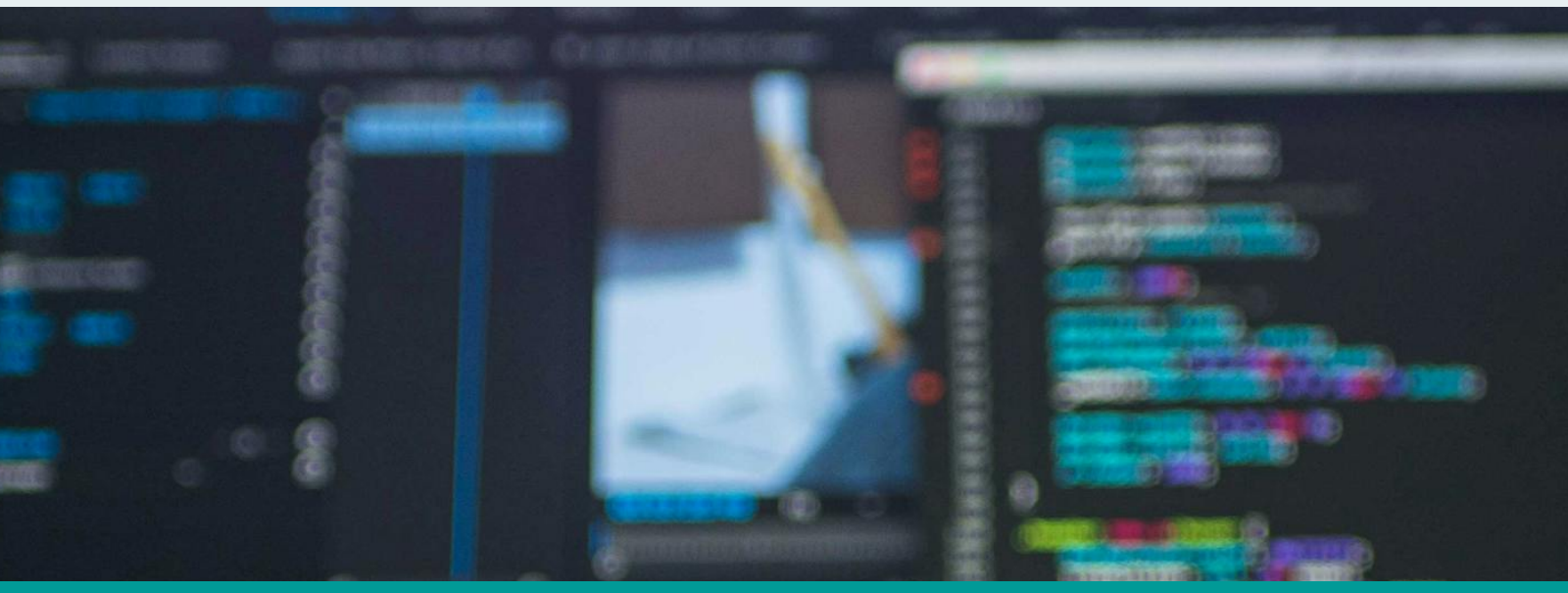
Third-Party Risk Management in Cybersecurity



Third-Party Risk Management (TPRM) in cybersecurity involves identifying, assessing, and mitigating risks associated with external vendors or service providers who have access to an organization's data or systems. Effective TPRM is crucial to prevent data breaches, maintain regulatory compliance, and ensure overall business continuity.

Key Points on Third-Party Risk Management in Cybersecurity:

- ***Vendor Assessment:*** Evaluate third-party vendors' cybersecurity posture before engagement.
- ***Risk Categorization:*** Classify vendors based on the level of access they have to sensitive data.
- ***Contractual Safeguards:*** Ensure contracts include security requirements and liability clauses.
- ***Continuous Monitoring:*** Regularly monitor third-party activities and security practices.
- ***Access Controls:*** Limit third-party access to essential data and systems only.
- ***Incident Response Plans:*** Ensure third parties have adequate incident response and recovery plans.
- ***Compliance Checks:*** Verify that third-party vendors comply with relevant industry regulations.
- ***Data Protection Policies:*** Ensure third parties adhere to strict data protection and privacy policies.
- ***Audit Capabilities:*** Conduct regular audits of third-party cybersecurity measures.
- ***Termination Procedures:*** Establish clear processes for terminating vendor relationships and securing data access afterward.

www.thecentexitguy.com

Centex Technologies

CENTEX TECHNOLOGIES

13355 Noel Road,Suite #1100
Dallas, TX 75240

Phone: (972) 375 - 9654

501 N. 4th Street,
Killeen, TX 76541

Phone: (254) 213 - 4740

1201 Peachtree ST NE,
400 Colony Square #200
Atlanta, GA 30361

Phone: (404) 994 - 5074

Capital Factory, 701
BrazosStreet, Suite 500
Austin, TX 78701

Phone: (512) 956 - 5454