datto

Vendor Assessment Cheat Sheet

Domain	Topics of Interest	Reference Documents	Applicable Vendor Types			
			Cloud (SaaS, IaaS, DBaaS, FaaS etc)	Contractors / Consultants	Software Vendors	Hardware Vendors
Information Security Program	- Does ISP follow a framework or guideline (which one) - Acceptable use of systems and assets (are they outlined) - Do security Roles exits, is leadership involved in security	- See Information Security Policy - Employe Handbooks - Acceptable Use Policies - Risk Management Policies	✓	✓	✓	✓
Employee Security	- Training and awareness, role based training - Background check processes - Onboarding and offboarding processes	- Employee Onboarding and Offboarding Policy - Security Awareness Programs - Security Training Programs	✓	✓	✓	✓
Application Security	- Does the development pipeline follow industry standards? - Are test environments logically and phsyically segregated? - how do they report and manage vulnerabilities?	- Vulnerability Management Policy - SDLC Documentation - Change Management Policy - See Application Security Standards	✓		✓	✓
System Security and Technology	- How are applications and servers protected? - Are Intrusion Detection Systems implemented? - Are systems and servers patched regularly? on a schedule?	- Vulnerability Management Standard - Configuration Standards	✓		✓	
Change Management	- What environments is change management enforced in - Software release cycle, explain process - Are testing environments isolated from production "	- Change Management Plan - Change Control Plans	✓		✓	
Network Security	- Is network topology understood and documented - Are firewalls configured according to best practices - Is a VPN part of the organizations network architecture"	- Network Security Policy - Data Management Plan - Secure Configuration Standard - Asset Management Standard	✓		✓	
Data Security	- Are dataFlow diagrams part of architecture - Is Data classified and properly segregated by process - Is encryption and key management part of a process	- Data Classification Policy - Dataflow Diagrams - Encryption Policies	✓			
Business Continuity	- Are BCP plans tested, details? - Backup locations, RAID configuration - Is redundancy architected against system loss, DDoS, etc	- Business Continuity Plan - Disaster Recovery Plan	✓			✓
Incident Response	- Is there a process for definying and categorizing an incident - Are tools and people in place to respond to an incident - Do they test their IR plans, and correct processes regularly	- IR Plan - Communication Plans - Forensic Security Policies	✓		✓	✓
Identity Management	- Password policies and requirements - Are administrative personnel and super users accounted for - Are user access reviews part of an established process	- Identity & Access Management Standard - Access Control Policies	✓	✓	✓	✓
Event Management	- Detail functions of organizational SOC - Do they administer SIEM, IDS, logs and security data - Are business critical systems identified	- Audit and Accountability Policy - Event Logging SOP - Incident Responce Plans	✓	✓		
Third Party Risk Management	- Do they have an understanding of vendors in their portfolio - Are vendors tiered based on their criticality and importance - Are there processes in place to evaluate vendors	- Vendor Risk Management Policy - Vendor Tiering Policies	✓		✓	✓
Data Center Security	- Is datacenter architecture a function of the program - Are physical security controls taken into consideration - Are geographic considerations known and understood	- Data Classification Policy - Dataflow Diagrams - Encryption Policies	✓			
Compliance	- Are there GDPR, SOX, HIPPA, etc controls they need to implement? - Will they handle data that you are responsible for under those - Do processes for notifying costumers of data changes exist?	- Compliance affirmations/ attestations - Compliance control maps	✓	✓	✓	✓

datto

Corporate Headquarters
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
United States
partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291

Updated May 2021