

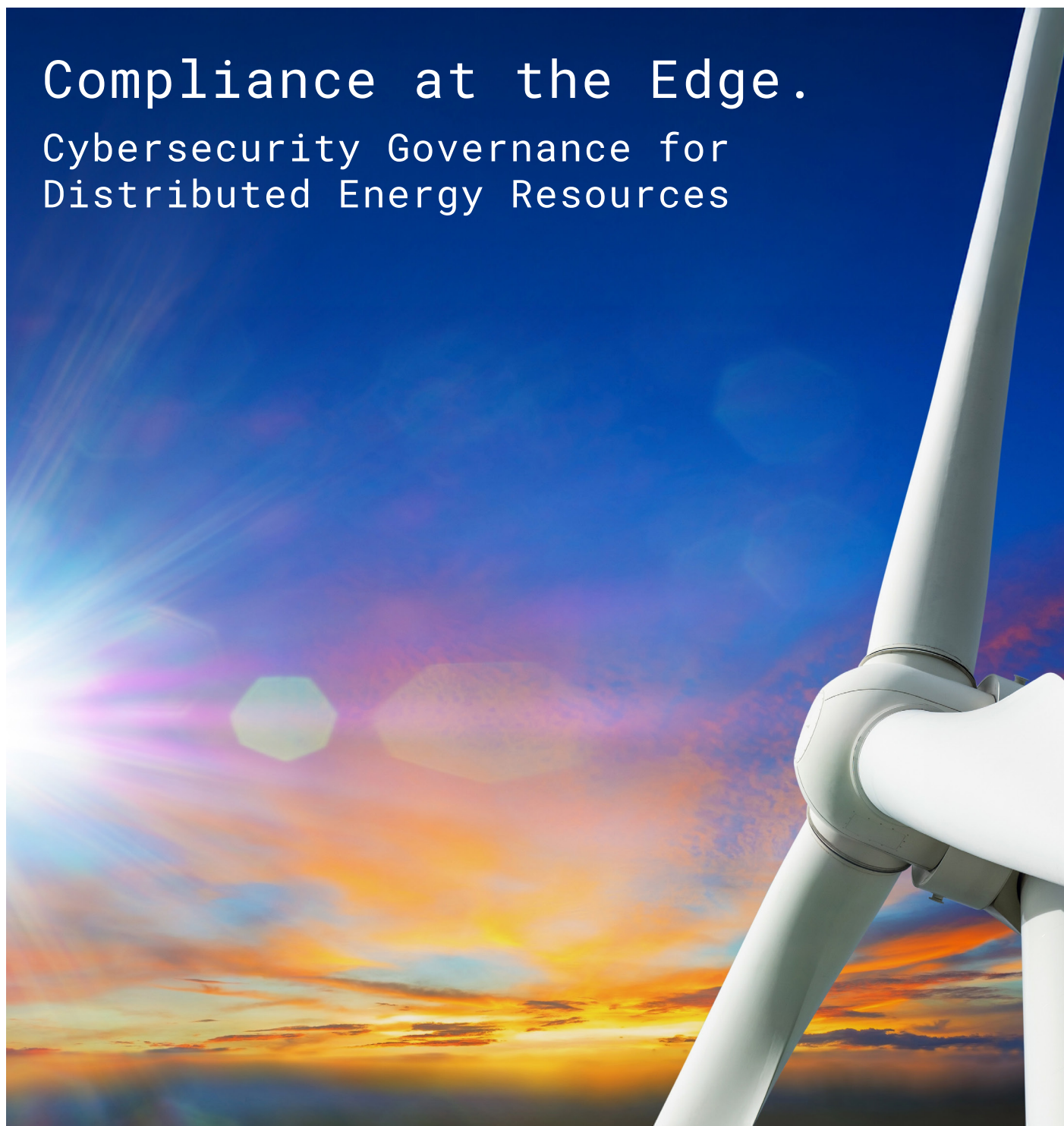


Cyberwatch Finland

WHITE PAPER 2026

Compliance at the Edge.

Cybersecurity Governance for
Distributed Energy Resources



Cybersecurity is Built by Small Actions and Management of Large Concepts



TABLE OF CONTENTS

Executive Summary	4		
1 Introduction	5	5 Regional Governance Approaches	21
2 The Emerging Energy Sector Context	7	5.1 European Union	22
3 The Cyber-Physical Threat Landscape	9	5.2 United Kingdom	23
3.1 Expanding Attack Surface	9	5.3 United States	24
3.2 A Threat Taxonomy	10	5.4 Asia-Pacific	25
4 Compliance to Govern Distributed Diversity	13	5.5 Africa	27
4.1 Edge – Core Problematique	13	5.6 Latin America & Caribbean	28
4.2 Standards as Foundations	15	5.7 Cross-Regional Synthesis	29
4.3 A Model Compliance Framework for the DER Layer	16	6 Recommendations: From Analysis to Action	31
Pillar 1: Scope – Who Must Comply	16	Task 1 – Establish the Common Technical Floor	32
Pillar 2: Baseline Obligations – What Must Be Achieved	17	Task 2 – Close the Distribution and DER Gap	33
Pillar 3: Verification – How Compliance Is Assessed	17	Task 3 – Make Supply Chains Auditable	33
Pillar 4: Accountability – Consequences and the Assignment of Responsibility	18	Task 4 – Build Enforcement and Reporting Capacity Where It Is Weakest	34
4.4 From Framework to Practice: The Implementation Problem	18	Implementation: From Decision to Practice	36
The instrument mix: sticks, carrots, and sermons	19	7 Conclusion	37
The capacity and harmonisation problems	19	References	38
The lifecycle problem	20	List of Abbreviations	40
		Annex 1: Cybersecurity Governance Principles by Region	41

Cyberwatch WHITE PAPER



PUBLISHER	Cyberwatch Oy Kansakoulukatu 1b 00100 Helsinki, Finland
LAYOUT	PuulaMedia / Mari Riepponen
ILLUSTRATIONS	AdobeStock, AI GENERATED
ISSN	2490-0761 (web)



Executive Summary

Decarbonising and diversifying energy production is challenging established cybersecurity governance models built for a centralised grid. The core governance question is how compliance with cybersecurity obligations can be assigned, verified, and enforced across a population of distributed energy actors radically more diverse than the population for which existing regimes were built.

The sector’s structure is changing faster than its governance. Distributed energy resources have moved from marginal to structural, with cumulative worldwide installed photovoltaic capacity passing 2,260 GW by the end of 2024 and a further estimated 510 GW added in 2025, shifting control of the electricity system from a small number of large, regulated facilities to millions of consumer-owned, software-controlled devices. The threat record has kept pace as energy has been the second most targeted sector in politically motivated cyber operations during geopolitical conflict. Most likely the first demonstrated cyber-to-physical effects on European energy infrastructure took place in 2025: the remote seizure of a Norwegian hydropower dam’s operational controls and a thwarted coordinated operation against distributed energy assets across more than thirty Polish sites.

Our analysis of American, Asian, African, European and Pacific practices, assessed against a four-pillar compliance framework derived from IEC 62443, NIST CSF 2.0, and the CISA Cross-Sector Cybersecurity Performance Goals 2.0, finds that governance intent is broadly shared but implementation capacity is not. The distributed energy resources (DER) layer is the most consistently under-governed segment in every case examined: regulatory attention remains concentrated on bulk transmission and generation, while the fastest-growing part of the system carries fragmented scope definitions, inconsistent incident reporting, thin supply-chain transparency, and a visibility gap when system operators cannot ade-

quately see connected devices they also cannot defend. The DER aggregator tier is the most consistent gap across all regions since no jurisdiction has made aggregator and virtual power plant compliance a condition of market access, even though the aggregator is the pivotal compliance node between the individual device and the grid operator.

What differs across regions, and differs enough to shape the recommendations, is not the desirability of cybersecurity baselines but four conditions that determine whether baselines can be enforced and sustained: enforcement capacity; institutional trust and public-private coordination; the maturity of distribution- and DER-level oversight; and the availability of financing and a specialised workforce. Technical baselines are universal. The governance architecture needed to enforce them is regionally contingent and must be adapted accordingly.

The accountability mechanisms that work across all regions share the design feature of market access conditioned on compliance rather than retrospective penalty after an incident. Chile’s fining powers, Australia’s licence conditions, and the EU’s supervisory sanctions all operate on this logic. The jurisdictions that have advanced furthest have made the same political choice, and it is available to others. Effective governance combines a common technical floor with regionally adapted enforcement architecture, and unavoidably with politics.

The report’s recommendations are organised as four strategic tasks, each with a stated goal, lines of action, and implementation measures. Each line of action is marked [Universal], where it applies in essentially the same form everywhere, or [Regional], where it must be adapted to local political ambitions, implementation capacity, institutional trust, or resourcing. More governance, or governance described as more mature, does not automatically produce improved resilience and security; thoughtful and relevant governance does.



1 Introduction

Energy and electricity systems are becoming more distributed, more software-dependent, and less centrally controlled as they decarbonise. The reliability of the energy system and the security of its diversifying digital layer are fundamentally aligned. Similarly intertwined are cybersecurity and wider societal and national concerns. Indeed, cyber-attacks are intentional and effect-seeking acts directed at producing a specific operational, financial, and often ultimately political outcome in a target system. The intentional and dynamic character of cyber-attacks makes governance a necessary complement to engineering-focused management.

This report analyses how cybersecurity governance in the energy sector should be designed, organised, and enforced. In particular, we focus on how compliance with cybersecurity obligations can be structured for a distrib-

uted energy sector whose actors are radically more diverse than those for which existing governance regimes were built. The report is intended as food-for-thought for public policy planners and energy sector administrators rather than a prescriptive blueprint. Its value lies in the questions it raises and the analytical structure it offers, not in any claim to a universal answer.

Accordingly, we approach energy-sector and DER cybersecurity as a governance question: who sets requirements, who enforces them, and how authority and capacity are distributed across institutions and regions, rather than as a technical question of which control, protocol, or architecture to deploy. The technical standards of energy resilience seem relatively well settled and widely documented: international and professional standards already specify

what secure-by-design, zero-trust, and supply-chain-verified energy infrastructure looks like. What those standards do not resolve is who is responsible for requiring, financing, and enforcing them, and how that responsibility should differ, if at all, between a jurisdiction with a mature regulator and one still building basic institutional capacity.

Governance concerns the rules and principles of an order and how power is organised within a system (that system being an entity or a policy area). Organised governance helps to align different, individually legitimate demands and domains so that they support the effective production of collective value. The principles of governance are common to all levels and sectors, but individualised approaches and implementation are a necessity. National and regional political ambitions, resources and approaches to energy-sector cybersecurity governance differ substantially. This objective reality challenges the presumption of universal, region-neutral governance solution.

Governance should further be distinguished from management: the two are inseparable but distinct. Whereas governance includes ideational aspects, a management systemic and organisational ones. Paraphrasing Kant, management system without the ideals of governance is blind, and governance without a systemic-organisational appearance remains empty. We therefore presume that energy and DER governance cannot fundamentally differ from the governance of other public policy areas.

As governance practices oscillate between enforcement of rules, performance-based indicators, voluntary approaches, and multi-stakeholder contributions, the strategies proposed in this report deliberately combine several of these modes rather than promoting any single silver bullet solution. Security governance can be oriented by risk or by precaution. A risk-based approach ties responsibility to foreseeable outcomes and depends on the accuracy of assessments about anticipated attackers; a precaution-based approach ties responsibility to an actor’s position in the system and to the vulnerabilities within it: what needs to be protected is more essential than knowing from whom it must be protected. This report’s recognition of enablers of cyber incidents and the under-governed DER layer follows the precautionary orientation. A central analytical question follows directly from this orientation: given the substantial

differences between regions in regulatory architecture, enforcement capacity, and DER penetration, should governance recommendations be regionalised, or are the fundamentals of cybersecurity governance essentially region-neutral, making local variation a matter of implementation rather than design? Our answer is: both, but at different levels. A defined set of technical and organisational practices functions the same way regardless of region, because it responds to properties of the technology itself rather than to local institutions — zero-trust architecture, secure-by-design procurement, component inventories, and time-bound incident reporting (NIST, 2020; NIST, 2022). At the diplomatic level, the 2015 UN Group of Governmental Experts established voluntary norms of responsible state behaviour covering critical infrastructure protection, supply-chain integrity, and CERT non-interference (UN GGE, 2015); the July 2025 UN Open-Ended Working Group reaffirmed these norms and established a permanent Global Mechanism for cyber capacity-building (UN OEWG, 2025). These technical standards and diplomatic norms are universal in the sense that they represent settled expectations; they are not universal in the sense of being self-enforcing. What differs across regions are the elements of governance architecture including enforcement capacity, institutional trust, the maturity of distribution- and DER-level oversight, and the availability of financing and a specialised workforce.

The CISA Cross-Sector Cybersecurity Performance Goals 2.0, released in December 2025 and aligned to the NIST Cybersecurity Framework 2.0, organise governance-relevant practices across six functions: Govern (leadership accountability, risk management strategy, policy development, roles and responsibilities, and supply-chain oversight); Identify (asset management and risk assessment); Protect (access control, secure-by-design, and data security); Detect (continuous monitoring and anomaly detection); Respond (incident response planning and communications); and Recover (recovery planning and improvement) (CISA, 2025). The DCAF Guide to Good Governance in Cybersecurity frames the same terrain through the lens of democratic governance, emphasising effectiveness and efficiency, responsiveness to the security needs of all members of society, accountability and oversight (parliamentary, civil society, and independent expert), the rule of law and legal framework, stakeholder cooperation, operational capacities and resilience, and awareness and cyber hygiene (DCAF, 2021; DCAF, 2024). Together, these two frameworks yield six governance principles that this report uses to organise the regional and the governance gap analysis, namely (i) legal and policy framework; (ii) institutional authority and accountability; (iii) risk governance; (iv) operational capacity; (v) supply-chain and technology security; and (vi) stakeholder cooperation and oversight.



What needs to be protected is more essential than knowing from whom it must be protected



2 The Emerging Energy Sector Context

Decarbonisation is driving a move from centralised, fossil-fuelled generation towards diversified portfolios of wind, solar, storage, and distributed energy resources. Control of the electric energy system has shifted from a small number of large, physically secured facilities to a much larger number of smaller, software-defined, and often remotely managed assets. Investment patterns illustrate the scale of this shift: clean-energy investment exceeded USD 2 trillion globally in 2024, with digital-native assets forming an increasing share of new capacity in every region (IEA, 2025).

The concept of distributed energy resources covers a broad and growing category of assets: rooftop and small-scale solar, behind-the-meter batteries, electric-vehicle chargers and vehicle batteries used for bidirectional flow, smart thermostats and other demand-response devices, small-scale wind and combined-heat-and-power units, and the smart meters and edge controllers that monitor and communicate with all of the above. What these assets have in common is their position in the system at

or beyond the customer meter, outside the perimeter that utilities have traditionally controlled directly.

This positional definition matches the one used by the International Energy Agency which defines DERs as “small-scale energy resources usually situated near sites of electricity use,” including rooftop solar, battery storage, electric vehicles, and comparable behind-the-meter installations, and documents the pace at which they have moved from marginal to structural. Global annual photovoltaic additions grew from an estimated 145 GW in 2020 to a record 602 GW in 2024, taking cumulative worldwide installed photovoltaic (PV) energy capacity past the 2,260 GW mark by the end of that year, a 29% year-on-year increase with almost half of all PV capacity ever installed added in just the preceding three years, before a further estimated 510 GW was added in 2025, taking the global total to roughly 2,380 GW (IEA-PVPS, 2025; REN21, 2025; IRENA, 2026). China alone accounted for close to 60% of new installations in 2024, underscoring

how concentrated this growth remains even as it diversifies geographically (REN21, 2025).

Bulk generation and transmission assets are overwhelmingly owned and operated by regulated utilities or licensed independent power producers, which makes them addressable through conventional regulatory instruments. DER units and systems are owned by households, commercial building operators, electric vehicle fleet managers, and third-party aggregators that contract with individual asset owners to bid combined capacity into markets as virtual power plants. A DER fleet is often technically dispatchable by an aggregator that has no direct regulatory relationship with the grid operator whose stability depends on that fleet behaving predictably. Furthermore, ownership diversity in particular makes DERs difficult to govern using instruments designed for a small number of large, regulated operators. Aggregators pooling small-scale resources and act on their owners’ behalf in power markets and virtual power plants optimising networks of decentralised generation, storage, and flexible demand turns the historically one-directional flow between grid and consumer into a bidirectional one (IEA, 2022).

The emerged DER layer sits in the regulatory perimeter, and who is accountable, and of what, varies by jurisdiction and is frequently unresolved. The IEA points out a visibility gap, that regulators and system operators lack sufficient information on behind-the-meter resources and adequate monitoring of low-voltage distribution grids,

many of which were designed for a twentieth-century system in which the DER share was small (IEA, 2022). The IEA also identifies a structural misalignment of interests between citizen-operators and the broader systemic needs (IEA, 2022). Diversified ownership is likely to leave many devices and systems outdated and unpatched unless governance and regulation would either penalise unwanted or reward wanted behaviour.

The IEA’s regulatory recommendations include that grid codes should be updated to require advanced inverter functions, specifically voltage and frequency ride-through and voltage regulation, as a condition of connection (IEA, 2022). The same connection-gate mechanism is the natural carrier for the authenticated device identity and secure-by-design requirements. Secondly, the roles and responsibilities of independent aggregators should be formally established as markets open to aggregated small-scale resources (IEA, 2022). Defining those roles for market participation without simultaneously defining the aggregator’s security obligations would repeat, now one layer up, the mistake made with the devices themselves.

The direction of DER growth is global but the pace, dominant asset type, and institutional readiness to manage it vary. Regional and jurisdictional variations in DER pace, direction, and institutional capacity help to direct the emphasis of governance and the balance between universal and individualised cybersecurity approaches. Table 1 summarises the variation at a high level.

Table 1: Indicative regional variation in the DER tendency

REGION	PRIMARY DER GROWTH DRIVER	DOMINANT DER TYPE	INSTITUTIONAL READINESS
Europe	Decarbonisation mandates, energy-security policy since 2022, emerging data-centre load growth	Rooftop solar, heat pumps, growing EV fleet	Comparatively high; DER security increasingly folded into existing product and entity regulation
North America	Electrification of transport and buildings, data-centre load growth	Behind-the-meter solar and storage, EV charging	Uneven; strong at bulk level, immature for DER-specific oversight
Asia-Pacific	Rapid renewables build-out, urban electrification	Large-scale distributed solar, inverter-based resources at scale	Mixed; advanced in Australia and strengthening in China and India; ASEAN uneven; advanced pilots in some states, limited coverage in others
Africa	Electrification and affordability, leapfrogging centralised grid build-out	Mini-grids, solar-home systems, mobile-enabled energy services	Early-stage; capacity still being built alongside deployment
Latin America & Caribbean	Renewable resource quality, distributed solar economics	Distributed solar, emerging storage	Early-to-mixed; digital deployment outpacing regulatory coverage

Table No 1. Indicative regional variation in the DER tendency. IEA (2022); IEA (2025); IEA-PVPS (2025); REN21 (2025); IRENA (2025); IRENA (2026); AFREC (2024); Inter-American Development Bank & OAS (2025). Author’s compilation.



3 The Cyber-Physical Threat Landscape

3.1 Expanding Attack Surface

Operational technology (OT), the systems and processes that operate directly with physical resources, differs from enterprise information technology (IT) in its requirements for real-time performance, safety, and continuity. Historically, OT has been protected mainly by physical and operational isolation by fences, walls, and strict access control. That isolation is disappearing as distributed generation, remote monitoring, cloud-based fleet management, and third-party maintenance access multiply the connections between OT, enterprise IT, and external networks. Increasing and integrating new means of connectivity, storage, and diversified systems means that each new connection point, telemetry path, and market interface becomes part of the sector’s trust boundary. Cybersecurity specialists need to be involved in inter-connection projects from the outset, and cyber-physical risk review should be a formal gate before new assets are energised.

Whereas centralised segments of the sector, nuclear facilities, and bulk transmission, generally have strong, well-enforced control regimes, distribution-level infrastructure, consumer-facing devices, and fleet-managed renewables generally do not. The practical effect is that the contemporary attack surface is defined less by the number of connected devices than by the implicitly trusted control relationships between operators, vendors, aggregators, and customers.

Between 2010 and 2024, the energy sector was, after telecommunications, the second most targeted sector in cyber operations (EuRepoC, 2026b). Roughly two-thirds of attributed operations against the energy sector in that period trace to three states: China, Russia, and Iran (CSIS, 2026). Energy-sector exposure is not a random by-product of general cybercrime, but it concentrates where geopolitical conflict and thinly covered digital dependency intersect.

3.2 A Threat Taxonomy

For the governance focus of this report, rather than focusing on threat actors as such, cyber threats are classified by the architectural layer they target, the entry method used, the dependency exploited, the operational effect produced, and the actor’s capability to translate a cyber intrusion into a physical consequence. Drawing on the MITRE ATT&CK for ICS framework (MITRE, 2025), the current threat landscape divides into three tiers.

Credential thefts, exploitations of remote access and VPNs, ransomware, denial-of-service attacks, and “living-off-the-land” persistence using legitimate administrative tools constitute a baseline cyber incident methodology. Industry monitoring recorded well over a hundred ransomware groups affecting thousands of industrial organisations in 2025, with measurable operational disruption in many OT-related cases (KPMG, 2025; Dragos, 2026). Separately, sector threat-landscape analysis has consistently ranked availability attacks and ransomware among the most significant categories affecting European energy entities (ENISA, 2024). Without necessarily directly targeting industrial control systems, serious operational harm to energy systems can be caused by penetrations through and identity compromises on the business network.

Cyber intrusions can thus transfer to and cause changes in administrative and physical system behaviour through protocol-aware manipulation of control traffic, and destructive activity targeting the communications pathways of distributed and edge assets alone. Distributed energy resources and microgrid fleets are increasingly treated by attackers as operational targets in their own right.

In April 2025, actors subsequently linked to Russian-aligned groups seized operational control of the Risevatnet hydropower dam in western Norway, opening its water valve at full capacity for hours before the intrusion was detected, constituting a direct translation of cyber intrusion into physical effect on energy infra-

structure (EuRepoC, 2026a). In December 2025, Polish national energy infrastructure was targeted by what EuRepoC assesses as the first large-scale, coordinated cyber operation directed against distributed energy resources across multiple sites simultaneously. The attack was thwarted before achieving systemic impact, but its design confirmed that the DER layer is now treated by capable attackers as a coherent operational target rather than a collection of individually insignificant devices (EuRepoC, 2026a). The same dataset quantifies the trend where disruptive elements now feature in over 69% of operations attributed to Russian-origin actors, up from 55% a year earlier, with the energy and transport sectors in Norway, France, and Poland absorbing the most significant damage (EuRepoC, 2026a).

A joint advisory issued in December 2025 by the US, European and Five Eyes cybersecurity and cybercrime agencies formally linked the self-styled hacktivist collective CARR to Russian military intelligence unit 74455 (Sandworm) (FBI, 2025). The issuing agencies assessed that Z-Pentest, the group behind the Norwegian dam intrusion, was founded by CARR members, while NoName057(16), the most active threat actor in Europe, was established by a Kremlin-affiliated entity that funds its infrastructure and selects its targets (FBI, 2025; EuRepoC, 2026a). The UK National Cyber Security Centre has recorded a stark increase in threats to critical national infrastructure systems, with adversaries seeking outcomes ranging from financial gain and economic advantage to pre-positioning, espionage, and disruptive and destructive attacks; ransomware remains the most immediate and disruptive threat to UK CNI, with state-linked groups now targeting industrial control systems (HMG, 2026). The obfuscation of the boundary between state and non-state actors is a structural feature of the current threat environment. The governance lesson underlines that defensive baselines must be attacker label or flag neutral.

There is good evidence that artificial intelligence is already increasing attacker productivity, accelerating malware development, and improving social-engineering effectiveness. There is much weaker evidence that autonomous, self-propagating, grid-disruptive AI malware has become an operational reality rather than a plausible future scenario. What can be claimed is that the speed and reach of intrusion campaigns are increasing, which is itself sufficient reason for operators and defenders to move faster than current compliance cycles typically allow.

The number of affected organisations has grown, testifying to the spill-over of effects across many smaller entities below the NIS2 definition of a large-scale incident. Without overwhelming or even triggering state response, the incidents cumulatively strain administrative and incident management capacity across sectors and borders, creating systemic pressure through persistent sub-threshold

activity (EuRepoC, 2026a). Reporting regimes and crisis mechanisms calibrated to single severe events will systematically under-count a threat environment whose real weight lies in accumulation.

Attackers quite typically pursue operational or financial effect through administrative IT and distributed-edge systems, not through direct control-room or OT intrusion. Security investment concentrated on bulk transmission and generation, while under-resourcing distribution, billing, and DER-facing systems, leaves those segments vulnerable.

Table 2 exemplifies six recent incidents which targeted and affected the energy sector. Each incident illustrates a distinct tactic, technique and procedures, but in each, a digital intrusion and its first-order effects cause second- or third-order physical effects. The attributions noted for the two European cases follow the EuRepoC record (EuRepoC, 2026a).

Table 2: Illustrative cyber-physical incidents affecting energy infrastructure

REGION	INCIDENT	PRIMARY TARGET	MECHANISM	OPERATIONAL OUTCOME
Europe	Coordinated attack on Polish wind, solar, and CHP assets (Dec. 2025)	30+ distributed generation sites	Coordinated intrusion into DER control pathways; December 2025 advisory links responsible proxy ecosystem to GRU unit 74455 (Sandworm)	Thwarted before systemic impact; assessed by EuRepoC as the first large-scale coordinated operation against DERs across multiple sites simultaneously (EuRepoC, 2026a)
Europe	Seizure of Lake Risevatnet hydropower dam controls, Norway (Apr. 2025)	Hydropower dam control systems	Remote takeover of operational controls by Z-Pentest, a proxy group founded by GRU-linked CARR members	Floodgate valve opened at full capacity for hours before detection; direct cyber-to-physical effect (EuRepoC, 2026a)
North America	Volt Typhoon / Voltzite pre-positioning	U.S. electric utility (Littleton Electric)	Living-off-the-land persistence using legitimate admin tools for 300+ days	No immediate disruption; exfiltration of network mapping data consistent with preparation for future disruption
Latin America	Administrative-systems ransomware against PDVSA	Venezuela’s state oil company	Ransomware targeting logistics and administrative systems during geopolitical tension	Cargo operations halted without any direct attack on physical infrastructure
Asia-Pacific	Combined DDoS and intrusion campaign against Indian power-sector systems	Power grid and coalfield administration	High-volume DDoS used to mask a separate intrusion campaign	Prompted Japan and other regional states to review active cyber-defence postures
Africa	Prepaid-token fraud against Eskom’s vending system	South Africa’s national utility	Exploitation of vulnerabilities in the electricity-token vending platform	Estimated revenue loss in the billions of rand, degrading capacity for physical maintenance

Table No 2. Illustrative cyber-physical incidents affecting energy infrastructure. EuRepoC (2026a); EuRepoC (2026b); CSIS (2026); Dragos (2026). Author’s compilation.



An analysis of state-on-state cyber operations identifies three recurring enabling condition categories behind successful cyber operations, only one of which is technical: infrastructure, technology and organisation; government, politics and law; and socio-cultural and human factors (Tikk, Hovhannisyan & Kerttunen, 2020). A governance strategy built to address only one type of enabler leaves other systemic vulnerabilities wide open.

Infrastructure, technology and organisation. Generic, undifferentiated security levels applied to high-value assets; reliance on obsolete equipment without upgrade paths; dependence on compromised or poorly secured third-party remote-access services; and lax patching and credential hygiene. In the energy sector this is precisely the mechanism behind the Polish incident, a compromised VPN credential reaching protection-relay firmware, and the pattern of unpatched, vendor-diverse DER hardware.

Government, politics and law. Legal and policy frameworks that lag behind the pace of technological change; unresolved questions of jurisdiction and responsibility; and inconsistent consequences for tolerated intrusion. In the energy sector this signifies the above-identified DER-aggregation governance gap, a dispatch layer that exists technically but has no clear regulatory home, as

> **A governance strategy built to address only one type of enabler leaves other systemic vulnerabilities wide open.**

well as the enforcement-capacity gap, which will be discussed later.

Socio-cultural and human factors. DER ownership being spread across households, commercial building operators, and aggregators, typically equals low awareness of cyber risk and a normalised tolerance of incidents rather than active resistance to them. Accordingly, a governance framework aimed at generation and distribution operators does not, on its own, reach that population, even where the technical and legal strategies are fully implemented.

Table 3 maps the principal cyber risk against each digitalisation pillar; prioritisation should track where risk is concentrated.

Table 3: Digitalisation pillars and their principal cyber-physical trade-off

DIGITALISATION PILLAR	PRINCIPAL OPERATIONAL BENEFIT	PRINCIPAL CYBER-PHYSICAL RISK
AI-driven load balancing	Reduced renewable curtailment; real-time frequency stabilisation	Manipulated telemetry triggering unnecessary automated load shedding
DER and IoT integration	Full visibility of distributed assets	Botnet-style exploitation of unpatched inverters and chargers
Cloud-native OT / virtualisation	Lower hardware footprint; rapid software-defined updates	Loss of physical air-gap enabling lateral movement from IT to control systems
Predictive maintenance (digital twins)	Extended asset life; fewer unplanned outages	Exfiltration of digital-twin data as a blueprint for physical sabotage
Smart metering and demand response	Optimised billing and peak-load management	Billing-system compromise and extortion targeting consumer data

Table No 3. Digitalisation pillars and their principal cyber-physical trade-off. ENISA (2024); Idaho National Laboratory (2026); MITRE (2025); Dragos (2026). Author’s compilation.



4.1 Edge – Core Problematique

Distributed, software-controlled, and consumer-owned assets are populating the edge of a new energy system at a pace that existing governance frameworks were not designed to accommodate. Cyber incidents signify the tendency. The Polish December 2025 operation and the Norwegian dam seizure were not accidents of geography, but deliberate targeting of the layer where regulatory oversight is weakest. The question this chapter firstly addresses is how compliance can be structured to govern that edge. Secondly, we turn attention to how obligations derived from those standards can be assigned to, verified across, and enforced upon a radically more diverse group of actors than the rather unified population for which compliance regimes were originally built.

The governance challenge is structural. In the bulk-power system, compliance is tractable since a small number of large, licensed operators hold assets that regulators can identify, inspect, and sanction. The DER layer inverts every one of these conditions. Millions of devices are owned by actors who have no licensing relationship with a grid regulator, procured through retail channels from manufacturers across multiple jurisdictions, operated by individuals or aggregators whose security competence varies, and connected to distribution utilities without contractual authority over the devices themselves. A compliance regime addressing this layer as if it were a smaller version of the bulk-system compliance regime will fail because the problem is not one of scale but of kind.

We argue for an approach which would clearly define compliance obligations; set tiered baseline requirements calibrated to the actor’s role and the asset’s systemic risk; design a verification architecture that does not presuppose an auditable professional operator at every point; and create an accountability structure assigning consequences for non-compliance to the actor with the greatest capacity to influence compliance, often the device or system owner at the edge of contemporary and asymmetric energy ecosystem.

The notions “edge” and “core” describe a structural rather than a physical relationship. The core, for purposes of this report, is the set of systems whose security is already addressed by established compliance regimes: bulk transmission and generation subject to NERC CIP in North America; entities designated as operators of essential services under NIS2 in the EU; critical information infrastructure under China’s Cybersecurity Law and similar national frameworks. The edge exists outside the defined perimeters. The boundary moves outward as DER penetration grows but the asymmetry remains

between the core which is governed and the edge which is not.

The security consequence of this asymmetry is direct. The core energy system, serving a wider base of societal and industrial functions, can be targeted from the edge. For example, a compromised aggregator controlling a virtual power plant can issue dispatch commands to tens of thousands of devices simultaneously producing a coordinated load event that the grid operator sees as a physical disturbance without a visible cyber cause. The Polish December 2025 operation demonstrated that attackers already conceptualise the DER fleet as a coherent target, even a coherent vector.

State cybersecurity strategies, critical infrastructure protection laws, and national security policies constitute the core’s governance layer at the political level. When DER assets are ungoverned at the edge, state critical infrastructure becomes also exposed to politically motivated attacks. The 2020’s incident record shows this pattern already in operation.



In the bulk-power system, compliance is tractable since a small number of large, licensed operators hold assets that regulators can identify, inspect, and sanction.

4.2 Standards as Foundations

International standards provide a technically sound foundation for DER compliance requirements. The challenge is their distribution across three distinct stakeholder groups — asset owners, system integrators, and component manufacturers — and the absence of a governance mechanism that assigns and enforces obligations across all three simultaneously. Where standards exist, national regulation has typically required compliance for only one group, leaving the others unaddressed.

The IEC 62443 series is the primary international standard for industrial automation and control system security, and its stakeholder structure maps directly onto the DER actor ecosystem. IEC 62443-2-1 (revised 2024) specifies security programme requirements for asset owners, organised around Security Programme Elements (SPEs) with a four-level maturity model (Initial, Managed, Defined, Improving) and explicit harmonisation with ISO/IEC 27001 to avoid duplication (ISA, 2025; IEC, 2026). IEC 62443-2-4 addresses the security requirements for system integrators, the entities, including DER aggregators and installation companies, which design and commission energy systems on behalf of asset owners. IEC 62443-4-1 and 4-2 specify secure product development requirements for component manufacturers, including inverter and smart meter producers. The standard’s Security Level framework, SL-1 (protection against casual or coincidental violation) through SL-4 (protection against state-level attackers with extended resources), provides a risk-proportionate basis for tiering compliance obligations by asset criticality.

Three features of IEC 62443 are particularly relevant to the DER compliance problem. First, security is explicitly a shared responsibility across the supply chain, not a problem assigned solely to the operator at the end: the standard requires that manufacturers, integrators, and asset owners each discharge obligations appropriate to their role and their position in the system lifecycle. Second, the zone-and-conduit model — dividing a system into security zones with defined communication conduits between them — provides a practical basis for treating the edge-core boundary as a governed interface rather than an open connection. Third, the standard is sector-agnostic, designed as a horizontal baseline onto which sector-specific requirements can be layered, the layering relationship this chapter’s compliance promotes.

NIST CSF 2.0, released in February 2024, adds a governance architecture that IEC 62443 does not directly provide. The new Govern function establishes that an organisation’s cybersecurity risk management strategy, expectations, and policy must be “established, communicated, and monitored” at the executive level, and that governance activities are critical for incorporating



Where standards exist, national regulation has typically required compliance for only one group, leaving the others unaddressed.

cybersecurity into broader enterprise risk management (NIST, 2024). The Govern function’s supply chain risk category explicitly requires organisations to audit their vendor ecosystems — directly addressing the DER hardware procurement problem described in Chapter 2. The CISA Cross-Sector Cybersecurity Performance Goals 2.0, aligned to CSF 2.0, operationalise the Govern function for critical infrastructure owners through specific, measurable outcomes rather than procedural requirements (CISA, 2025). Together, IEC 62443 and NIST CSF 2.0 / CISA CPG 2.0 cover the technical and organisational dimensions of a DER compliance baseline. What neither resolves is the question of regulatory authority, of mandate to require compliance from actors who currently have no licensing or regulatory relationship with the bodies administering these frameworks.

ISO/IEC 27001:2022 provides the third relevant layer: an information security management system (ISMS) standard that is widely certified, internationally recognised, and explicitly harmonised with IEC 62443-2-1. For aggregators, virtual power plant operators, and other DER intermediaries that operate primarily as digital platforms rather than physical infrastructure operators, ISO 27001 certification provides a credible, auditable compliance pathway. Several national frameworks, such as India’s CEA Guidelines and the EU’s NIS2, accept management-system certification as evidence of compliance with their substantive requirements, making ISO 27001 a practical bridge between the DER platform layer and national regulatory obligations.

What the standards collectively leave open is the compliance obligation for the individual device owner. Neither IEC 62443 nor NIST CSF 2.0 was designed for this citizen-operator. ISO 27001 certification is not realistic at this scale, either. The technical answer is to push compliance obligations upstream to the manufacturer (via product standards such as the EU’s CRA), to the installer (via grid connection requirements), and to the aggregator (via market and licence conditions). This would ensure that individual devices are compliant by the time they are connected and without requiring the owner to be a competent cybersecurity actor. Such secure-by-design principle requires a regulatory authority with jurisdiction over each of these upstream actors.

4.3 A Model Compliance Framework for the DER Layer

Drawing on the principles of governance and the standards reviewed above, we model a compliance framework organised around four pillars, or: aspects,scope, baseline obligations, verification, and accountability. The framework produces a governance architecture for assigning and enforcing compliance with those standards across the diverse actor population of the DER layer. Each pillar addresses one of the structural conditions that makes DER compliance harder than bulk-system compliance. Together, the pillars constitute a minimum viable compliance architecture, maybe even a norm, for any jurisdiction seeking to close the edge-core gap.

Pillar 1: Scope – Who Must Comply

Compliance obligations for the DER layer must be assigned by actor role and capacity to ensure security and not automatically by asset ownership. The following role taxonomy, derived from the IEC 62443 stakeholder model and the aggregator frameworks emerging in EU and Australian regulation, provides a tractable basis for scope definition.

Table 4: DER compliance scope by actor role

ACTOR ROLE	EXAMPLES	PRIMARY COMPLIANCE BASIS	OBLIGATION LEVEL	REGULATOR WITH JURISDICTION
Component manufacturer	Inverter OEM, smart meter supplier, EV charger manufacturer	IEC 62443-4-1/4-2; EU Cyber Resilience Act; national product safety law	Product: secure-by-design, SBOM, patch support commitment, vulnerability disclosure	Product/market regulator; customs and standards authority
System integrator / installer	DER installer, energy service company, microgrid developer	IEC 62443-2-4; grid connection code requirements; licence conditions	Installation: authenticated device commissioning, default credential removal, network segmentation at connection point	Distribution system operator (connection gate); licensing authority
Aggregator / Virtual Power Plant operator (VPP)	DER aggregator, virtual power plant operator, demand-response provider	IEC 62443-2-1; ISO/IEC 27001; NIS2 (EU); CEA Guidelines (India); SOCI Act (Australia)	Platform: ISO 27001 or equivalent ISMS; platform security assessment; incident reporting to CSIRT; supply-chain vendor vetting	Energy regulator; national cybersecurity authority (NIS2 or equivalent)
Distribution system operator (DSO)	Electricity distribution utility, cooperative, municipal utility	Sector-specific national regulation; NIS2 (EU); NERC CIP where applicable (North America)	Network: asset inventory for all DER connections; monitoring of grid-edge communications; incident notification to TSO and national authority	National energy regulator; national cybersecurity authority
Individual asset owner	Household, SME, building owner with behind-the-meter DER	Relies on upstream compliance; minimum awareness obligation at point of connection	Baseline: relies on secure-by-design devices and compliant installation; minimum obligation: follow installer baseline notice; report outages to DSO	No direct regulator outside basic cyber hygiene; compliance primarily achieved through upstream activities

Table No 4. DER compliance scope by actor role. IEC (2026); ISA (2025); NIST (2024); CISA (2025); European Commission (2025); European Union (2026); Australian Government (2024); Central Electricity Authority (2021). Author’s compilation.

The proposed logic finds support in emerging national practices. The UK Energy Sector Cyber Security Strategy 2026 proposes Cyber Essentials as a baseline for all Ofgem licensees, explicitly extending compliance scope beyond existing NIS operators to entities previously outside the regulatory perimeter (HMG, 2026). The Cyber Security and Resilience Bill, introduced to Parliament in November 2025, would give UK regulators broader scope, stronger incident-reporting obligations, and a fuller enforcement toolkit, mirroring the EU legislative trajectory.

The most efficient point of intervention is upstream: a compliant device from a compliant manufacturer, installed by a compliant installer, connected through a compliant aggregator, achieves coverage without requiring the citizen-operator to be a competent cybersecurity actor. The aggregator is the pivotal compliance node with both the technical access to the fleet and a commercial relationship which can carry regulatory obligations. The distribution system operator’s obligation is one of visibility, maintaining a verified inventory of connected DER assets and monitoring the grid-edge communications layer rather than direct security management of each device. Without this visibility, neither the distributed system operators nor any national authority can assess whether other actors, functions and levels are performing as required.

Pillar 2: Baseline Obligations – What Must Be Achieved

Baseline obligations should be outcome-specified rather than prescriptively technical. They can be calibrated to Security Level 2 of IEC 62443 (protection against intentional violation using simple means) as the minimum floor for grid-connected DER assets, with higher Security Levels required for assets above defined capacity thresholds or designated as high-impact under national CII frameworks. SL-2 is the appropriate floor because it corresponds to the threat pattern most frequently observed in the incident record: opportunistic attacks exploiting default credentials, unpatched firmware, and open remote access.

Manufacturers must demonstrate that devices shipped for grid connection are secure by default: no hardcoded credentials, firmware integrity verification, documented patch support lifecycle (minimum five years for grid-connected devices), a Software Bill of Materials, and a vulnerability disclosure programme with defined response timelines. The EU Cyber Resilience Act, which enters its core compliance phase in 2026-2027, provides the most developed legal expression of these requirements for the EU market (European Commission, 2025). Where the CRA does not reach, for example, equipment procured outside EU market reach, development-bank financing

conditions and grid-connection codes are the practical substitute.

Installers must apply a commissioning checklist as a condition of grid-connection approval: removal of default credentials, firmware version verification against the manufacturer’s current release, network segmentation between the device and any domestic or commercial IT network, and registration of the device in the DSO’s flexibility resource registry. The connection-gate mechanism is both the most powerful and the most underused compliance lever in the current regulatory landscape. Extending it to include a minimum cybersecurity commissioning check requires no new regulatory authority in most jurisdictions but only that an existing grid-code obligation be updated to include a cybersecurity condition.

Aggregators must maintain a security management system equivalent to ISO/IEC 27001 or a sector-specific equivalent, conduct an annual penetration test or security assessment of their platform, maintain an inventory of all connected devices with firmware version and patch status, and report significant incidents to the relevant national CSIRT within the timelines specified in applicable national law. In short, compliance should be made a licence condition for aggregators.

Distribution system operators (DSO) must maintain a verified registry of all DER assets connected to their network, implement anomaly detection on distribution-level communication flows, establish a clear incident escalation path to the national cybersecurity authority, and incorporate DER cybersecurity risk into their network risk assessments. The IEA’s flexibility resource registry recommendation serves both the market-integration and security-visibility functions simultaneously (IEA, 2022) as a registry which records asset identity, capacity, and connectivity also records the attack surface.

Pillar 3: Verification – How Compliance Is Assessed

Verification architecture must match the diversity of the actor population. For manufacturers, product certification against IEC 62443-4-2 or an equivalent national product standard, conducted by an accredited third-party laboratory, provides the verification mechanism. The EU’s CRA conformity assessment regime is the most mature expression of this. Where product certification is not yet required, market surveillance authorities can use sampling-based post-market testing by drawing devices from retail channels and testing against the baseline.

For installers, the connection-gate commissioning check is itself the verification event. The DSO or grid authority approving the connection confirms that the commissioning checklist has been completed and records the result

in the flexibility resource registry. For aggregators, third-party audit against ISO/IEC 27001 or equivalent provides annual verification. Incident reporting data also functions as a continuous, risk-proportionate verification mechanism: an aggregator that reports incidents demonstrates operational awareness; one that never reports warrants closer scrutiny. The safe-harbour model, protecting good-faith reporters from punitive use of reported information, is essential for this mechanism to function. For distribution system operators (DSO), the national energy regulator's existing audit and inspection powers provide the verification mechanism, extended to cover cybersecurity as a component of the DSO's operational licence obligations.

Pillar 4: Accountability – Consequences and the Assignment of Responsibility

Compliance without accountability remains aspirational. Effective accountability for DER compliance

requires two design choices that most current frameworks have not made. The first is to concentrate accountability on the actors with the greatest capacity to influence compliance outcomes. An accountability regime imposing the same obligations on all actors is neither equitable nor efficient. The most productive regulatory design assigns accountability to the actor best placed to act, not to the actor closest to the individual device.

The second design choice is to make market access conditional on compliance. Licensing, market participation, and financing conditions are more effective levers for DER actors than penalty-based enforcement after the fact, because the populations involved are too diverse and too numerous for systematic ex post inspection. An aggregator that cannot demonstrate compliance loses its licence to participate in the energy market; a manufacturer whose products fail post-market testing loses CE marking and therefore EU market access. Development-bank financing conditions serve the equivalent function in jurisdictions where domestic regulatory capacity is insufficient to impose market-access conditions directly.

4.4 From Framework to Practice: The Implementation Problem

Proposing a compliance framework is easier than implementing one. A consistent finding in the academic and policy literature is that compliance-based cybersecurity strategies generate structural weaknesses even when formally satisfied: organisations turn security into a set of discrete, auditable controls that can be implemented, documented, and certified without building actual resilience. Power (2007) named this pattern “organised hypocrisy” — the presence of formal structures and processes that satisfy external verification requirements while leaving operational exposure unchanged. Checklist compliance meets auditors and protects organisations against liability; it does not necessarily protect against adversaries (Adabara et al., 2024; Akinsola, 2025).

A model compliance framework defined by scope, baselines, verification, and accountability is only as effective as the governance architecture that implements it. A designated authority must hold responsibility for the DER layer. The current fragmentation of regulatory authority among energy regulators, cybersecurity authorities, product safety agencies, and market regulators means that no single body owns the DER compliance gap as a regulatory problem. The first governance condition for an effective compliance framework is assignment of authority to define, enforce, and report on DER compliance. Without this assignment, the framework exists as policy aspiration rather than regulatory practice.

A national cybersecurity or energy security strategy is the instrument that performs this codification at the political level. A strategy, properly understood, is more than a declaratory document: it is a balanced calculation which provides political guidance, chooses between policy options, prioritises objectives, allocates resources and responsibilities, legitimises the chosen direction, and informs domestic and international audiences (Kerttunen & Tikk, 2019). A jurisdiction without a current, implemented strategy, or one that never resolved who is responsible for the distribution and DER layer, exhibits the legal-political enabling condition in its purest form: unallocated responsibility, lagging frameworks, and no authoritative statement of priorities against which performance can be audited. Within the EU, adopting a national cybersecurity strategy is a legal obligation under NIS2 (European Union, 2026). A strategy is contingent and must be tailored to the political, operational, financial, and technological realities of the jurisdiction; standardised, checklist-driven strategies imported wholesale contradict the very nature of strategy, and the mastery of strategy lies in optimal allocation rather than maximal pursuit (Kerttunen & Tikk, 2019). ENISA's National Capabilities Assessment Framework offers a ready-made instrument for the maturity self-assessment that strategy development and lifecycle review require (ENISA, 2023).

The governance architecture through which the compliance framework operates must also be specified. A central authority or office, within the energy ministry, the national cybersecurity authority, or shared between them by explicit agreement, plans, coordinates, steers, and supervises sector cybersecurity policy and its implementation. Implementation of mandated measures takes place at the technical or specialist level closest to the assets: utilities, distribution system operators (DSO), aggregators, and device certifiers. Tasks demanding wider scope or deeper specialisation, including sector CSIRT functions, supply-chain verification, and cyber intelligence on energy-sector threats, are concentrated in a competent national agent rather than duplicated across operators. Relationships and the division of labour between the central authority, its agencies, and the private operators of critical energy services including DER aggregators are defined in binding and non-binding instruments: contracts, licence conditions, agreements, and memoranda of understanding. Models of cooperation and interaction, covering information-sharing fora and platforms, agreed terms of reference, and principles of mutual and external communication, are defined in advance, not improvised during incidents. The implementation and efficiency of sector cybersecurity policy, and the performance of all designated actors are continuously monitored, annually reported, and audited in the same way as any other national policy area.

The choice between centralisation and decentralisation is not either-or but a matter of calibrated balance. Given the near-simultaneous appearance of harmful cyber effects across interconnected systems and the scarcity of skilled personnel, unqualified subsidiarity in incident management can lead to unintended escalation; some functions must be centralised precisely so that distributed operators are not left to face sophisticated adversaries alone. We are, however, sceptical whether any single agency or unit can master the diversities and combination of cybersecurity and distributed energy resources; this reservation is built into the model above through the division between central steering and distributed implementation. A central governing body exercises three distinct modes: fiduciary (financial discipline and oversight), strategic (aligning internal capability with external opportunity), and generative (framing the problems that drive policy). Governance is effective only when all three are present. A sector regulator that audits compliance but cannot frame emerging problems such as aggregation-layer risk is exercising one mode of three, and the gap will show precisely where the threat landscape is changing fastest.

Evaluation of the compliance framework should measure more than inputs (resources committed) and outputs (activities performed): it should measure outcomes, meaning verifiable change in the sector's security condition against politically agreed objectives. For the compliance framework proposed in this chapter, that means track-

ing movement in the exposure: the share of DERs with authenticated device identity, the proportion of aggregators inside the regulatory perimeter, verified supply-chain disclosure coverage, reporting rates under safe-harbour arrangements, and the share of new grid-connected assets that have passed a commissioning cybersecurity check. These are metrics which distinguish a compliance framework that is producing security outcomes from one that is producing audit records.

The instrument mix: sticks, carrots, and sermons

Government has three classes of policy instruments available to move private-sector operators towards compliance: authority-based mandates (“sticks”), incentive-based measures (“carrots”), and information-based approaches (“sermons”). Each operates on a different behavioural mechanism, and effective implementation typically requires combinations rather than reliance on any single class (Auld et.al., 2010; Choi & Ghez, 2026). Mandates establish a floor below which performance cannot legally fall, but they are costly to enforce across large, diverse actor populations, and produce organised-hypocrisy dynamics when penalties make documented non-compliance cheaper than genuine compliance. Mandates are credible and necessary for manufacturers, aggregators, and DSOs as these populations are small enough to be systematically audited. Incentive-based instruments reach actors for whom compliance costs exceed their perceived security benefit, which describes most individual DER owners and many small installers. Development-bank financing conditions are the most powerful existing incentive instrument for DER compliance in regions where domestic regulatory capacity is limited (Hiller, 2024). Information-based instruments, (such as guidance documents, sector advisories, threat-sharing platforms, training programmes) address the awareness and technical complexity barriers that research identifies as the primary obstacles for smaller operators. A 2025 study of NIS2 compliance barriers found that lack of awareness, technical complexity, financial constraints, and regulatory uncertainty were the four principal barriers for entities newly brought into regulatory scope (Adabara et al., 2024).

The capacity and harmonisation problems

Even where mandates, incentives, and information are all in place, organisations cannot comply with requirements they lack the technical personnel to understand and implement. The global cybersecurity workforce shortfall is estimated at 3.4 million professionals, concentrated precisely in the sectors and regions where DER growth is

fastest (Adabara et al., 2024). The UK Energy Sector Cyber Security Strategy 2026 names this challenge directly: the UK faces a significant shortage of professionals with the required combination of cyber and engineering skills, with an insufficient number of security-cleared industry staff (HMG, 2026). This combined cyber-and-OT competence gap is not a UK-specific phenomenon; it is the workforce dimension of the structural problem the compliance framework must work around.

The design responses able to address the workforce issue include shared regional compliance support centres that pool assessment and advisory functions across multiple operators, tiered safe-harbour protections for operators demonstrating active engagement with a recognised compliance pathway during a defined transition period, and development of a commercial certification market so that compliance services are available at scale beyond what regulators can provide alone. A parallel structural barrier is regulatory fragmentation. For example, a 2025 US GAO report found that federal agencies have made limited progress in harmonising cybersecurity regulations, with industry representatives reporting that overlapping requirements consume resources that would otherwise fund actual security improvement (GAO, 2025). Our compliance framework is outlined to be harmonisation-compatible. It specifies requirements for qualitatively different actors and the defined outcome levels allow different jurisdictions to map their existing

instruments to the same framework without requiring identical technical specifications.

The lifecycle problem

Compliance tends to be treated as a state of affairs rather than a continuing process. Academic analysis consistently finds that organisations achieving certification at a point in time experience security degradation as threats evolve and systems age without corresponding obligation to update (Adabara et al., 2024). For the DER layer, e.g. inverters, smart meters, and EV chargers installed to the security baseline of 2024 will, without ongoing obligation, be running unpatched firmware on known-vulnerable configurations by 2028. Lifecycle compliance requires instruments that most current frameworks do not yet deploy: mandatory patch-deployment timelines for grid-connected devices, verified at the point of connection; periodic re-attestation for aggregator platform certifications rather than one-time certification; and scheduled regulatory review cycles that update baseline obligations as the threat landscape evolves, rather than leaving organisations to comply indefinitely with a standard written for the threat environment of its promulgation year.

The IEC 62443-2-1 maturity model explicitly addresses the lifecycle issue by requiring the security programme at the ‘Improving’ level to include continuous monitoring and systematic improvement.

Table 5: Model compliance framework – summary

PILLAR	CORE QUESTION	PRIMARY INSTRUMENT	KEY STANDARD/REFERENCE	GOVERNANCE PRECONDITION
Scope	Who must comply?	Actor-role taxonomy (manufacturer / installer / aggregator / DSO / owner)	IEC 62443 stakeholder model; IEA flexibility registry	Designated authority with mandate across all actors (stakeholders)
Baseline obligations	What must each actor achieve?	Outcome-specified requirements calibrated to IEC 62443 SL-2 as minimum floor	IEC 62443-2-1/2-4/4-1/4-2; NIST CSF 2.0 Govern; CISA CPG 2.0; ISO/IEC 27001	Updated grid codes and market/licence conditions carrying baseline into regulatory obligation
Verification	How is compliance assessed?	Differentiated by: product certification; connection-gate commissioning; third-party audit; regulatory licence audit	CRA conformity assessment; IEC 62443-4-2 certification; ISO 27001 audit; ENISA NCAF	Audit infrastructure and accredited assessment bodies; safe-harbour for incident reporting
Accountability	What follows non-compliance?	Market-access conditionality: loss of grid connection, market participation, CE marking, or financing access	EU CRA; SOCI PSOs (Australia); NIS2 supervisory powers; IDB/World Bank financing conditions	Political decision to make market access conditional; resourcing of enforcement bodies

Table No 5. Model compliance framework – summary. IEC (2026); ISA (2025); NIST (2024); CISA (2025); European Commission (2025); Australian Government (2024); IEA (2022); ENISA (2023). Author’s compilation.



5 Regional Governance Approaches

Public policy governance models differ by continent, region and jurisdiction. Historical legacies, political cultures, objective realities such as geography, financial and human resources, and contemporary geopolitics condition immediate and long-term ambitions, the balance between binding and enforced regulations and voluntary and non-binding guidance, and the degree of centralisation and decentralisation. Political cultures, in particular, affect

the roles and responsibilities of the state, the individual, and the private sector — a question of direct importance in designing governance for diversified energy resources. This chapter examines each region through the lens of the above-developed four-pillar compliance framework, asking how far the existing governance architecture advances or constrain the scope, baseline obligations, verification, and accountability of DER-layer compliance.

5.1 European Union

The EU is the legally most comprehensive model in this comparison, and the electricity sector is the clearest example of why: it is regulated by both a horizontal law and a sector-specific one. Assessed against the four compliance pillars, the EU has made the furthest progress of any jurisdiction examined, but significant gaps remain in defining scope and verification for the DER layer specifically.

SCOPE NIS2 classifies energy as a high-criticality sector, and the Network Code on Cybersecurity for cross-border electricity flows (NCCS, Commission Delegated Regulation (EU) 2024/1366) designates transmission and distribution operators as the primary compliance actors (European Commission, 2024; European Union, 2026). The Cyber Resilience Act extends obligations to product manufacturers (European Commission, 2025). However, NIS2 entity obligations do not clearly reach aggregators operating virtual power plants across multiple member states unless they cross the thresholds that trigger “important entity” classification. Grid-connection codes do not yet universally require a cybersecurity commissioning check for installers either. The device owner has no direct regulatory obligation beyond the CRA’s product requirements.

BASELINE OBLIGATIONS NIS2 reporting timelines — 24-hour early warning, 72-hour incident notification, one-month final report — are defined and binding for entities in scope (European Union, 2026). The ECII asset classification under the NCCS introduces risk-proportionate tiering (high-impact / critical-impact) for cross-border electricity assets, with heavier obligations at each tier (ACER, 2024). The CRA mandates secure-by-design and conformity assessment for connected digital products. Compliance with the NCCS can serve as evidence of NIS2 compliance and vice versa, a deliberate design choice to avoid duplicative audits. For assets and actors outside these perimeters — distribution-level DER hardware and smaller aggregators — the baseline obligations are advisory rather than binding.

VERIFICATION The CRA conformity assessment regime provides the product certification mechanism. NIS2 establishes supervisory powers for national competent authorities to audit entities in scope. The NCCS requires designation of a national competent authority for the electricity sector by each member state by December 2024 (European Commission, 2024). The main weakness is not the design of the verification instruments but their application: enforcement quality still depends on national implementation capacity and resourcing, producing uneven outcomes at member-state level — precisely the enforcement-capacity gap this report treats as regionally, not technically, determined.

ACCOUNTABILITY NIS2 supervisory powers include fines of up to 2% of global annual turnover for important entities and 10 million euros for essential entities that fail to meet obligations. The CRA introduces market surveillance mechanisms with the power to withdraw CE marking. Supply-chain diversification is treated as both a cybersecurity and an industrial-policy tool through the Critical Raw Materials Act. The accountability gap is the aggregator and installer level below the NIS2 essential-entity threshold: the path of consequence from a DER-layer incident back to a regulatory sanction is unclear for the majority of the new intermediary layer.

5.2 United Kingdom

The United Kingdom, post-Brexit, operates outside the EU regulatory perimeter but on a convergent trajectory. The NIS Regulations 2018 remain the primary regulatory lever for energy-sector cybersecurity. Ofgem and the Department for Energy Security and Net Zero jointly regulate Downstream Gas and Electricity under NIS. The Energy Sector Cyber Security Strategy 2026 sets a four-year plan to expand scope across the whole energy system, raise baseline resilience through licence conditions and international standards, and build supply chain security assessment capability by end 2027, with critical suppliers designated by 2030 (HMG, 2026). Assessed against the four compliance pillars: scope is currently limited to NIS operators but explicitly planned to expand to all Ofgem licensees; baselines will be extended through the CSRB and licence conditions; verification is being strengthened through the Cyber Resilience Audit framework; and accountability gains a fuller enforcement toolkit under the CSRB subject to Royal Assent.



5.3 United States

The United States has no single federal cybersecurity regulator for the energy sector. Responsibility is distributed across federal agencies, independent regulators, and fifty state jurisdictions, each with its own statutory authority and enforcement capacity. Assessed against the four compliance pillars, the US has strong baseline obligations and partial accountability at the bulk level, but has made minimal progress on the DER layer scope, verification, and accountability.

SCOPE	NERC’s mandatory CIP standards apply only to Bulk Electric System (BES) assets, that is transmission facilities at 100 kV or above and generation aggregating 75 MVA or more, representing roughly 10-20% of the physical grid asset base (Idaho National Laboratory, 2026). Even NERC’s Operations and Planning standards, which now extend to inverter-based resources of 20 MW or more, carry no corresponding CIP cybersecurity requirement, so a growing share of grid-connected renewable capacity sits inside NERC’s reliability mandate but outside its cybersecurity one. Below the BES threshold, regulatory authority passes to the states, and the cooperative and municipal sector representing a large share of DER-connected distribution capacity falls largely outside PUC jurisdiction. Aggregators, VPP operators, and DER installers have no systematic federal cybersecurity compliance scope. The constitutional division between federal and state authority is the structural fact that conditions every other element of US energy-sector cybersecurity governance.
BASELINE OBLIGATIONS	At the bulk level, NERC CIP standards provide detailed, enforceable technical obligations. The principal federal response at the distribution and DER level has been non-binding. For example, in February 2024, NARUC, funded by DOE’s CESER, published voluntary Cybersecurity Baselines for Electric Distribution Systems and DER, intended to give states a common starting point rather than a mandate (NARUC & U.S. Department of Energy, 2024). Whether individual states adopt them is discretionary, which clearly illustrates a technically sound baseline failing to close a governance gap because the institutional mechanism to enforce it is absent.
VERIFICATION	At the bulk level, NERC conducts mandatory compliance monitoring and enforcement against registered entities. Below the BES threshold, verification is state-dependent and inconsistent. No systematic product certification or connection-gate commissioning requirement exists for DER hardware.
ACCOUNTABILITY	The Trump administration’s Cyber Strategy for America, released in March 2026, sets a more assertive national posture while simultaneously signalling a lighter regulatory touch (White House, 2026). The deregulatory emphasis is consequential: the strategy calls for reducing compliance burdens and regulatory fragmentation, which cuts against the direction of mandatory, sector-specific rulemaking. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), enacted in 2022, would introduce cross-sector accountability through mandatory reporting timelines (72 hours for significant incidents, 24 hours for ransomware payments), but the final rule has been delayed to mid-2026 at the earliest (CISA, 2026). CISA itself has lost roughly one-third of its workforce since January 2025 and has undergone a reorganisation that narrows its mission, further constraining the enforcement agency at the moment the compliance gap is largest.

5.4 Asia-Pacific

The Asia-Pacific region presents the widest range of compliance framework maturity in this comparison, from Australia’s advanced statutory model to the fragmented ASEAN sub-regional landscape.

CHINA SCOPE	China’s CII designation regime, mandated by the 2021 State Council regulation implementing the 2016 Cybersecurity Law, extends to the energy sector and subjects designated operators to materially heavier obligations under the Multi-Level Protection Scheme (MLPS) than ordinary networks (State Council of the People’s Republic of China, 2021). The scope does not clearly reach individual DER device manufacturers or installers below the CII threshold.
CHINA BASELINE OBLIGATIONS	The CSL 2026 amendments, effective 1 January 2026, increased penalty ceilings for CII operators tenfold, introduced personal liability for CISOs, broadened extraterritorial reach, and added AI governance provisions. The Measures on the Management of National Cybersecurity Incident Reporting, effective November 2025, tighten reporting timelines.
CHINA VERIFICATION	The Cyberspace Administration of China (CAC) carries oversight and enforcement functions; 2026 marks the first year of its new five-year cycle, characterised by a stated shift from monitoring to control.
CHINA ACCOUNTABILITY	Enforcement is centralised and intensifying; personal liability for senior managers is the most significant accountability innovation in the 2026 amendments. The governance model is coherent and its trajectory clear, even if its logic with centralised classification, tiered technical mandates, and state-controlled information flows operates on premises that diverge from the frameworks examined elsewhere in this chapter.
INDIA SCOPE	The Central Electricity Authority’s 2021 Guidelines mandated CISO appointments and 24-hour incident reporting for covered entities. The October 2025 draft CEA Regulations extend binding obligations to all entities operating OT infrastructure linked to the power system, i.e. generation, transmission, distribution, power exchanges, load dispatch centres, and ICT and control system vendors, materially broadening scope (Central Electricity Authority, 2021; 2025).
INDIA BASELINE OBLIGATIONS	The draft regulations mandate periodic security audits, mandatory incident reporting to CSIRT-Power within defined timelines, and specific OT asset protections representing the most extensive upgrade of India’s power-sector cybersecurity framework since the 2021 guidelines.
INDIA VERIFICATION	CSIRT-Power, established April 2023, provides the sector incident-response and verification function. The draft regulations require periodic audits.
INDIA ACCOUNTABILITY	Implementation will depend on enforcement capacity across a sector that spans hundreds of state and private utilities; the draft moves from guidance to binding obligation but the gap between legal obligation and operational enforcement remains significant. The trajectory is convergent with EU and international standards practice.

AUSTRALIA SCOPE	The SOCI Act, substantially amended by the Enhanced Response and Prevention Act 2024, designates 11 critical infrastructure sectors including electricity generation, transmission, and distribution, with Systems of National Significance (SoNS) carrying the heaviest obligations. By late 2024, over 200 SoNS had been designated. The Cyber Security Act 2024 extended IoT security standards to consumer devices. The scope gap is the same as elsewhere: third-party DER aggregators and installers are not directly within the SOCI perimeter (Australian Government, 2023; 2024).
AUSTRALIA BASELINE OBLIGATIONS	Three core Positive Security Obligations apply to asset owners: risk management programme adoption, government access for incident response, and mandatory incident reporting. SoNS carry enhanced obligations including mandatory cybersecurity exercises and vulnerability assessments. Ransomware payment reporting is mandatory under the Cyber Security Act 2024.
AUSTRALIA VERIFICATION	CISC (Cyber and Infrastructure Security Centre, Department of Home Affairs) combines regulatory, coordination, and incident-response functions under a single authority, resolving the fragmentation between sector regulators and the national cybersecurity agency that characterises the US and, to a lesser degree, the EU. Parliamentary oversight through the Joint Committee on Intelligence and Security provides independent scrutiny.
AUSTRALIA ACCOUNTABILITY	Market-access and licence conditionality exists for SOCI-designated entities; the 2023-2030 Cyber Security Strategy, entering Horizon 2 (2026-2028), is broadening obligations towards the economy as a whole. The aggregation-layer gap, that is the security obligations of third-party DER operators and aggregators, remains unresolved.
ASEAN	At the sub-regional level, ASEAN presents a more fragmented picture. The ASEAN Power Grid, proposed in 1999 with a 2045 full-integration target, had reached approximately 7.7 GW of interconnection capacity across nine of eighteen priority projects by 2026, a gap attributed more to the absence of a dedicated multilateral coordinating institution than to any shortage of technical or financing ambition. An ASEAN Regional Computer Emergency Response Team (ASEAN CERT) was launched in 2025, fulfilling a commitment under the ASEAN Cybersecurity Cooperation Strategy 2021-2025. Its successor strategy for 2026-2030 focuses on cyber readiness and capacity-building (ASEAN, 2025). The APAEC 2026-2030 does not incorporate cybersecurity as a programme area, and the cybersecurity cooperation strategy addresses critical infrastructure only in general terms. Against the four pillars, ASEAN has no binding regional compliance scope, no harmonised baseline obligations, no cross-border verification mechanism, and no shared accountability structure. National frameworks vary from advanced (Singapore, Malaysia) to nascent.

5.5 Africa

Africa’s compliance framework profile is defined by the distance between normative ambition and operational capacity. Against the four pillars, the continental and most national frameworks have made most progress on scope definition while baseline obligations, verification, and accountability remain largely undeveloped.

SCOPE	The African Union’s Malabo Convention, in force June 2023, requires member states to identify sectors including energy as critical information infrastructure (African Union, 2014; 2023). Nigeria’s Cybercrimes Amendment Act 2024 and accompanying CNII Order 2024 designate specific systems in the energy sector as Critical National Information Infrastructure, establishing a Trusted Information Sharing Network. Kenya’s Critical Information Infrastructure Regulations 2024 require continuous monitoring of designated energy systems. These represent genuine advances in scope definition at the national level; fewer than a third of AU states have ratified the Malabo Convention, and scope definition has not yet extended to the aggregators, installers, or manufacturers in any continental or most national frameworks (Ifeanyi-Ajufo, 2023).
BASELINE OBLIGATIONS	Most African national frameworks specify obligations at the general principles level — designate, protect, report — without the outcome-specified, tiered baselines that the compliance model requires. Nigeria’s CNII Order requires compliance from designated stakeholders without specifying the technical baseline. Kenya’s CII Regulations require continuous monitoring without specifying what monitoring technology or outcome constitutes compliance. The critical gap is the DER hardware layer: African energy infrastructure, particularly the mini-grids, solar-home systems, and prepaid metering platforms that constitute the DER layer across much of the continent, is overwhelmingly procured from international vendors with no continent-specific security baseline requirement.
VERIFICATION	Most African member countries lack the essential IT infrastructure to investigate and prosecute cybercrime, pointing to a systematic shortfall in enforcement capacity that affects energy-sector cybersecurity as much as any other domain (INTERPOL, 2025). INTERPOL’s coordinated capacity-building operations remain the primary verification and enforcement mechanism at the continental level, supplementing national CSIRTs where they exist. Product certification infrastructure for DER hardware does not exist at the national level in most African jurisdictions.
ACCOUNTABILITY	The primary accountability mechanism is development-bank financing conditions: the World Bank Mission 300 initiative and AfDB energy financing programmes carry implicit and sometimes explicit cybersecurity requirements as conditions of lending (World Bank, 2024; 2025). This is the most effective lever available given the absence of domestic enforcement capacity, but it reaches only development-bank-financed assets and only at the point of procurement. The structural constraint is not an absence of legal or normative ambition but a persistent gap between that ambition and the enforcement and technical capacity needed to act on it (AFREC, 2024). As security and development objectives align and can be mutually reinforcing, the African governance deficit is a concern not only for public cyber policy but for energy policy and economic governance more broadly.

5.6 Latin America & Caribbean

The region’s compliance framework profile has shifted since 2024. Chile’s Law 21.663 is the most operationally complete compliance framework for energy-sector cybersecurity in the region and a reference case for what a full four-pillar implementation looks like at national scale. Brazil signals intent to follow while the rest of the region remains at the early stages of defining scope.

SCOPE	Chile’s ANCI designated 915 Operators of Vital Importance in December 2025, including 307 organisations in electricity generation, transmission, and distribution (Chile, 2024; ANCI, 2025). This is the most specific DER-adjacent scope definition in the region. The OVI regime does not yet clearly reach aggregators or DER installers as distinct compliance actors, and the individual device-owner relies on upstream obligations not yet systematically implemented. Brazil’s Bill No. 4752/2025 in the Senate would establish a National Cybersecurity Authority with standard-setting and scope-defining powers but as of mid-2026 it had not been enacted. Elsewhere, development banks exert more influence over cybersecurity scope than domestic regulation.
BASELINE OBLIGATIONS	Chile’s OVI obligations of certified information security management systems, auditable business continuity plans, mandatory cybersecurity audits represent outcome-specified, verifiable requirements. The obligation is heavier than most EU member states apply below the NIS2 essential-entity threshold. Brazil’s ANEEL 2021 resolution sets minimum cybersecurity standards without the enforcement architecture Chile now provides. Elsewhere, obligations are advisory. Chile’s electricity sector had already been moving towards these obligations voluntarily before the law required them, as the 2021 CIGRE Chile industry master plan documented (CIGRE Chile, 2021), suggesting that domestic sector readiness is the precondition for effective baseline implementation.
VERIFICATION	Chile’s ANCI is not an advisory body but issues binding technical regulations, supervises OVIs, and can impose fines of up to 40,000 UTM for serious infractions. The sanctioning regime provides the verification and accountability mechanism that development-bank conditions cannot. Brazil alone accounts for as many ransomware and extortion incidents as the next five largest Latin American markets combined, a concentration of risk that the current verification-free governance framework is not designed to address. The OAS-IDB 2025 Cybersecurity Report finds that structural gaps in resources, talent development, and cross-sector coordination persist across 30 countries, with most of the region still without a current, implemented national strategy (Inter-American Development Bank & OAS, 2025).
ACCOUNTABILITY	Chile’s ANCI fining powers and OVI regime represent the most complete Pillar 4 implementation in the region. Development banks remain the primary accountability lever for the rest of the region through lending conditions and technical assistance. Academic research on private-sector disclosure confirms that accountability without enforcement produces systematically low and unevenly distributed cybersecurity disclosure across the region (Ramírez et al., 2022). Brazil signals intent to close this gap through the pending law; whether it does so while maintaining the momentum of its energy digitalisation programme is the central governance question for the region’s largest economy.

5.7 Cross-Regional Synthesis

Mapped against the four compliance pillars, the regional analysis reveals a consistent pattern where governance progress concentrates on scope definition for bulk actors while baseline obligations, verification, and accountability remain underdeveloped for the DER layer specifically. No jurisdiction has fully implemented all four pillars for the distributed edge. Table 6 summarises the assessment.

Table 6: Compliance framework maturity by region and pillar

REGION	SCOPE	BASELINE OBLIGATIONS	VERIFICATION	ACCOUNTABILITY
European Union	Strong for bulk and DSO; CRA reaches manufacturers; aggregators partially; absent for installers	Strong for entities in scope; ECII tiering for cross-border assets; advisory below NIS2 threshold	CRA conformity assessment (T1); NIS2 supervisory audits (T3/T4); national competent authority variation	NIS2 fines; CRA market surveillance; supply-chain conditionality; aggregator/installer accountability gap
United States	Strong for BES; no systematic federal scope below BES; state variation; aggregators, installers, and manufacturers unsystematic	Mandatory at BES (NERC CIP); voluntary baselines for distribution/DER (NARUC 2024); no federal mandate below BES	NERC compliance monitoring (BES only); no product certification or connection-gate requirement; CIRCIA verification pending	NERC enforcement (BES); deregulatory federal posture (2026 Cyber Strategy); CIRCIA accountability pending; CISA capacity reduced
Asia-Pacific	China: CII designation covers energy sector. India: draft 2025 regs extend to OT operators. Australia: SOCI covers generation/transmission/distribution. ASEAN: national variation	China: CSL 2026 tenfold penalties, personal liability. India: binding regs pending 2026. Australia: PSOs + SoNS obligations. ASEAN: varies	China: CAC enforcement intensifying (monitoring to control). India: CSIRT-Power + periodic audits. Australia: CISC integrated authority; JCIS oversight. ASEAN: ASEAN CERT 2025, no energy-specific verification	China: personal liability (CSL 2026). India: binding enforcement pending. Australia: licence conditions + market access. ASEAN: no shared accountability mechanism
Africa	Malabo Convention: energy as CII (principles only). Nigeria CNII Order 2024. Kenya CII Regs 2024. Most states: guidance only; no aggregator/installer/manufacturer scope	Principles-level only for most states. Nigeria/Kenya: continuous monitoring obligations. No technical baseline for DER hardware	Most states: insufficient IT infrastructure for verification. INTERPOL: capacity-building. No product certification or connection-gate mechanism	Development-bank financing conditions primary lever. Nigeria/Kenya fledgling national mechanisms. AU frameworks unenforced
Latin America & Caribbean	Chile: 915 OVIs incl. 307 electricity entities (Dec. 2025). Brazil: pending law. Elsewhere: development-bank scope only	Chile: ISMS certification, audits, business continuity (binding). Brazil: ANEEL resolution (advisory-level). Elsewhere: advisory	Chile: ANCI with binding powers and fining authority. Brazil: no verification mechanism. Elsewhere: IDB/OAS capacity-building only	Chile: ANCI fines up to 40,000 UTM; market conditionality emerging. Brazil: no enacted authority. Elsewhere: development-bank conditions only

Table No 6. Compliance framework maturity by region and pillar. CISA (2025); DCAF (2021); DCAF (2024); European Union (2026); European Commission (2024; 2025); ACER (2024); White House (2026); CISA (2026); Idaho National Laboratory (2026); NARUC & U.S. Department of Energy (2024); State Council of the People’s Republic of China (2021); CAC (2025); Central Electricity Authority (2021; 2025); Australian Government (2023; 2024); ASEAN (2025); African Union (2014/2023); INTERPOL (2025); Nigeria (2024); Chile (2024); ANCI (2025); Inter-American Development Bank & OAS (2025). Author’s compilation.

The most consistent regulatory gap across all regions concerns the aggregators. First, no jurisdiction has systematically made aggregator and VPP operator compliance a condition of market access, even though the aggregator is the pivotal compliance node in the four-pillar model. Second, product certification for DER hardware exists only in the EU through the CRA, and even there it does not yet reach assets procured outside EU market channels. Third, the accountability mechanisms that work, Chile’s ANCI fining powers, Australia’s SOCI licence conditions, the EU’s NIS2 supervisory sanctions, share a common design in which market access is conditioned on compliance, not retrospective penalty after an incident. The gaps documented above follow from the structural conditions that vary systematically across regions. Enforcement capacity determines whether a rule that exists on paper produces a differ-

ent real-world outcome than no rule at all. The EU’s member-state implementation gap and Africa’s enforcement-lags-ambition pattern are both instances of the same condition, despite very different starting points. Institutional trust determines whether formal reporting obligations produce transparency or underreporting: where operators fear punitive use of disclosed information, safe-harbour protections are a governance prerequisite. Distribution- and DER-level maturity determines the regulatory and technical complexity of the compliance problem. Regions with rapidly growing distributed generation need governance mechanisms that reach individual inverters, meters, and aggregators, a materially different problem from regulating a small number of large, licensed operators. Financing and workforce availability determines whether a technically sound baseline is practically achievable.



6 Recommendations: From Analysis to Action

The compliance framework in Chapter 4 and the regional assessment in Chapter 5 converge that the instruments needed to govern the DER edge exist, and the political decisions needed to require compliance with them have not been made in most jurisdictions. The strategic tasks below translate that finding into actionable recommendations for three audiences: executives and operators, policymakers and regulators, and investors and financiers. Each strategic task states a goal, lines of action, and implementation measures. Each line of action is labelled [Universal] where it applies in essentially the same form everywhere, or [Regional] where the substance must be adapted to local enforcement capac-

ity, institutional trust, or resourcing. The tasks correspond directly to the four compliance pillars: Task 1 to Pillar 2 (baseline obligations), Task 2 to Pillars 1 and 3 (scope and verification), Task 3 to Pillar 3 (verification of supply chains), and Task 4 to Pillar 4 (accountability and enforcement capacity). More governance, or governance described as more mature, does not automatically produce improved resilience and security. Thoughtful and relevant governance does. The strategic tasks below do not constitute a maximum programme but identify the minimum viable interventions that can close the identified edge-core compliance gap.

Table 7: Recommendation overview

TASK	GOAL	PRIMARILY UNIVERSAL OR REGIONAL	COMPLIANCE PILLAR AND ENABLING CONDITION ADDRESSED
1. Common technical floor	Baseline secure-by-design, SBOM/HBOM, and zero-trust practice in place everywhere	Universal	Pillar 2 (baseline obligations); Infra / tech / org
2. Close the distribution/DER gap	Extend oversight to the most under-governed and fastest-growing segment	Mixed, regionally sequenced	Pillar 1 (scope); Pillar 3 (verification); Infra / org; socio-cultural (partial)
3. Auditable supply chains	Verifiable component provenance for critical hardware and firmware	Mixed, regional financing routes	Pillar 3 (verification); Pillar 4 (accountability); Infra / tech; gov / legal (capacity)
4. Enforcement and reporting capacity	Match institutional capacity to policy ambition	Predominantly regional	Pillar 4 (accountability); Gov / politics / law

Table No 7. Recommendation overview. Author’s compilation.

TASK 1

– ESTABLISH THE COMMON TECHNICAL FLOOR

Goal: Ensure that the baseline security practices are in place across all new and, over time, existing energy infrastructure, regardless of region. This task responds to the infrastructure, technology and organisation enabling condition: the undifferentiated security levels, obsolete equipment, and lax patching that enable the majority of incidents in the current record.

Lines of Action

- [Universal] Require secure-by-design and default-authenticated connectivity in procurement specifications for all new grid-connected equipment.
- [Universal] Mandate verifiable software and hardware bills of materials (SBOM/HBOM) for critical control-system components.
- [Universal] Apply zero-trust authentication and network segmentation to all IT/OT boundaries and remote-access pathways.

Implementation measures

- Reference an existing international standard, IEC 62443, ISO/IEC 27019, or NIST SP 800-82, directly in procurement contracts rather than drafting new bespoke requirements.
- Require vendors to disclose component provenance and patch-support timelines as a condition of contract award.
- Set a defined compliance date for new assets, with a longer, resourced transition period for legacy equipment rather than an unfunded mandate.

TASK 2

– CLOSE THE DISTRIBUTION AND DER GAP

Goal: Extend meaningful oversight to distribution-level infrastructure and distributed energy resources, the most consistently under-governed segment across all regions (Chapter 5, Table 6). This task responds to the scope and verification gaps in the compliance framework: the aggregators who sit inside the grid’s trust boundary but outside its regulatory perimeter.

Lines of Action

- [Universal] Bring DER aggregators, EV-charging operators, and smart-meter platforms within the scope of existing cybersecurity obligations, rather than leaving them outside the perimeter defined for bulk-system operators.
- [Regional] In jurisdictions with strong bulk-system enforcement but weak distribution-level rules (notably North America), extend existing reliability-enforcement mechanisms downward to distribution and DER operators rather than creating a parallel, weaker regime.
- [Regional] In jurisdictions with rapid DER growth and limited existing oversight capacity (parts of Asia-Pacific, Africa, Latin America), prioritise a minimum viable baseline of authenticated device identity and basic patching capability, rather than a comprehensive framework that cannot realistically be enforced at current capacity.

Implementation measures

- Require device-level cryptographic identity for new DERs and smart meters as a condition of grid connection.
- Establish a tiered compliance schedule scaled to operator size, so that baseline obligations do not fall disproportionately on smaller distribution utilities and cooperatives.
- Fund third-party or regulator-run device certification where individual operators lack the technical capacity to assess DER security themselves.
- Require aggregators and DER installers to provide individual device owners with a minimum cybersecurity-awareness notice at point of sale or connection, covering default-password change, update settings, and an incident-reporting contact, reaching the socio-cultural enabling condition that the other measures in this strategy do not.

TASK 3

– MAKE SUPPLY CHAINS AUDITABLE

Goal: Reduce exposure to hardware and firmware compromise introduced through multi-tier international supply chains. The regional analysis in Chapter 5 shows that product certification for DER hardware exists only in the EU through the CRA and that no jurisdiction has systematically applied supply-chain verification below the bulk-system asset level. The four compliance gaps identified in the previous chapter are mutually reinforcing: fragmented standards make supply-chain verification harder, inconsistent reporting obscures the true scale of DER-level exposure, and weak DER oversight increases the consequence of any single supply-chain compromise. Addressing supply-chain opacity addresses the interaction.

Lines of Action

- [Universal] Require component-level provenance disclosure for critical control-system hardware and firmware.
- [Regional] Where procurement leverage is limited (Africa, parts of Latin America and Southeast Asia), pool demand through regional procurement consortia or multilateral development-bank financing conditions, since individual operators or governments may lack the market power to require disclosure unilaterally.
- [Regional] Where procurement leverage already exists (EU, US), extend current supply-chain disclosure requirements to cover distribution-level and DER hardware, not only bulk-system equipment.

Implementation measures

- Include supply-chain transparency clauses in development-bank and multilateral financing agreements for energy infrastructure projects.
- Establish shared vendor-assessment registries at the regional level, so that verification cost is not duplicated by every individual operator.
- Require independent firmware audits for equipment sourced from jurisdictions where verification is otherwise difficult.



TASK 4 – BUILD ENFORCEMENT AND REPORTING CAPACITY WHERE IT IS WEAKEST

Goal: Close the gap between the ambition of governance frameworks and the institutional capacity to enforce and sustain them. The cross-regional synthesis in Section 5.7 identified a consistent finding: the accountability mechanisms that work share a common design — market access conditioned on compliance, not retrospective penalty. This task responds to the government, politics and law enabling condition and to Pillar 4 of the compliance framework.

Lines of Action

- [Regional] Where policy design is strong but national-level enforcement is uneven (EU), prioritise funding and mandate for national supervisory authorities and cross-border incident-response coordination, rather than further central rule-making.
- [Regional] Where reliability enforcement is strong, but distribution/DER enforcement is fragmented across jurisdictions (US), pursue harmonisation across states through incentive-based mechanisms rather than relying solely on federal mandate, given the limits of federal authority below the bulk-power threshold.
- [Regional] Where enforcement capacity is still developing alongside electrification (Africa, parts of Asia-Pacific, parts of Latin America), use donor and development-bank financing explicitly to build regulatory and technical capacity, not only physical infrastructure, and to structure financing conditions to require this.
- [Universal] Replace purely punitive incident-reporting regimes with a safe-harbour approach that protects operators who report promptly and in good faith, to address the trust gap documented across multiple regions in Chapter 5 without weakening reporting obligations themselves.
- [Universal] Improve political oversight of sector cybersecurity: incorporate energy-sector cyber governance into the agendas of relevant parliamentary committees and into national exercises and raise the competence of legislative staff on sector cybersecurity policy, so that oversight capacity grows alongside executive capacity.
- [Universal] Codify the sector's cybersecurity governance in strategy: adopt, or update, a national cybersecurity strategy and, where the energy transition warrants it, a dedicated energy-sector security strategy aligned with it, explicitly covering the distribution and DER layer that most existing strategies predate.

Implementation measures

- Set multi-year funding commitments for national and regional cybersecurity supervisory bodies, rather than one-off grants tied to individual projects.
- Establish regional information-sharing bodies modelled on existing examples, such as the EU's cross-border crisis coordination mechanisms, in regions that currently lack an equivalent, and draw on the capacity-building track of the UN's new Global Mechanism, launched following the 2025 conclusion of the Open-Ended Working Group, as a channel for cross-border support.
- Require development-bank financing for grid digitalisation to include a specified share allocated to regulatory and workforce capacity building, not solely to hardware and software procurement.
- Before consolidating authority, complete the definitional groundwork that governance design requires, including agreed terms of reference; designation of the central office, the sector cybersecurity centre, and the core value-producers; mandates for rule-setting, steering, and communication; procedures for budgeting, information exchange, reporting, and evaluation; and any organisational or legal adjustments these require.

- Build the strategy along recognised good-practice steps such as setting the vision, scope and priorities; take stock of existing policies and capabilities; develop a clear governance structure; identify and engage relevant actors; establish trusted information-sharing mechanisms; develop contingency plans; organise exercises; and manage it as a lifecycle with scheduled evaluation and revision rather than as a one-off publication.
- Tailor the strategy to the jurisdiction rather than importing a standardised template. Prioritise the objectives that match national ambitions, concerns, and resources; align the cybersecurity strategy explicitly with energy, digital, and development policy; and schedule reviews frequent enough to keep pace with the technological change.



Implementation: From Decision to Practice

The strategic tasks above state what should be done. Experience from jurisdictions that have moved furthest shows that the distance between a regulatory decision and operational compliance is substantive. Most compliance frameworks fail in implementation due to insufficient attention to sequencing, the instrument mix, capacity building, and what to measure.

Sequencing matters. The strategic tasks are not of equal urgency or equal feasibility, and attempting to implement all four simultaneously stretches regulatory capacity and operator attention beyond what most jurisdictions can sustain. We recommend a three-phase sequencing based on the dependency structure of the pillars. Phase 1 (Scope and floor, 0-12 months): designate the responsible authority; define the actor-role taxonomy in national regulation; update grid-connection codes to include a cybersecurity commissioning check; publish the national DER compliance baseline aligned to IEC 62443 SL-2 or equivalent. These are regulatory design decisions, and they create the framework within which everything else can be verified and enforced. Phase 2 (Verification infrastructure, 12-36 months): establish or designate the product certification body; launch the DER flexibility resource registry that doubles as the asset inventory for DSO oversight; initiate the aggregator audit programme under existing market participation authority; publish the sector-specific implementation guide that translates baseline obligations into role-specific checklists. Phase 3 (Accountability and lifecycle, 36+ months): activate market-access conditionality for aggregators and manufacturers; set patch-deployment timelines and re-attestation cycles; integrate DER compliance into the energy regulator's periodic licence audit; schedule the first regulatory review cycle.

The instrument mix must be explicit. Each line of action in the four tasks carries an implicit instrument type: mandates, incentives, or information. Mandates without accompanying information produce confusion; mandates without accompanying incentives produce non-compliance by actors who lack capacity to comply. For each strategic task, the regulator implementing it should ask: for which actors is a mandate alone sufficient?

For which must it be paired with a grant, a tax credit, or a shared service? For which is a guidance document the primary instrument, because the actor population is too large or too resource-constrained for enforcement-based approaches to be credible? The device owner requires information instruments almost exclusively; the manufacturer requires mandates backed by market surveillance; the installer requires a mandate at the connection gate paired with a training and certification programme; the aggregator requires a mandate backed by market-access conditionality; the DSO requires a mandate backed by the energy regulator's existing licence enforcement powers.

Measuring implementation requires outcome metrics, not output metrics. A regulator that counts regulations issued, audits completed, and guidance documents published is measuring its own activity, not the security condition of the sector. The metrics that distinguish a compliance regime that is producing security outcomes from one that is producing audit records are: the share of new grid-connected DER assets that have passed a commissioning cybersecurity check; the proportion of active aggregators that hold a current, verified platform security certification; the share of DSOs that maintain a complete, current DER asset inventory; the coverage of supply-chain transparency requirements across the hardware procurement base; and the incident reporting rate under safe-harbour arrangements as a proxy for institutional trust. These are the metrics on which the four strategies should be evaluated. A jurisdiction that cannot report against these metrics has not yet implemented the compliance framework; it has adopted it on paper.

For executives and operators, the priority is Tasks 1 and 2 in Phases 1 and 2 of the implementation sequence: building the technical floor and closing the DER gap are within direct organisational control and address the exposure most consistent with recent incidents. For policymakers and regulators, the priority is Task 4: enforcement capacity determines whether the other strategies produce results in practice. For investors and financiers, the priority is Task 3: procurement leverage and financing conditions are the most direct tools available to influence supply-chain practice, particularly in regions where individual operators lack that leverage.

7 Conclusion

This report began with two observations: energy systems are adding assets at the distributed edge faster than governance can follow, and this gap has been noticed by adversaries. The Polish December 2025 coordinated operation against thirty distributed generation sites and the Norwegian dam seizure indicate failures of compliance governance: actors at the edge of the system operating outside the regulatory perimeter of every framework designed to protect the core.

The four-pillar compliance framework developed in Chapter 4 — scope, baseline obligations, verification, and accountability — provides a governance architecture for closing that gap. Its contribution is not a new standard; international standards already specify what secure-by-design, zero-trust, and supply-chain-verified energy infrastructure looks like. Its contribution is a structured answer to the question of who must comply, what they must do, how compliance is assessed, and what follows when it is not met. The framework is designed to be applied specifically to the DER actor ecosystem which existing frameworks were not designed to address.

Our regional assessment finds a consistent pattern of existing governance ambition exceeding governance implementation, and of a structural gap at the aggregator level. No jurisdiction has made aggregator and VPP compliance a condition of market access. Conditioning market access is the single most productive regulatory intervention available to jurisdictions that wish to improve DER cybersecurity without building a new enforcement apparatus. The aggregator already has a commercial relationship with both distribution system and transmission operators which carries market access making a compliance condition a political priority question.

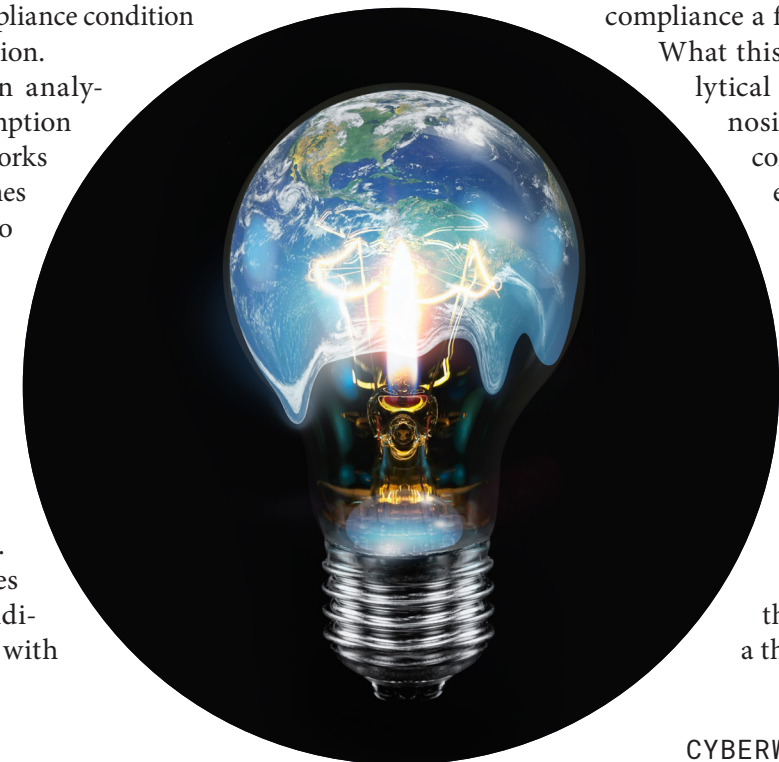
The implementation analysis challenges the assumption that compliance frameworks produce security outcomes automatically. They do not. Compliance-based strategies that produce documented conformity without operational security improvement are well-documented in the literature, organised hypocrisy in Power's (2007) formulation. The DER context creates particularly fertile conditions for that outcome with

diverse actors, limited enforcement capacity, and an audit infrastructure that is easier to satisfy formally than substantively. The antidote is not more requirements but better implementation design with the right instrument mix for each actor and operator, sequenced implementation that matches regulatory capacity, and outcome metrics that measure movement in the exposure rather than the volume of compliance activity.

The report's analysis supports three normative conclusions that, we argue, are not contested by the evidence and should not wait for further study. First, DER compliance governance as a national question goes beyond a sector-regulatory one. Ungoverned DER assets at the edge expose state-level infrastructure to adversarial influence without triggering the thresholds at which national security and CIP frameworks activate. Policymakers who treat DER cybersecurity as a matter for energy regulators alone are underestimating the governance problem and the issue dynamics. Second, the compliance obligation for the aggregators should be a precondition of market access in every jurisdiction that has opened its energy market to aggregation. The legal authority to impose this condition often exists. Third, development-bank financing for energy infrastructure should systematically include cybersecurity compliance conditions as a standard term and particularly for DER procurement in jurisdictions where domestic regulatory capacity cannot enforce the baseline independently.

The compliance framework and the four strategic tasks are not a checklist. A checklist satisfied without regard to the security condition it is meant to produce is precisely the organised hypocrisy that makes compliance a false proxy for resilience.

What this report offers is an analytical structure, a way of diagnosing which elements of a compliance regime are present, which are absent, and what governance decisions are required to close the gap. The diagnosis differs by region, and the recommended interventions differ accordingly. What does not differ is the starting point: governance without substance remains aloof. The edge of the energy system is already a theatre of operations.



REFERENCES

Adabara, I., Sadiq, B. O., Shuaibu, A. N., & Danjuma, Y. (2024). Identifying and Modelling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *Journal of Cybersecurity and Privacy*, 5(4), 97. <https://doi.org/10.3390/jcp5040097>

African Energy Commission (AFREC). (2024). African Energy Transition Strategy and Action Plan.

African Union. (2014; 2023). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). Adopted 27 June 2014, Malabo; entered into force 8 June 2023.

Agency for the Cooperation of Energy Regulators (ACER). (2024). Cybersecurity Network Code for Electricity: Implementation Guidance.

Akinsola, O. (2025). From Compliance to Cyber Resilience: Bridging the Gap. *Applied Information Sciences*, 2025.

ANCI (Agencia Nacional de Ciberseguridad, Chile). (2025). Final List of Operators of Vital Importance (OVI), First Qualification Procedure. Exempt Resolution published in the Official Gazette, 17 December 2025. Santiago: ANCI.

ASEAN. (2025). ASEAN Cybersecurity Cooperation Strategy 2026–2030. Singapore: ASEAN Secretariat.

ASEAN Centre for Energy (ACE). (2026). ASEAN Plan of Action for Energy Cooperation (APAEC) 2026–2030. Jakarta: ASEAN Centre for Energy.

Auld, G., Bernstein, S., Cashore, B., & Levin, K. (2010). Playing it forward: Path dependency, progressive incrementalism, and the ”Super Wicked” problem of global climate change. Working paper, Yale School of the Environment.

Australian Government. (2023). 2023–2030 Australian Cyber Security Strategy. Canberra: Department of Home Affairs.

Australian Government. (2024). Critical Infrastructure Annual Risk Review 2024. Canberra: Cyber and Infrastructure Security Centre (CISC), Department of Home Affairs.

Central Electricity Authority (CEA), Government of India. (2021). Guidelines on Cyber Security in Power Sector, 2021.

Central Electricity Authority (CEA), Government of India. (2025). Draft Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2025. New Delhi: CEA, Ministry of Power, October 2025.

Center for Strategic and International Studies (CSIS). (2026). Iran Conflict Heightens Cyber Threats to U.S. Energy Infrastructure. Analysis drawing on EuRepoC incident data, 2010–2024.

Chile, Congreso Nacional. (2024). Ley N° 21.663: Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información. Published 8 April 2024; in force from 1 January 2025 (OVI provisions from 1 March 2025).

Choi, S., & Ghez, J. (2026). Policy instruments to strengthen the cybersecurity of critical infrastructure. *Journal of Cyber Policy*, 2026. <https://doi.org/10.1080/23738871.2026.2648977>

CIGRE Chile (Comité Nacional Chileno de CIGRE). (2021). Cyber Security Master Plan for the Electricity Sector 2021–2023.

CISA. (2025). Cross-Sector Cybersecurity Performance Goals, Version 2.0. Washington, DC: Cybersecurity and Infrastructure Security Agency, December 2025.

CISA. (2026). CIRCIA Rulemaking: Frequently Asked Questions. Washington, DC: Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

Cyberspace Administration of China (CAC). (2025). Measures on the Management of National Cybersecurity Incident Reporting. Effective 1 November 2025.

DCAF – Geneva Centre for Security Sector Governance. (2021). Guide to Good Governance in Cybersecurity. Geneva: DCAF.

DCAF – Geneva Centre for Security Sector Governance. (2024). Accountability in Cybersecurity. Ed. Franziska Klopfer. Geneva: DCAF, December 2024.

Dragos. (2026). 2026 OT Cybersecurity Year in Review.

European Repository of Cyber Incidents (EuRepoC). (2026a). Cyber Activity Balance 2025: The European Union in Focus (Rottinger, L., Bendiek, A., & Hemmelskamp, J.). EuRepoC Cyber Conflict Briefing, February 2026.

European Repository of Cyber Incidents (EuRepoC). (2026b). Global Database of Cyber Incidents. <https://eurepoc.eu> (accessed July 2026).

European Commission. (2024). Commission Delegated Regulation (EU) 2024/1366 Establishing a Network Code on Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows.

European Commission. (2025). Cyber Resilience Act (Consolidated).

European Union. (2026). NIS2 Directive: Securing Network and Information Systems.

European Union Agency for Cybersecurity (ENISA). (2016). NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies. Updated edition, November 2016.

European Union Agency for Cybersecurity (ENISA). (2023). Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies.

European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024.

Federal Bureau of Investigation (FBI). (2025). Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure. Joint Advisory, December 9, 2025.

GAO (U.S. Government Accountability Office). (2025). Cybersecurity Regulations: Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization. GAO-25-108436, July 30, 2025.

Hiller, J. S. (2024). Cybersecurity carrots and sticks. *American Business Law Journal*.

HMG (Department for Energy Security and Net Zero, National Cyber Security Centre, Office of Gas and Electricity Markets, National Energy System Operator). (2026). Energy Sector Cyber Security Strategy: Building Resilience through Partnership. London: HM Government, May 2026.

Idaho National Laboratory (INL). (2026). Navigating U.S. Standards and Regulation for Digital Energy Systems.

Ifeanyi-Ajufo, N. (2023). Cyber Governance in Africa: At the Crossroads of Politics, Sovereignty and Cooperation. *Policy Design and Practice*, 6(2), 146–159.

Inter-American Development Bank (IDB) & Organization of American States (OAS). (2025). 2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean. Washington, DC: IDB.

International Electrotechnical Commission (IEC). (2026). IEC 62351: Cybersecurity for IEC 61850 and Related Power-System Protocols.

International Energy Agency (IEA). (2022). Unlocking the Potential of Distributed Energy Resources: Power System Opportunities and Best Practices. IEA, Paris.

International Energy Agency (IEA). (2025). World Energy Outlook 2025 – Executive Summary.

International Energy Agency Photovoltaic Power Systems Programme (IEA-PVPS). (2025). Trends in Photovoltaic Applications 2025.

International Organization for Standardization (ISO). (2024). ISO/IEC 27019:2024 — Information Security Controls for the Energy Utility Industry.

International Renewable Energy Agency (IRENA). (2026). Renewable Capacity Statistics 2026 (H1 data release).

International Society of Automation (ISA). (2025). ISA/IEC 62443 Series of Standards.

INTERPOL. (2025). Africa Cyberthreat Assessment Report 2025, 4th Edition. Interpol, Lyon.

Kerttunen, M. & Tikk, E. (2019). National Cyber Security Strategies: A Commitment to Development. Cyber Policy Institute, February 2019.

KPMG. (2025). Cybersecurity Considerations 2025: Energy and Natural Resources Sector.

MITRE. (2025). ATT&CK for ICS Matrix.

National Association of Regulatory Utility Commissioners (NARUC) & U.S. Department of Energy (DOE), Office of Cybersecurity, Energy Security, and Emergency Response (CESER). (2024). Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources.

National Institute of Standards and Technology (NIST). (2020). SP 800-207: Zero Trust Architecture.

National Institute of Standards and Technology (NIST). (2022). SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

National Institute of Standards and Technology (NIST). (2023). SP 800-82 Rev. 3: Guide to Operational Technology Security.

National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework 2.0. NIST CSF 2.0, February 2024.

Nigeria, Federal Government. (2024). Designation and Protection of Critical National Information Infrastructure Order, 2024. Abuja: Office of the President.

Power, M. (2007). Organized Uncertainty: Designing a World of Risk Management. Oxford: Oxford University Press.

Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. *Sustainability*, 14(3), 1390.

REN21. (2025). Renewables 2025 Global Status Report – Solar PV. REN21 Secretariat, Paris.

State Council of the People’s Republic of China. (2021). Regulation on Protecting the Security of Critical Information Infrastructure. Effective 1 September 2021.

Tikk, E., Hovhannisyan, K. & Kerttunen, M. (2020). The Cyber Conflict Factbook. Cyber Policy Institute.

United Nations General Assembly (UN GGE). (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc. A/70/174, 22 July 2015.

United Nations Open-Ended Working Group (UN OEWG). (2025). Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. UN Doc. A/AC.292/2025/CRP.1, adopted 11 July 2025.

White House. (2026). President Trump’s Cyber Strategy for America. Washington, DC: The White House, March 2026.

World Bank. (2024). Mission 300: Universal Energy Access by 2030.

World Bank. (2025). Enhancing Cyber Resilience in Developing Countries. Results Brief, 29 January 2025.

LIST OF ABBREVIATIONS

ACER	Agency for the Cooperation of Energy Regulators	HBOM	Hardware Bill of Materials
AFREC	African Energy Commission	HMG	His/Her Majesty’s Government
AI	Artificial Intelligence	ICS	Industrial Control System
ANCI	Agencia Nacional de Ciberseguridad (Chile)	ICT	Information and Communications Technology
APAEC	ASEAN Plan of Action for Energy Cooperation	IDB	Inter-American Development Bank
ASEAN	Association of Southeast Asian Nations	IEA	International Energy Agency
AU	African Union	IEA-PVPS	IEA Photovoltaic Power Systems Programme
BES	Bulk Electric System	IEC	International Electrotechnical Commission
CAC	Cyberspace Administration of China	ISMS	Information Security Management System
CARR	CyberArmyofRussia_Reborn	ISA	International Society of Automation
CEA	Central Electricity Authority (India)	ISO	International Organization for Standardization
CERT	Computer Emergency Response Team	IT	Information Technology
CESER	Office of Cybersecurity, Energy Security, and Emergency Response (US DOE)	JCIS	Joint Committee on Intelligence and Security (Australia)
CHP	Combined Heat and Power	KPMG	KPMG International (professional services)
CII	Critical Information Infrastructure	MLPS	Multi-Level Protection Scheme (China)
CIP	Critical Infrastructure Protection	MVA	Megavolt-Ampere
CISA	Cybersecurity and Infrastructure Security Agency (US)	MW	Megawatt
CISC	Cyber and Infrastructure Security Centre (Australia)	NARUC	National Association of Regulatory Utility Commissioners (US)
CISO	Chief Information Security Officer	NCCS	Network Code on Cybersecurity (EU)
CNII	Critical National Information Infrastructure (Nigeria)	NCIIPC	National Critical Information Infrastructure Protection Centre (India)
CPG	Cybersecurity Performance Goals (CISA)	NERC	North American Electric Reliability Corporation
CRA	Cyber Resilience Act (EU)	NIS2	Network and Information Security Directive 2 (EU)
CSIRT	Computer Security Incident Response Team	NIST	National Institute of Standards and Technology (US)
CSIS	Center for Strategic and International Studies	OAS	Organization of American States
CSRB	Cyber Security and Resilience Bill (UK)	OEWG	Open-Ended Working Group (UN)
DCAF	Geneva Centre for Security Sector Governance	OT	Operational Technology
DER	Distributed Energy Resource(s)	OVI	Operator of Vital Importance (Chile)
DOE	Department of Energy (US)	PDVSA	Petróleos de Venezuela, S.A.
DSO	Distribution System Operator	PUC	Public Utility Commission
ECII	Electricity Cybersecurity Impact Index	PV	Photovoltaic
ENISA	European Union Agency for Cybersecurity	SBOM	Software Bill of Materials
EU	European Union	SL	Security Level (IEC 62443)
EuRepoC	European Repository of Cyber Incidents	SOCI	Security of Critical Infrastructure Act (Australia)
EV	Electric Vehicle	SoNS	System of National Significance (Australia)
FERC	Federal Energy Regulatory Commission (US)	TSO	Transmission System Operator
GAO	Government Accountability Office (US)	UN	United Nations
GGE	Group of Governmental Experts (UN)	US / USD	United States / United States Dollar
GRU	Main Directorate of the General Staff, Armed Forces of Russia	VPN	Virtual Private Network
GW	Gigawatt	VPP	Virtual Power Plant

ANNEX 1 : CYBERSECURITY GOVERNANCE PRINCIPLES BY REGION

Table A1 maps regional cybersecurity governance against the six principles introduced in Chapter 1: (1) legal and policy framework; (2) institutional authority and accountability; (3) risk governance; (4) operational capacity; (5) supply-chain and technology security; and (6) stakeholder cooperation and oversight. The table is an indicative assessment; underlying data availability and definitions vary by region, and within-region variation is understated by any single-cell summary. Sources: CISA (2025); DCAF (2021); DCAF (2024); European Union (2026); European Commission (2024; 2025); ACER (2024); White House (2026); CISA (2026); Idaho National Laboratory (2026); NARUC & U.S. Department of Energy (2024); State Council of the People’s Republic of China (2021); CAC (2025); Central Electricity Authority (2021; 2025); Australian Government (2023; 2024); ASEAN (2025); African Union (2014/2023); INTERPOL (2025); Nigeria (2024); Chile (2024); ANCI (2025); Inter-American Development Bank & OAS (2025). Author’s compilation.

REGION	LEGAL AND POLICY FRAMEWORK	INSTITUTIONAL AUTHORITY AND ACCOUNTABILITY	RISK GOVERNANCE	OPERATIONAL CAPACITY	SUPPLY-CHAIN AND TECHNOLOGY SECURITY	STAKEHOLDER COOPERATION AND OVERSIGHT
European Union	NIS2 (binding, horizontal); NCCS sector-specific (2024); CRA product law (2025). Among the most legally comprehensive globally.	National competent authorities per NIS2; ENISA; ACER for energy coordination. Enforcement quality varies by member state.	ECII asset classification (high-impact/critical-impact). Risk-based NIS2 tiering. Supply-chain risk in CRA and Critical Raw Materials Act.	NIS2: 24h/72h/1-month reporting. ENISA CSIRT network. Cross-border crisis coordination. NCCS energy-sector CERT functions.	CRA: secure-by-design mandate. Supply-chain diversification as industrial policy. NCCS provisions for cross-border assets.	ENISA multi-stakeholder platform. NIS2 public-private cooperation. ENTSO-E and EU DSO Entity. Parliamentary oversight (IMCO/ITRE).
United States	No comprehensive federal energy cybersecurity law. NERC CIP mandatory at BES level. CIRCIA cross-sector rule pending (delayed mid-2026). 2026 Cyber Strategy deregulatory.	Fragmented: DOE/CESER (policy); FERC (bulk markets); CISA (cross-sector, capacity reduced ~one-third since Jan. 2025); state PUCs (investor-owned utilities). No single authority below BES.	NERC CIP risk-based standards for BES (~10-20% of grid). No systematic risk governance at distribution or DER level. NARUC voluntary baselines (2024) for guidance only.	CIRCIA reporting rule pending. Bulk-level mandatory; distribution/DER inconsistent. DOE CESER funds exercises and threat-sharing. E-ISAC for information sharing.	NERC CIP-013 supply-chain (bulk only). No equivalent for distribution or DER. Procurement leverage not yet applied below BES level.	E-ISAC for bulk-power sharing. NARUC/DOE public-private coordination. Congressional oversight fragmented. Trust in CISA reporting constrained by punitive framing.
Asia-Pacific (heterogeneous)	China: CSL 2016 + 2026 amendments. India: CEA Guidelines 2021; draft binding Regs 2025. Australia: SOCI Act + ERP Act 2024 + Cyber Security Act 2024. ASEAN: no binding cross-border framework.	China: CAC; CII-designating ministries. India: NCIIPC + CSIRT-Power + CEA. Australia: CISC (integrated authority). ASEAN: national authorities; no shared enforcement.	China: MLPS + CII designation; monitoring-to-control shift (2026 cycle). India: CEA framework; 24h to NCIIPC. Australia: SoNS (200+ assets); mandatory risk management. ASEAN: no shared framework.	China: tightened timelines (CAC Nov. 2025). India: CSIRT-Power (est. 2023). Australia: SOCI mandatory reporting; SoNS exercises; ransomware reporting (Cyber Security Act 2024). ASEAN CERT 2025.	China: CSL 2026 supply-chain provisions. India: vendor disclosure in draft CEA Regs 2025. Australia: SoNS obligations; IoT standards (Cyber Security Act 2024). ASEAN: limited.	China: centralised; limited independent oversight. India: parliamentary committees; CERT-In coordination. Australia: JCIS oversight; CISC industry engagement; ASD threat-sharing. ASEAN: no joint energy-cybersecurity mechanism.

REGION	LEGAL AND POLICY FRAMEWORK	INSTITUTIONAL AUTHORITY AND ACCOUNTABILITY	RISK GOVERNANCE	OPERATIONAL CAPACITY	SUPPLY-CHAIN AND TECHNOLOGY SECURITY	STAKEHOLDER COOPERATION AND OVERSIGHT
Africa	AU Malabo Convention in force June 2023 (fewer than one-third ratified). Nigeria: Cybercrimes Amendment Act 2024 + CNII Order 2024. Kenya: CII Regulations 2024. Most states: guidance-only.	No dedicated continental authority. Nigeria: NSA-led CNII coordination. Kenya: Communications Authority. Most states: no cybersecurity agency with energy-sector enforcement powers.	Nigeria CNII Order 2024: energy designated; Trusted Information Sharing Network. Kenya CII Regs: continuous monitoring. Most states: no systematic CII designation or risk-management mandate.	INTERPOL capacity-building operations. National CSIRTs where established; capacity thin. Incident reporting nascent outside national leaders. Energy-sector incident response very limited.	DER hardware (mini-grids, solar-home systems, prepaid meters) from international vendors via development-bank channels. No continental or most national frameworks specify supply-chain baselines.	Development banks (World Bank, AfDB) as de facto governance levers. AU frameworks unenforced. Civil society limited. Parliamentary oversight nascent. INTERPOL as principal external coordination body.
Latin America & Caribbean	Chile: Law 21.663 fully operational (ANCI Jan. 2025; 915 OVIs designated Dec. 2025 incl. 307 electricity entities). Brazil: Bill 4752/2025 in Senate; ANEEL 2021 resolution as interim. Elsewhere: development-bank conditions dominant.	Chile: ANCI with binding powers, mandatory audits, fining authority (up to 40,000 UTM). Brazil: no enacted cybersecurity authority; ANEEL for energy. Most states: no designated authority with enforcement capacity.	Chile OVI framework: mandatory risk management; audits; tiered obligations. Brazil: ANEEL resolution sets minimum standards without risk-based classification. Most of region: no systematic CII or DER risk governance.	Chile: 3h early warning / 72h notification to national CSIRT. Brazil: no mandatory reporting enacted. Most states: inconsistent. IDB/OAS as principal capacity provider. Energy-sector CSIRT functions absent across most of region.	Chile: OVI supply-chain obligations emerging. Elsewhere: development-bank lending conditions as principal supply-chain lever. No regional verification mechanism. DER hardware through retail channels without security baselines.	IDB/OAS Cybersecurity Report (2025) as principal regional assessment. Chile: ANCI public-private consultation; parliamentary oversight. Brazil: multi-stakeholder consultation on pending law. Development banks most influential external actor.

➤ Our Aim is to Add Cyber Capabilities in the World



Contact

Cyberwatch Oy | Kansakoulukatu 1b | 00100 Helsinki, Finland
aapo@cyberwatchfinland.fi | info@cyberwatchfinland.fi | +358 40 500 8177