Mitigating Third Party Cyber Risk for Enhanced Business Security

Effectively addressing potential threats posed by third party vendors allows your organisation to maintain focus on core business activities.

devoteam
Cyber Trust

In today's interconnected digital world, businesses rely heavily on third party vendors and suppliers to perform critical functions and services. These vendors may have access to sensitive data, networks, and systems, making them potential entry points for cyber attacks. Unfortunately, many businesses don't have the necessary resources or expertise to effectively manage third party cyber risk on their own.

This is where third party cyber risk management comes in. It's a process of identifying, assessing, and mitigating cyber risks associated with third party vendors and suppliers. Third party cyber risk management helps businesses ensure that their third party vendors and suppliers are implementing adequate security controls and adhering to industry standards and regulations.

The need for third party cyber risk management has become increasingly critical in recent years as cyber attacks have become more sophisticated and frequent. These attacks can result in data breaches, financial loss, reputational damage, and regulatory fines. Implementing a robust third party cyber risk management program can help businesses protect their sensitive information, reduce the risk of a cyber attack, and maintain trust with their customers and stakeholders.

Overall, third party cyber risk management is essential for any business that relies on third party vendors and suppliers to ensure the security of their systems and data.

By managing third party cyber risk, businesses can proactively identify and address potential vulnerabilities before they become major security incidents.

Devoteam Cyber Trust
experience

At Devoteam Cyber Trust, we have over 15 years of experience in providing cutting-edge offensive security and cybersecurity engineering services to organisations of all sizes across a wide range of industries. Our expert consultants are highly skilled and certified in industry standards such as PCI QSA, CISSP, CCSP and ISO 27001, and have deep knowledge of the latest methodologies and tools used by potential attackers.

Our defined third party risk management strategies, our ability to adapt to the specific requirements of every customer complemented by our management platform, offer ongoing visibility into your security posture and enable proactive identification and mitigation of potential vulnerabilities and risks.

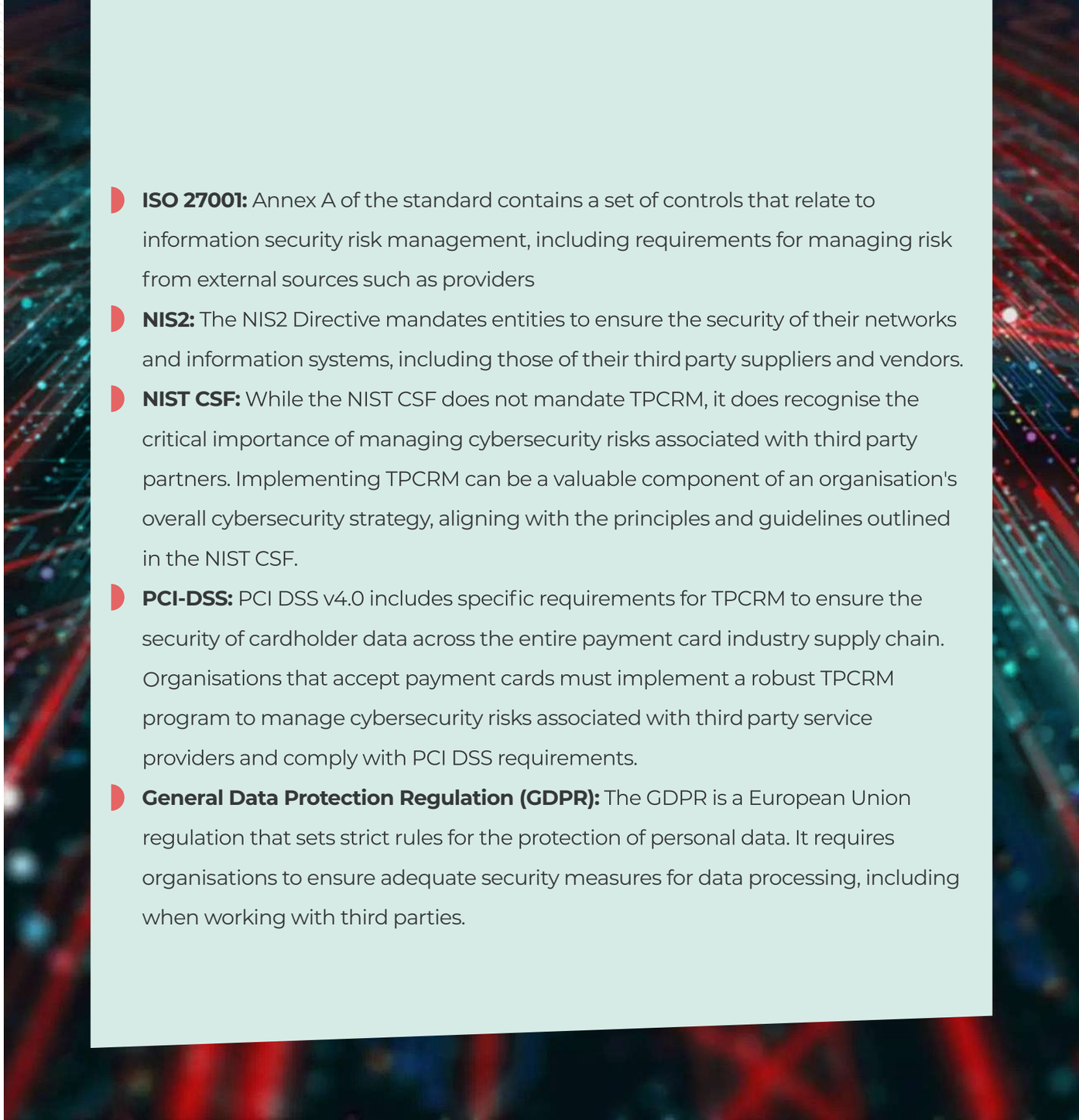
By working with us, you can have the confidence that comes with knowing that you are partnering with a mature partner in the subject of Third Party Cyber Risk Management.

(*) According to a recent report by IBM Security and the Ponemon Institute, the average cost of a data breach in 2021 was $4.24 million, or roughly 3.53 million euros

TPCRM
Standards & Regulations

Beyond its operational benefits in identifying and mitigating potential risks, Third Party Cyber Risk Management (TPCRM) is also becoming increasingly important for organisations from a regulatory and compliance perspective.

By engaging in TPCRM, organisations can demonstrate their commitment to meeting regulatory and compliance requirements, as well as aligning with best practices for information security management.



- **ISO 27001:** Annex A of the standard contains a set of controls that relate to information security risk management, including requirements for managing risk from external sources such as providers
- **NIS2:** The NIS2 Directive mandates entities to ensure the security of their networks and information systems, including those of their third party suppliers and vendors.
- **NIST CSF:** While the NIST CSF does not mandate TPCRM, it does recognise the critical importance of managing cybersecurity risks associated with third party partners. Implementing TPCRM can be a valuable component of an organisation's overall cybersecurity strategy, aligning with the principles and guidelines outlined in the NIST CSF.
- **PCI-DSS:** PCI DSS v4.0 includes specific requirements for TPCRM to ensure the security of cardholder data across the entire payment card industry supply chain. Organisations that accept payment cards must implement a robust TPCRM program to manage cybersecurity risks associated with third party service providers and comply with PCI DSS requirements.
- **General Data Protection Regulation (GDPR):** The GDPR is a European Union regulation that sets strict rules for the protection of personal data. It requires organisations to ensure adequate security measures for data processing, including when working with third parties.

"Even when it’s third party’s fault, it’s still your fault."

It’s all about compatibility.

With cyber attacks being a constant threat, it's no longer a question of if an attack will occur, but when.

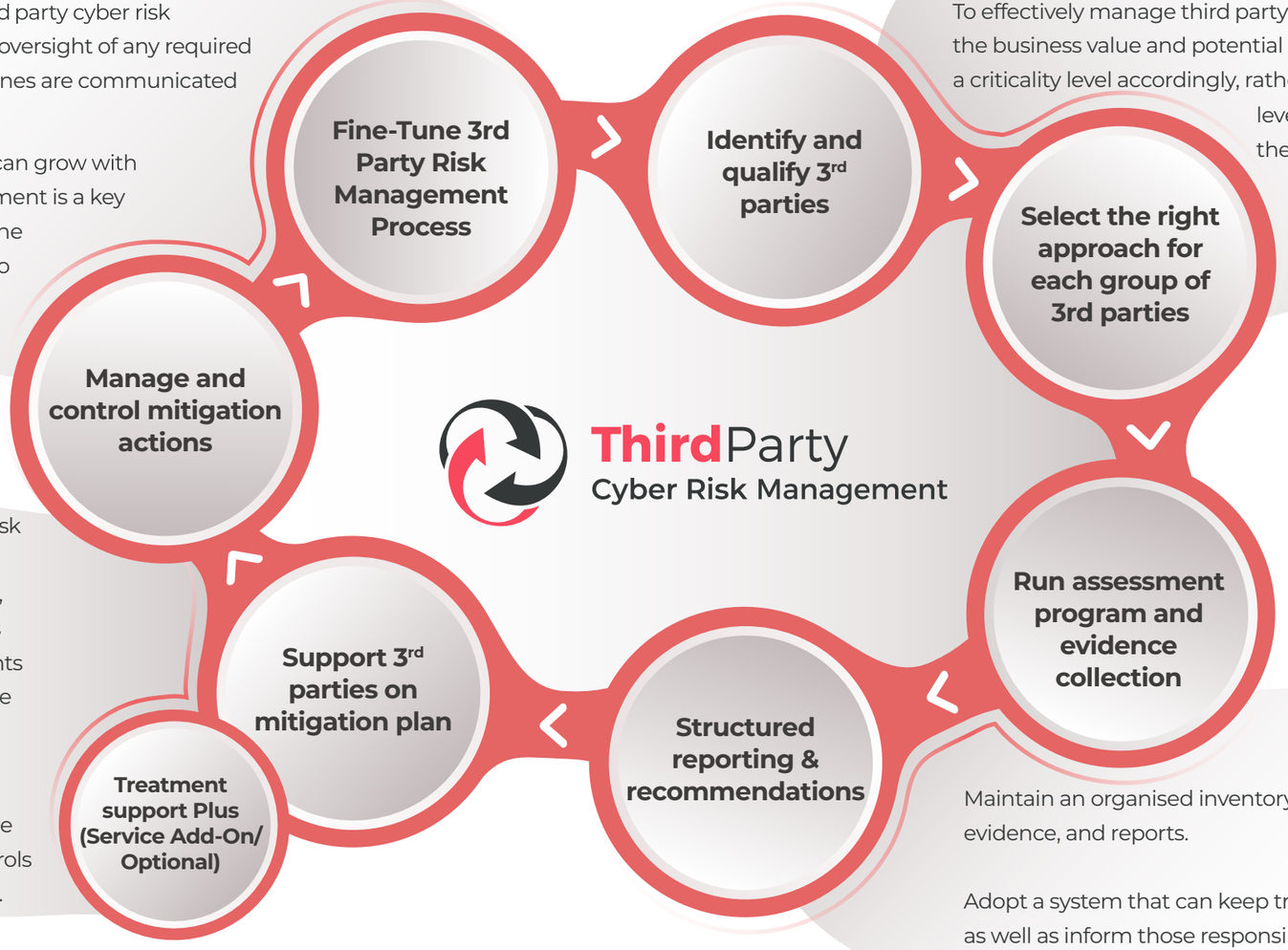
To effectively manage this risk, organisations need to adopt a proactive approach to cybersecurity, including managing the cyber risk inherited from their third parties.

Our approach to mitigating the cybersecurity risks posed by your third party

To maximize the benefits of your investment in third party cyber risk management, it is important to maintain constant oversight of any required actions and ensure that the agreed plan and deadlines are communicated to all parties involved.

Additionally, adopting a system that is flexible and can grow with your organisation is critical, as continuous improvement is a key aspect of any effective risk management process. The supporting system should be agile and adaptable to support your organisation's evolving needs.

To effectively manage third party cyber risk, it is important to identify the business value and potential impact of each third party and assign a criticality level accordingly, rather than assigning the same criticality level to all third parties which may hinder the ability to assess and work with them.



Supporting third party vendors and suppliers in implementing effective cybersecurity controls and risk management practices is essential because these third party entities may have access to sensitive data, networks, and systems. If their cybersecurity controls are weak or inadequate, they can become entry points for cyber attackers to gain unauthorised access to the organisation's data and systems.

By providing support and guidance to third party vendors and suppliers, organisations can help ensure that they are implementing adequate security controls and adhering to industry standards and regulations.

Maintain an organised inventory of all assessments, supporting evidence, and reports.

Adopt a system that can keep track of all gathered information, as well as inform those responsible of any required actions.

What we cover in our

Third Party review

Identify and qualify 3rd parties

Identify and qualify each 3rd Party in scope, taking into consideration the organisation business and according its relevance.

Run assessment program and evidence collection

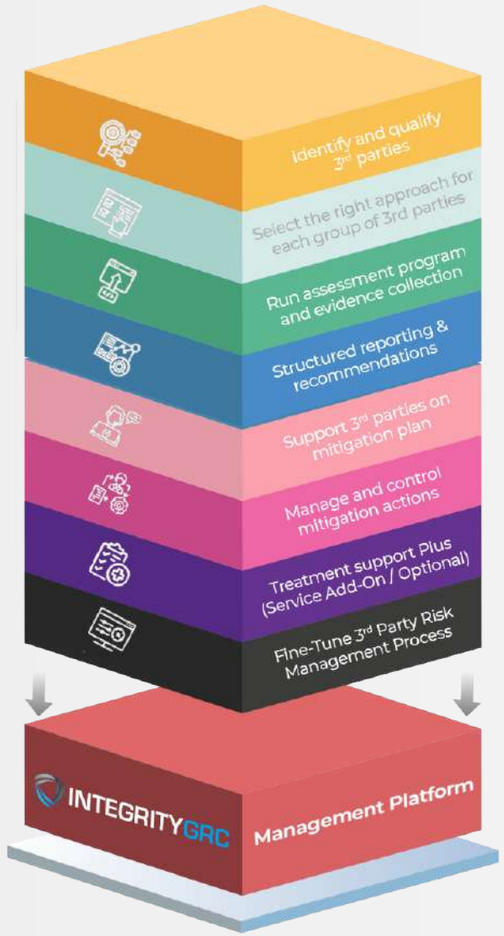
A predefined assessment program will be run via interviews and evidence collection, outputting the results from the assessment action.

Support 3rd parties on mitigation plan

All relevant parties participating in the mitigation process and supported by Devoteam Cyber Trust will be able to act and update the mitigation plan in the IntegrityGRC Platform.

Treatment support Plus (Service Add-On / Optional)

Devoteam Cyber Trust will participate on behalf of the client to interact with internal / external peers for an effective management of the mitigation process.



Select the right approach for each group of 3rd parties

Define the assessment program/plan with the scenarios for each group or 3rd parties.

Structured reporting & recommendations

A cyber security expert will put into context the identified issues and define recommendations for their mitigation. All findings will be reported in the IntegrityGRC platform.

Manage and control mitigation actions

The organisations will be able to manage and control mitigation actions on the IntegrityGRC Platform, as well as the entire finding lifecycle.

Fine-Tune 3rd Party Risk Management Process

Together evaluate lessons learned and define optimisations for a continuous fine-tune the Devoteam Third Party Cyber Risk Management process.

Service Plans

Every organisation has a set of third parties that provide distinct services to the organisation, but not all of them are equivalent in terms of criticality or potential impact for the organisation.

The service provides the potential of selection of the number and types of third parties, according to the following services:

Third Parties	Cyber Compliance Evaluation	Technical Evaluation
Type 1	• **Analysis framework:** Up to 50 questions from the information security categories model database of questions.	• N/A
Type 2	• **Analysis framework:** Up to 100 questions from the information security categories model database of questions.	• **CSSC (Devoteam Cyber Trust Cybersecurity Scorecard):** Devoteam Cyber Trust CSSC contains a set of cybersecurity controls to be assessed against organisation's cybersecurity environment. Once executed, it provides a clear and objective view of the organisation's cybersecurity posture.
Type 3	• **Analysis framework:** Customised questions from the information security categories model database of questions and/or customer specific questions.	• **CSSC (Devoteam Cyber Trust Cybersecurity Scorecard);** • **Full technical checks:** Security architecture review, detailed and in-depth technical checks for each 3rd party/technology; • **External integrations:** May include other services provided by Devoteam Cyber Trust, like pen-test.

Reporting Deliverables

At Devoteam Cyber Trust, we offer both formal and dynamic reporting for our TPCRM services.

Formal Report per Third Party

1. **Executive Summary:** A high-level overview of the key findings, including identified vulnerabilities, risks, and recommendations.
2. **Findings:** A detailed analysis of identified findings, including severity, impact, and likelihood of exploitation, as well as potential attack vectors and scenarios.
3. **Recommendations:** Specific recommendations for remediation and mitigation of identified findings, including technical solutions, process improvements, and training or education initiatives.
4. **Conclusion:** A summary of the key findings and recommendations, as well as any additional insights or observations from the engagement.
5. **Appendices:** Additional technical details, charts, graphs, and other supporting information to supplement the findings and recommendations in the main report.

// Structure might vary depending on specific service

Dynamic

Our powerful IntegrityGRC platform will provide you with all the findings and all the tools to manage the remediation process. You can manage globally the risk of your Third Parties or by groups or individuals.

Know the Benefits

- **Improved security posture:** TPCRM helps organisations identify and assess potential cybersecurity risks associated with third party vendors and suppliers, enabling proactive risk mitigation and strengthening overall security posture.

- **Reduced risk of cyber attacks:** Effective TPCRM can help reduce the risk of cyber attacks through third party channels, preventing data breaches, financial loss, and reputational damage.

- **Compliance with regulations:** Many industry regulations and standards, such as the NIS2 Directive and PCI DSS, mandate the implementation of TPCRM. Implementing TPCRM helps organisations comply with these regulations and avoid potential fines and penalties.

- **Enhanced trust with stakeholders:** By effectively managing third party cybersecurity risks, organisations can maintain trust with their customers, partners, and stakeholders, protecting their sensitive information and data.

- **Cost savings:** Implementing TPCRM can help organisations avoid costly cybersecurity incidents caused by third party vulnerabilities and reduce the costs associated with managing these incidents.

Certifications & Clients

Backed by a diverse portfolio of global clients and a wide range of certifications, including CREST, ISO 27001, ISO 27701, ISO 9001 and PCI QSA, Devoteam Cyber Trust is the premier choice for organisations seeking the highest level of expertise in third party cyber risk management.

ISO 27001 (2012)

CREST (2014)

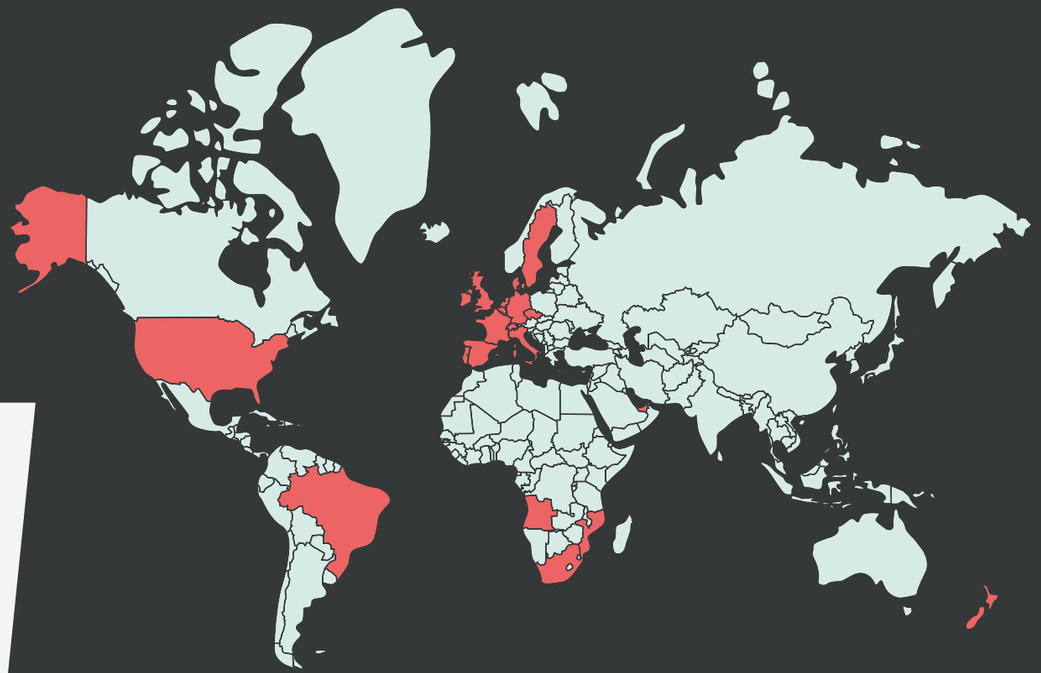
ISO 9001 (2014)

PNSC (2017)

PCI (2020)

Bancontact (2021)

ISO 27701 (2023)



More than 20 countries over the world

With HQ in Lisbon, we provide services to a wide **number of large and medium-sized companies**, both at a national and international level.

Case Studies

Risk Management of Strategic Partners

Type of Client: Pharmaceutical / Biotechnology with more than 15,000 employees and global presence

Challenge: The Client has a set of strategic partners that provide technological solutions, mainly in CaaS (Cloud as a Service) model, and the client did not have the structure nor the in-depth knowledge to regularly perform the assessment of the cybersecurity posture of its partners and the potential risks that may arise from this.

Compliance Risk Management

Type of Client: Global Agri-Business with over 11.000 employees in 37 countries

Challenge: In a prominent Agri-Business company, an extensive set of third parties required compliance assessments as part of a broader, multi-layered Third Party Cyber Risk Management (TPCRM) process. The challenge was to efficiently conduct these initial assessments to identify high-risk third parties for further in-depth evaluations, while minimizing resources and time spent on low-risk third parties.

Supplier Evaluation

Type of Client: Financial Entity with more than 35,000 employees and with global presence

Challenge: At a sizable financial organization, there is a need for a robust supplier evaluation process as part of their Third Party Cyber Risk Management (TPCRM) strategy. The challenge lies in accurately assessing each supplier's risk profile, ensuring they adhere to strict security and compliance standards while maintaining efficiency in the evaluation process.

What our clients are saying about us

"

The project is a success, the team has loads of technical expertise, they performed above expectations.

HEALTH

"

This is a win-win service and the report level is amazing.

ENERGY

"

It's very easy and reliable to work with Devoteam Cyber Trust.

BANKING

Click **here** to know more about these and other case studies, the solutions applied and the impact

Why engage with Devoteam Cyber Trust

- Deep expertise and experience in Cybersecurity Engeneering, with over 15 years of industry-leading experience.
- A team of highly certified and experienced security professionals, with certifications including CISSP, CCSP, ISO 27001 Lead Auditor, PCIP and PCI QSA.
- A commitment to quality and excellence, with a focus on delivering the highest levels of service and customer satisfaction.
- Access to advanced technology and tools, including a proprietary GRC platform.
- Compliance with industry standards and regulations, including PCI-DSS, ISO 27001, NIS2, GDPR, and other relevant guidelines and frameworks.
- A focus on long-term partnerships and ongoing support with continuous improvement of the offered services.
- A global footprint and reputation, with clients in over 20 countries and a proven track record of delivering effective and high-quality offensive security testing services.

How to Engage

01

Schedule an initial conversation with our expert consultants to discuss your needs, goals, and concerns.

02

Review and approve our customised proposal outlining the scope of our services, timeline, and costs.

03

Finalize the details of the engagement, including testing methodologies and scope.

04

Gain real-time insights into your security risks and vulnerabilities through our vulnerability management platform.

05

Receive regular updates on our progress, including detailed reports and remediation recommendations.

06

Access ongoing support and guidance from our team as needed.

Devoteam Cyber Trust is the right partner to support your organisation in this intense and evolving threat landscape, with best-in-class Offensive Security Services.

This is why dozens of medium-large clients from over 20 countries worldwide trust our services.

We are happy to share our **experience** and help you improve your **cybersecurity practice.**

Balanced risk management management requires a solid strategy.

Talk to us.

Contact us

info@integrity.pt

Present in 18 countries in the EMEA region

www.integrity.pt

devoteam Cyber Trust

About devoteam Cyber Trust

www.integrity.pt

www.devoteam.com/expertise/cyber-trust

Devoteam Cyber Trust is the Cybersecurity specialist arm of the Devoteam Group. With our 800+ experts located across EMEA, we aim to establish cybersecurity as an enabler of business success rather than a gatekeeper. We leverage an end-to-end approach to Cyber Resillience, Applied Security, and Managed Security services to secure the tech journey of large and medium-sized companies from all sectors and industries.

Since 2009, previously known as INTEGRITY, our team based in Portugal is specialised in providing cutting-edge Managed Security Services that combine its expertise and proprietary technology to consistently and effectively reduce the cyber risk of our clients. The comprehensive service range includes Persistent intrusion Testing, ISO 27001, PCI-DSS, GRC Consulting and Solutions, and Third Party Risk Management, ISO 27001 (Information Security), ISO 27701 (Privacy Information Management) and ISO 9001 (Quality) certified, PCI-QSA, and member os CREST and CIS - Center for Internet Security, we provide services to a considerable number of clients, operating in more than 20 countries.

About devoteam

www.devoteam.com

Devoteam is a leading consulting firm focused on digital strategy, tech platforms and cybersecurity.

By combining creativity, tech and data insights, we empower our customers to transform their business and unlock the future.

With 25 years' experience and 10,000 employees across Europe, the Middle East and Africa, Devoteam promotes responsible tech for people and works to create better change.

Creative tech for Better Change