Vendor Risk Assessment Checklist

Use this Third Party Risk Management checklist to secure your supply chain, ensuring alignment with trusted service providers and enforcing rigorous baseline security requirements from your vendors & third parties, in compliance with NIST CSF, ISO 27001:2022 & applicable data protection laws.

1. Checking Vendor Risk and Compliance Functions

- ❑ Dedicated Risk and Compliance Team: Verify that the vendor has a dedicated team responsible for risk management and compliance.
- ❑ Leadership Involvement: Ensure that senior leadership is involved in overseeing risk management and compliance efforts.
- ❑ Regular Internal Audits: Confirm that the vendor conducts regular internal audits to assess and improve their cybersecurity posture.

2. Availability of External Audit Reports

- ❑ Third-Party Audit Reports: Request recent third-party audit reports, such as SOC 2 Type II or ISO 27001 certification.
- ❑ Compliance with Standards: Verify that the vendor complies with relevant standards, including NIST CSF, PCI DSS, and ISO 27001.
- ❑ Audit Frequency: Ensure that the vendor undergoes regular external audits, at least annually, to maintain compliance and identify potential gaps.

3. Availability of a Risk Management Program

- ❑ Comprehensive Risk Management Program: Assess the vendor's risk management program to ensure it covers identification, assessment, and mitigation of risks.
- ❑ Policy Enforcement Mechanisms: Confirm that the vendor has mechanisms in place to enforce security policies and procedures.
- ❑ Incident Response Plan: Ensure the vendor has a documented incident response plan that is tested regularly and aligns with NIST CSF and ISO 27001 guidelines.

Other Recommendations for Vendor Cybersecurity Due Diligence and TPRM

- **Data Protection Measures**: Verify that the vendor employs robust data protection measures, including encryption, access controls, and regular data backups.
- **Employee Training Programs**: Ensure the vendor provides ongoing cybersecurity training and awareness programs for their employees.
- **Access Controls and Identity Management**: Confirm that the vendor uses strong access control and identity management practices, including multifactor authentication.
- **Patch Management**: Check that the vendor has a rigorous patch management process to keep systems and applications up to date with the latest security patches.
- **Supply Chain Security**: Assess the vendor's approach to securing their own supply chain, ensuring they conduct due diligence on their sub-vendors and service providers.
- **Business Continuity and Disaster Recovery**: Ensure that the vendor has a business continuity and disaster recovery plan that is tested regularly.

These steps will help you evaluate and ensure the cybersecurity posture of your vendors and service providers, conforming to NIST CSF, PCI DSS, and ISO 27001 standards.

Let's create a cybersecurity awareness program:
https://www.supplychainsecurity.ca

DATARISK
CANADA