assessment and analysis

Contact Us

Sean M. O'Brien
Director

T: +44 (0) 161 476 8700
E: sobrien@dvvs.co.uk

DVV Solutions Limited
Grosvenor House, St. Thomas's Place
Stockport, Cheshire, SK1 3TZ
United Kingdom

www.dvvs.co.uk

Find us www.dvvs.co.uk

Follow us LinkedIn.com/company/dvv-solutions


DVV
solutions