TEXAS RE

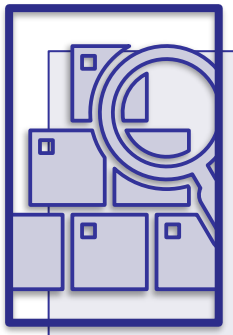
CrowdStrike

Devin Ferris
Manager, CIP Compliance Monitoring

CrowdStrike Windows Outage

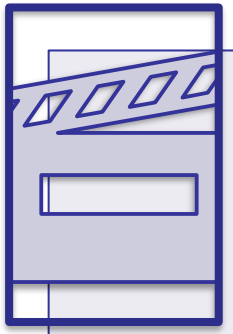
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

CIP-007-6 Table R2 – Security Patch Management

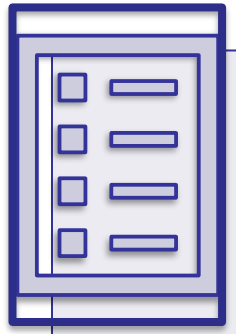


Part 2.1 – Identify

Part 2.2 – Evaluate

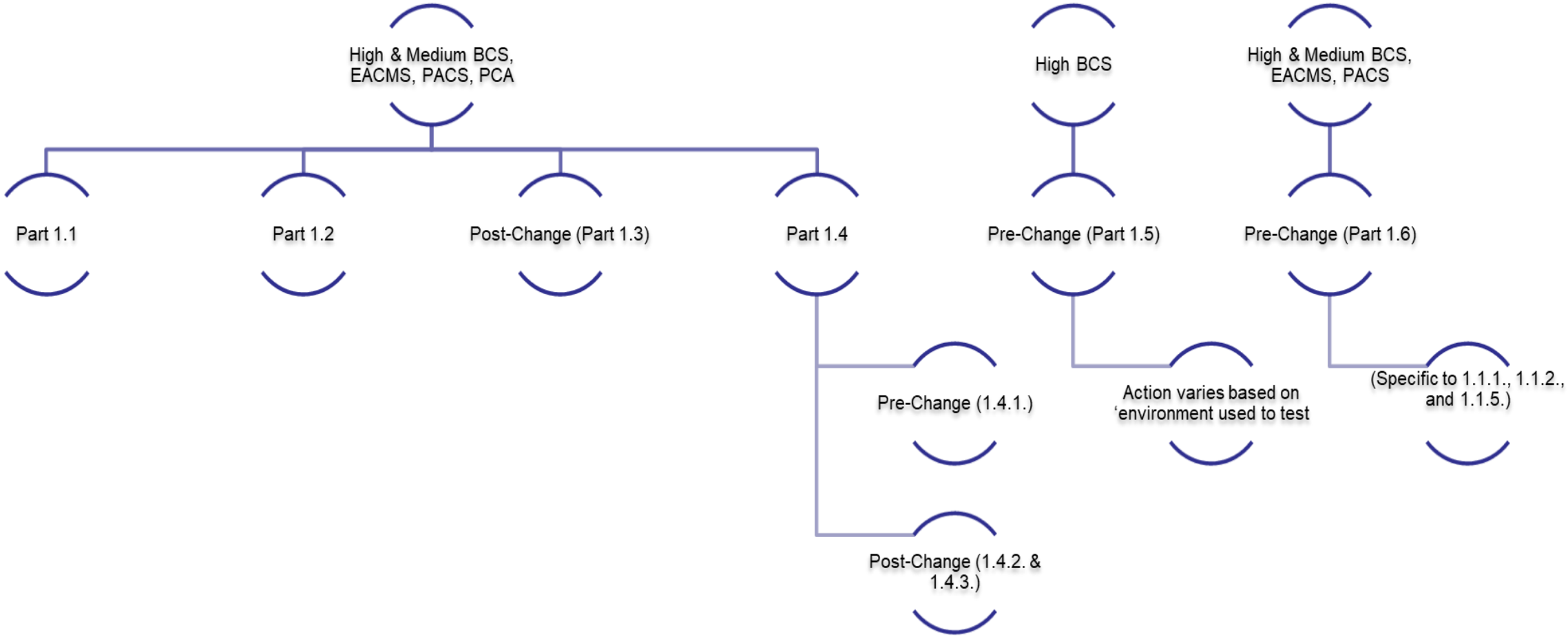


Part 2.3 – Actions



Part 2.4 – Mitigation Plans

CIP-10-4 Table R1 – Configuration Change Management



Internal Controls

Protect (PR)		throughout removal, transfers, and disposition	
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-4:** Adequate capacity to ensure availability is maintained	AU-4, CP-2, PE-11, SC-5
		PR.DS-5: Protections against data leaks are implemented	AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7, SI-10
		PR.DS-7: The development and testing environment(s) are separate from the production environment	CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	SA-10
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	SA-3, SA-4, SA-8, SA-10, SA-11
		PR.IP-3: Configuration change control processes are in place	CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested	CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	PE-1
		PR.IP-6: Data is destroyed according to policy	MP-6, SR-12
		PR.IP-7: Protection processes are improved	CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6

TEXAS RE
Ensuring electric reliability for Texans