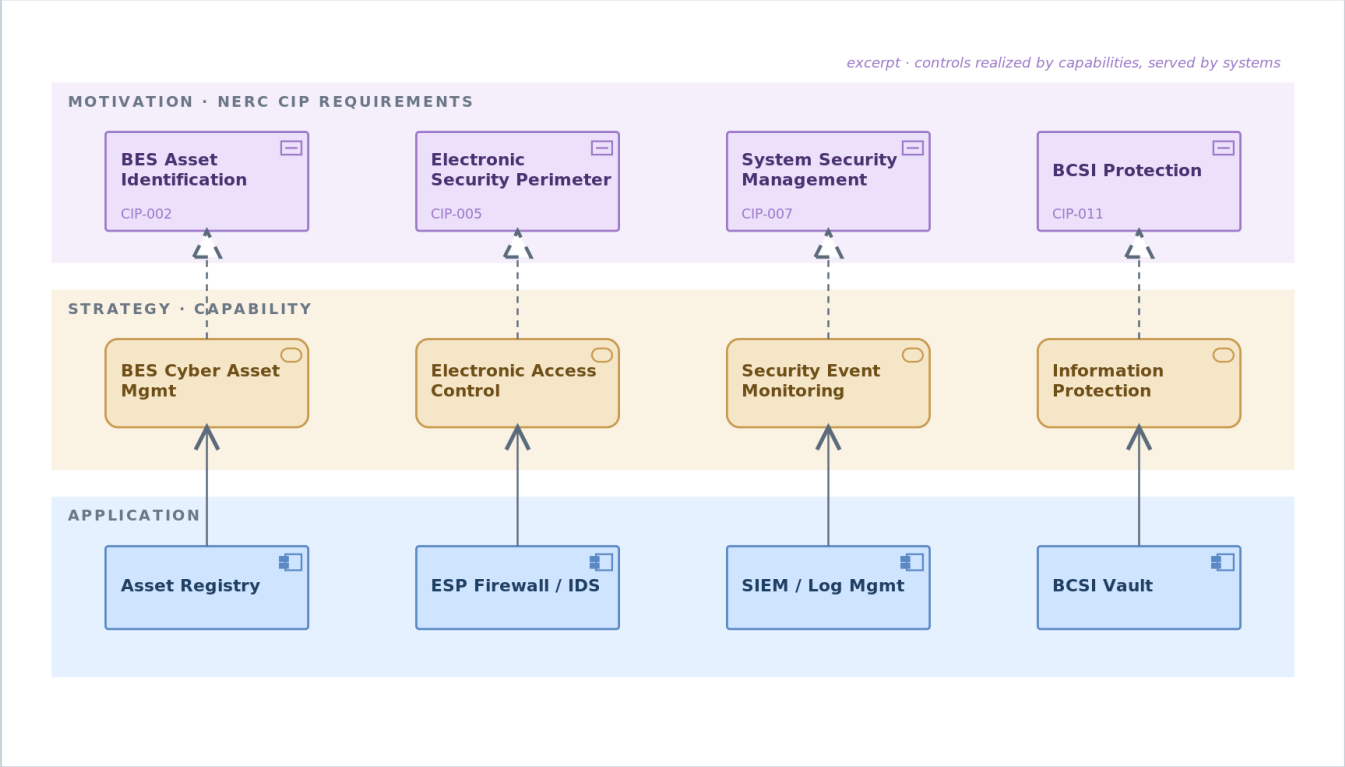
NERC CIP Compliance Pack

Sample excerpt · control-to-capability overlay

The NERC CIP Compliance Pack maps NERC CIP requirements to the business capabilities and application systems that satisfy them, on top of the Architecture Foundation — so a compliance review starts from a defensible, modeled baseline rather than a blank spreadsheet.



Control-to-capability mapping — excerpt

CIP standard	Business capability	Realizing system
CIP-002	BES Cyber Asset identification & management	Asset Registry
CIP-005	Electronic access control (ESP)	ESP Firewall / IDS
CIP-007	Security event monitoring	SIEM / Log Management
CIP-011	Information protection (BCSI)	BCSI Vault

The full Compliance Pack includes

- Control mappings across CIP-002 through CIP-014, traced to capabilities and systems
- BCSI handling architecture — storage, access, and chain-of-custody patterns
- Evidence-collection model aligned to audit expectations
- Audit-defensible documentation templates
- Builds on the F-01 meta-model foundation (required substrate)

This pack is a compliance architecture, not a compliance attestation. It gives an EA and compliance team a modeled starting point; the entity remains responsible for its own controls and evidence.