Comparison: AS IEC 62443 vs Essential Eight vs NIST CSF

Feature / Dimension	**AS IEC 62443**	**Essential Eight (E8)**	**NIST Cybersecurity Framework (CSF)**
Origin	IEC (International Electrotechnical Commission) / ISA	Australian Cyber Security Centre (ACSC)	National Institute of Standards & Technology (US)
Purpose	Secure **Industrial Automation & Control Systems (IACS)** & **OT environments**	Reduce **common cyber threats** through **baseline mitigation strategies** (focused on endpoints & IT)	Broad, **risk-based framework** for managing cybersecurity for all sectors
Scope	OT & ICS: hardware, software, processes, lifecycle security of industrial environments	IT endpoints & enterprise networks: prevent, limit, recover from malware & attacks	Universal: IT & OT, governance, risk management, operations
Structure	4 Categories: General, Policies & Procedures, System Requirements, Component Requirements	8 mitigation strategies mapped to maturity levels (0–3)	5 Functions: Identify, Protect, Detect, Respond, Recover
Focus Area	OT-centric: zones & conduits, security levels, secure development, ICS lifecycle	IT-centric: patching, hardening, access control, backups (basic hygiene)	Risk management, governance, resilience, continuous improvement

Feature / Dimension	AS IEC 62443	Essential Eight (E8)	NIST Cybersecurity Framework (CSF)
Level of Detail	Detailed technical & procedural controls for IACS security at all levels (asset owner, integrator, vendor)	Simple, actionable controls (8 strategies)	High-level, adaptable to different organizations & sectors
Maturity Model?	Yes – security levels (SL1–SL4), risk-based	Yes – maturity levels (0–3)	Optional – tiers (Partial → Adaptive) to assess implementation maturity
Examples of Controls	Zone/conduit segmentation, SL requirements, secure software development lifecycle, system hardening	Application whitelisting, patching OS & apps, admin privilege control, backups	Asset inventory, access control, anomaly detection, response planning
Legal/Regulatory Fit (Australia)	Supports SOCI Act, CIRMP, AESCSF for critical infrastructure	Mandatory for some government systems; recommended for businesses	Referenced in various Australian guidance documents & risk frameworks
Ease of Implementation	Complex – requires specialized OT expertise & planning	Relatively simple, focused, good starting point	Flexible, but may require tailoring & interpretation
Who should use?	Critical infrastructure operators, OT vendors, integrators	Small-to-large businesses, government, anyone with IT systems	Any organization (especially at board & executive level for governance)