Cyber-Physical Security for Data Centres: Making Resilience Lender-Grade

A Control, Evidence and Recovery Framework for Financing Digital Infrastructure

Authored by Chennakeshav Adya
Independent Researcher
August 2026

Abstract

Cyber-physical security has become a cash-flow and financing issue for data centres. The facility depends on operational technology, building-management systems, electrical protection, cooling control, physical access, remote vendor support and networked monitoring. A compromise can affect availability, safety, customer acceptance, regulatory reporting, insurance and debt service at the same time. Lenders therefore need evidence that the operating system can prevent, contain, respond to and recover from disruptive events.

This paper develops a board and lender framework for converting security claims into financeable evidence. It maps critical services and trust zones, joins physical and cyber controls, assigns accountable owners, builds a test programme, and connects recovery objectives to revenue, liquidity and covenant analysis. It also proposes a data-room architecture, construction-to-operations acceptance gates and a 180-day resilience office.

The evidence base includes NIST Cybersecurity Framework 2.0, NIST guidance for operational technology and enterprise risk management, CISA performance goals and Secure by Demand guidance, the European Union's NIS2 regime and implementing rules for data-centre service providers, the UK's NCSC and NPSA, Singapore's Cyber Security Agency, Saudi Arabia's National Cybersecurity Authority, Dubai Electronic Security Center, Australia's Cyber and Infrastructure Security Centre, India's Central Electricity Authority and CERT-In, and the IEC 62443 family. These authorities establish governance, control and reporting expectations. They do not establish the security posture, compliance, insurance, outage exposure, credit approval or financeability of a specific asset.

Six original figures and six implementation tables support the control architecture, evidence ladder, incident timeline, loss waterfall and debt-capacity discussion. Every facility size, outage duration, revenue amount, cost, probability, reserve, debt quantum and coverage ratio in the worked case is a management assumption created solely to demonstrate the method. Live projects require qualified cyber, OT, physical-security, engineering, legal, regulatory, insurance, tax, accounting, customer-contract and financing advice.

JEL Classification: G21, G31, G32, L86, O33

Keywords: data centres, cyber-physical security, operational technology, resilience, project finance, lender diligence, business continuity, digital infrastructure

1. Treat cyber-physical resilience as a cash-flow condition

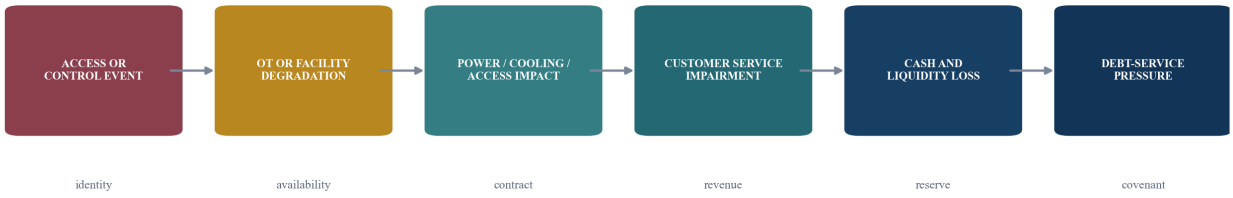
A data centre earns revenue through continuous delivery of power, cooling, connectivity, access and contracted service. Those services depend on more than servers and perimeter firewalls. Switchgear controllers, generator controls, uninterruptible power supplies, battery-management systems, chillers, pumps, fire detection, building-management systems, data-centre infrastructure management, security cameras and access-control systems exchange commands and telemetry. Vendor engineers may reach them through remote support paths. A security event can therefore become an operational interruption.

NIST Special Publication 800-82 Revision 3 describes operational technology as programmable systems and devices that interact with the physical environment, and it emphasises performance, reliability and safety requirements that can differ from conventional information technology. That description fits the data-centre control environment. A change to a cooling set point, protection relay or generator controller can affect the physical service supporting customer equipment.

The financing question is whether a defined adverse event can interrupt billable capacity, trigger service credits, require emergency expenditure, delay completion or impair the ability to meet debt obligations. The answer needs a traceable chain from asset and control to service, contract, cash flow and liquidity. A certification badge or policy document does not complete that chain.

Figure 1. Cyber-physical event to cash-flow transmission chain

RESILIENCE BECOMES LENDER-GRADE WHEN THE ENTIRE CHAIN IS EVIDENCED



The financing review follows each event from control failure to service and debt consequences.

2. Define the service and asset boundary

The first diligence task is to define the service whose continuity matters. The boundary should cover utility intake, on-site generation, fuel, high- and medium-voltage distribution, UPS and batteries, cooling, water, fire and life-safety, physical access, monitoring, communications, customer cages and relevant cloud-based management services. It should state which systems are owned, leased, operated by a tenant or maintained by a vendor.

An asset register should identify hardware, firmware, software, network address, location, owner, support status, criticality, dependencies, remote connections, backup method and recovery procedure. NIST CSF 2.0 places asset management, risk assessment and

technology-infrastructure resilience inside a wider governance model. The UK NCSC's 2025 operational-technology guidance also calls for a definitive view of OT architecture, documented connectivity and third-party risk.

The register should distinguish installed, commissioned, accepted and recoverable assets. A controller that appears on a network scan may lack a current configuration backup. A standby generator can pass a mechanical test while its remote monitoring route remains unmanaged. A door controller may operate locally while the central identity service is unavailable. Lender diligence needs the service dependency, operating state and recovery evidence for each critical component.

Table 1. Critical asset, threat and lender-evidence map

Asset or service	Material cyber-physical event	Operating consequence	Lender-grade evidence
utility intake and protection	unauthorised relay change, loss of telemetry or disabled interlock	trip, unsafe switching or delayed restoration	signed settings, access logs, tested backup, relay-change approval and restoration record
generators and fuel control	remote-control compromise, controller failure or fuel-system manipulation	reduced backup duration or failed start	protected local mode, start-test history, controller backup, fuel assurance and recovery drill
UPS and batteries	configuration change, firmware defect or monitoring loss	reduced ride-through or unplanned bypass	approved baseline, alarm test, firmware register, capacity test and rollback evidence
cooling and water	false sensor data, set-point change or controller outage	thermal excursion, derating or shutdown	zone architecture, set-point governance, manual fallback and integrated load test
building and infrastructure management	account compromise, flat connectivity or unavailable historian	impaired visibility and control	identity records, segmentation, protected logs, backup and restore test
physical access and surveillance	credential abuse, tailgating or controller outage	unauthorised entry or lost evidence	layered access design, visitor records, alarm test, offline mode and incident procedure

Site-specific controls and testing remain subject to qualified technical review.

3. Build one cyber-physical architecture

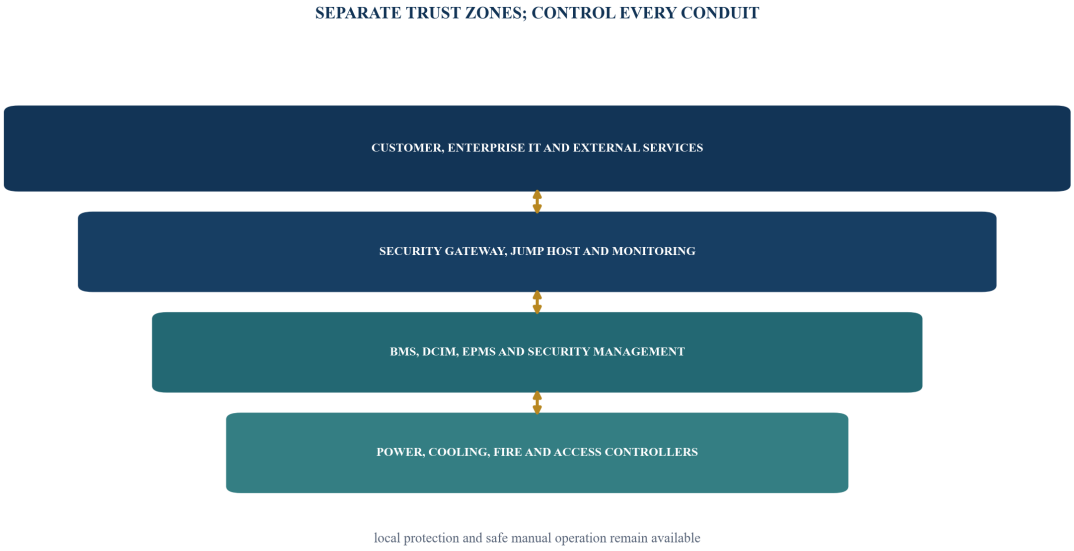
The architecture should show enterprise IT, customer networks, management services, security systems and OT as separate trust zones with controlled conduits. The design needs enough detail to reveal every route that can change a physical process or security state. Internet access, vendor portals, wireless links, serial gateways, engineering laptops, jump hosts, cloud dashboards and building-operator workstations belong on the same map.

IEC 62443 uses zones, conduits and security levels to organise industrial-automation risk. IEC 62443-4-2 identifies seven foundational requirements for control-system components: identification and authentication, use control, system integrity, data confidentiality, restricted data flow, timely response to events and resource availability. The framework offers a useful design vocabulary. Application and conformity require the licensed standards, competent specialists and

a project-defined target.

The architecture should also show safe local operation. A failed enterprise identity platform should not leave the plant without an authorised emergency path. Loss of remote telemetry should not disable local protection. A maintenance connection should be time-bound and visible. Safety and life-safety systems need their own control logic, regulatory acceptance and manual procedures.

Figure 2. Layered data-centre cyber-physical architecture



Controlled conduits connect distinct trust zones; no diagram proves implementation.

4. Translate global requirements into an applicability register

Global data-centre portfolios face overlapping regulatory and contractual requirements. The EU NIS2 Directive expressly covers data-centre service providers and requires an all-hazards approach protecting network and information systems and their physical environment. Required areas include incident handling, continuity, supply-chain security, secure acquisition and maintenance, effectiveness testing, training, cryptography, human resources, access control, asset management and multi-factor authentication where appropriate.

Commission Implementing Regulation 2024/2690 adds technical and methodological requirements for covered data-centre providers. It treats complete unavailability, availability limited for more than one hour, certain data compromises and compromised physical access as significant incidents for this sector. The same regulation requires risk treatment, a supplier registry, acquisition controls, business impact analysis, testing and documented responsibility. Scope and local enforcement require jurisdiction-specific legal advice.

Other jurisdictions use different legal forms. Singapore's Cybersecurity Code of Practice applies to owners of designated critical information infrastructure. Saudi Arabia's Operational Technology Cybersecurity Controls extend its Essential Cybersecurity Controls and set minimum requirements for relevant OT systems. Dubai DESC publishes an ICS Security Standard for government and semi-government entities operating critical infrastructure or OT. Australia's Critical Infrastructure Risk Management Program covers cyber, physical, personnel, supply-chain and natural hazards for responsible entities. India applies CEA cyber guidelines to power-sector

responsible entities, while CERT-In directions impose incident, logging and customer-information requirements on specified organisations including data centres.

Table 2. Jurisdictional anchors for the applicability register

Jurisdiction or framework	Public anchor	Relevance to the evidence plan	Project action
United States and global voluntary use	NIST CSF 2.0, SP 800-82 Rev. 3 and CISA performance goals	governance, OT risk, prioritised outcomes, response and recovery	create current and target profiles with named evidence owners
European Union	NIS2 and Implementing Regulation 2024/2690	all-hazards controls, supplier lifecycle, incident significance and reporting	confirm entity scope, Member State law, control evidence and reporting workflow
United Kingdom	NCSC OT principles and NPSA protective-security guidance	definitive architecture, secure connectivity, supplier trust and physical protection	document connectivity decisions, physical layers and security culture
Singapore	CSA Cybersecurity Code of Practice for CII	governance, protection, detection, response and recovery for designated CII	confirm designation and map applicable code requirements
Saudi Arabia and Dubai	NCA OTCC and DESC ICS Security Standard	minimum OT controls for relevant organisations and critical infrastructure	obtain current applicability advice and local assessment evidence
Australia and India	CIRMP, CEA cyber guidelines and CERT-In directions	all-hazard programme, power OT, reporting and log retention	map entity and asset scope, responsible officers, testing and evidence retention

The table summarises public sources and is not legal advice or a compliance determination.

5. Create a lender evidence ladder

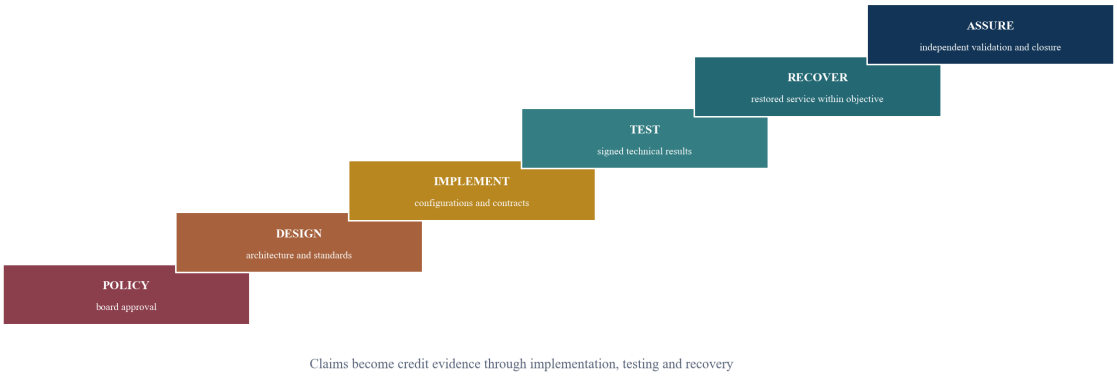
Evidence should progress from policy to operation. A board-approved policy shows intent. An architecture shows design. Configuration records, access logs and signed test results show implementation. Independent validation and repeated recovery exercises show operating effectiveness. Incident records and remediation closure show whether the control system learns.

NIST IR 8286 Revision 1, published in December 2025, links cybersecurity risk registers to enterprise risk management and calls for directors and senior leaders to understand cybersecurity risk posture. That principle is useful for financing. A lender needs a concise risk register that states the affected service, plausible event, existing control, residual exposure, financial consequence, owner, action, deadline and evidence location.

An evidence ladder also protects the transaction from overstatement. A vendor presentation is weaker than an executed support agreement. A backup job log is weaker than a successful restore. A penetration-test report is incomplete until material findings are closed or accepted by an authorised risk owner. A tabletop exercise is weaker than a controlled recovery test using the actual operating team.

Figure 3. Lender evidence ladder

THE EVIDENCE QUALITY RISES WITH OPERATING PROOF



Higher steps add operating and independent evidence; each control remains project-specific.

6. Assign governance from board to control owner

The board should approve the cyber-physical risk appetite, critical services, material scenarios, recovery objectives, investment plan and risk-acceptance authority. Management should translate that direction into control standards and a funded programme. Site operations, information security, engineering, physical security, safety, customer operations, procurement, legal, insurance and finance each own defined evidence.

NIST CSF 2.0 added a Govern function to place cybersecurity inside enterprise risk management. The CSF applies across the organisation and supply chain. A data-centre governance model should therefore avoid treating OT as an isolated engineering matter or cybersecurity as a security-operations-centre matter. The risk committee should review service availability, safety, customer and financing consequences together.

Every material exception needs an expiry date and compensating control. Unsupported firmware, shared accounts, uncontrolled remote access, untested recovery or missing physical-access logs should appear in one exception register. The accountable executive should approve remediation funding and the financing team should decide whether the item affects construction drawdown, debt sizing, insurance or customer disclosure.

7. Control identity, privilege and remote maintenance

Remote support provides operational value and creates a path into critical systems. CISA's 2025 Secure by Demand guidance asks OT owners and operators to evaluate products for secure logging, open standards, ownership of data, secure defaults, vulnerability handling and secure communications. The UK NCSC advises organisations to document the business need, risk tolerance, contractual controls, component visibility and supplier trustworthiness before adding OT connectivity.

Each human and machine identity should be unique where technology permits. Privileged access should require approval, strong authentication, time limitation, recording and review. Shared

emergency accounts need sealed credentials, dual control and post-use investigation. Vendor access should terminate automatically when the approved task or support contract ends.

The operating team should maintain an authorised support matrix: supplier, system, permitted route, approved users, authentication method, support hours, monitoring, data access, emergency procedure and contract owner. A lender can then test whether a vendor can reach critical plant through an undocumented modem, unmanaged laptop, common password or permanent tunnel.

Table 3. Access and segmentation control matrix

Control objective	Required design evidence	Operating evidence	Failure test
unique accountable access	identity architecture, role matrix and break-glass design	active-user list, approvals and periodic recertification	sample terminated users and emergency access
controlled remote maintenance	approved jump path, contract clause and session-recording design	work tickets, time-bound grants and reviewed recordings	attempt connection outside approved window
restricted data flow	zone and conduit diagram, rule owner and change procedure	current firewall or gateway rules and change logs	validate blocked paths and fail-closed behaviour
protected engineering tools	managed-build standard, media control and malware process	laptop inventory, patch state and scan records	introduce approved test media and verify workflow
resilient authentication	local emergency method and dependency map	successful failover and recovery records	isolate central identity service under controlled test
privileged event visibility	logging standard, time synchronisation and retention plan	searchable records and alert-response tickets	create authorised test event and trace it end to end

Control design should accommodate safety, availability and legacy constraints.

8. Integrate physical security and insider risk

Physical access can bypass network controls. The perimeter should combine site selection, stand-off, barriers, lighting, surveillance, security staff, credentialed entry, visitor management, loading-bay control, anti-tailgating measures and protected critical rooms. The design should consider utilities, roof access, fuel systems, water systems, cable routes, generator yards and emergency exits.

The UK NPSA recommends layered protective security and emphasises employee behaviour for critical national infrastructure. Australia's CIRMP guidance treats physical, personnel, supply-chain, cyber and natural hazards as connected programme areas. A data-centre plan should therefore connect background screening, role changes, contractor supervision, visitor sponsorship, credential revocation, asset removal and suspicious-behaviour reporting.

The physical system also needs degraded-mode procedures. Door controllers, cameras and visitor systems may depend on central servers, networks or cloud services. The site must know how it authenticates authorised people, records entry, preserves life safety and restores evidence during an outage. A lender-grade test should verify those procedures without creating unsafe access.

9. Secure the supply chain over the full lifecycle

Supply-chain risk begins during specification. Procurement should require supported product lifecycles, secure configuration guidance, vulnerability disclosure, patch and mitigation processes, software and component transparency where appropriate, secure remote support, logging, data ownership, incident cooperation, recovery assistance and end-of-life notice. These terms should flow to integrators and critical subcontractors.

NIST CSF 2.0 explicitly integrates supply-chain governance, due diligence, contract requirements, monitoring and incident participation. EU Implementing Regulation 2024/2690 requires relevant entities to keep an up-to-date directory of direct suppliers and services and to manage acquisition risk for critical components throughout their lifecycle. IEC 62443-4-1 addresses secure product-development lifecycle processes, including requirements, design, verification, vulnerability and patch management and product end of life.

The lender file should identify single-source dependencies, unsupported products, proprietary protocols, escrow or configuration access, spare hardware, alternate integrators and recovery rights after supplier insolvency. A supplier certification does not prove that the installed version, configuration and service route satisfy the project's requirements.

10. Make detection useful to operations

Detection should focus on events that can change service. The monitoring design needs logs and alarms for privileged access, configuration changes, new devices, remote sessions, disabled protection, failed backups, abnormal controller communication, physical-access exceptions and safety-system interaction. The priority is timely recognition and safe response rather than collection without use.

Time synchronisation, secure retention and ownership matter. CERT-In's 2022 directions require specified Indian organisations, including data centres, to enable ICT-system logs and retain them securely for a rolling 180 days within India, together with other reporting and customer-information obligations. Scope and current implementation should be confirmed with Indian counsel. The requirement illustrates how local evidence-retention rules can shape architecture.

Every material alert should have an operating playbook. The playbook states who can isolate a conduit, disable vendor access, move to local control, call emergency services, communicate with customers, preserve evidence, notify authorities and authorise restoration. Operations and safety leaders should participate in its design.

11. Join incident response to safe operation

The incident process begins with triage and safety. The team should determine whether a cyber event is affecting or could affect power, cooling, fire, access or customer service. It should preserve safe local control, prevent uncontrolled changes, establish an incident command and separate containment from recovery decisions.

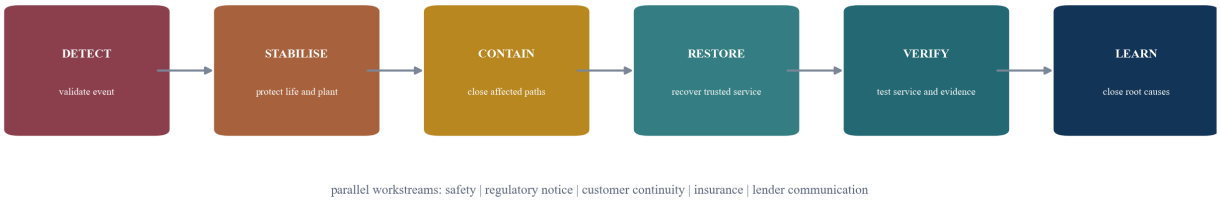
Notification clocks vary by jurisdiction, contract and incident type. The EU implementing regulation identifies sector-specific significance criteria for data-centre providers, including complete unavailability, limited availability lasting more than one hour, certain data compromises

and compromised physical access. Customer contracts, insurance policies, regulators and financing documents may impose additional notice obligations.

The board should approve a communications matrix before an event. It should name regulator, customer, insurer, lender, law-enforcement, technical adviser and public-communications contacts. The matrix should state the evidence threshold, decision owner, notice window and approved secure channel.

Figure 4. Integrated incident and recovery timeline

RESTORATION REQUIRES A TRUSTED OPERATING STATE



parallel workstreams: safety | regulatory notice | customer continuity | insurance | lender communication

Timing is illustrative; legal and contractual notification periods require current advice.

12. Design backup, restore and black-start evidence

Backups should include controller logic, protection settings, switch and firewall configurations, building-management databases, infrastructure-management data, access-control data, critical documentation and approved software or firmware. Copies should be protected from the same identity, network and ransomware event that could affect production. The team should know which backups are authoritative and how to rebuild a trusted system.

Recovery objectives need service meaning. A four-hour configuration restore may be irrelevant if safe plant restart requires twelve hours of engineering validation and customer acceptance. The recovery-time objective should include isolation, forensic decision, rebuild, configuration verification, equipment test, staged load and return to contracted service. The recovery-point objective should reflect the operational value of lost history and changes.

Black-start and degraded-mode procedures should cover loss of utility, loss of management networks, unavailable remote vendors and untrusted central systems. NIST SP 800-82 and NCSC OT guidance emphasise operational constraints and resilience. A live test must be designed by qualified engineers and safety personnel to avoid creating the failure it seeks to assess.

13. Use testing as a financing acceptance mechanism

The test programme should begin during design and procurement. Factory tests can verify product security features and configuration export. Site acceptance can verify segmentation, account management, logging, failover and local control. Integrated systems testing can examine utility loss, generator start, cooling response, access continuity and communications. Cyber exercises can then overlay loss of trust, vendor compromise or ransomware.

Testing should use a signed plan, safety review, preconditions, expected results, observers, evidence capture, deviation process and closure authority. Findings should be graded by service, safety, exploitability, recovery consequence and contractual exposure. A high-severity issue remains open until corrected, tested and accepted by the authorised owner.

CISA's Cross-Sector Cybersecurity Performance Goals provide a prioritised baseline across IT and OT, while NIST CSF Profiles can express current and target outcomes. These tools can organise the test catalogue. They do not certify a site or replace qualified testing.

Table 4. Construction-to-operations test and acceptance schedule

Gate	Required test	Acceptance evidence	Financing consequence
design freeze	architecture, critical-service and threat review	signed zone map, requirements trace and exception list	security capex and schedule included in base case
factory acceptance	identity, configuration export, logging, failure mode and recovery feature	witnessed protocol, results and closed deviations	supplier milestone can become eligible for draw
site acceptance	segmentation, remote access, account lifecycle, alarm and local-control test	signed site results and asset baseline	installation completion can be recognised
integrated systems test	power, cooling, access, communications and degraded-mode scenarios	coordinated test record and operating procedure	operational-readiness condition can be satisfied
recovery exercise	protected backup, rebuild, restoration and service verification	measured recovery time, evidence log and approved exceptions	liquidity and covenant stress can use tested values
operating assurance	recurring access review, vulnerability response, drills and independent validation	board pack, closure register and assurance report	ongoing undertakings and reporting remain current

Test scope and safety controls require project-specific engineering approval.

14. Integrate insurance and contractual risk allocation

Insurance review should cover property damage, machinery breakdown, business interruption, cyber, crime, professional liability, construction and delay exposures as applicable. The project should understand triggers, sublimits, exclusions, waiting periods, deductibles, contingent business interruption, restoration cost, incident consent, panel providers and evidence duties. A policy quote does not prove that a loss will be covered.

Customer contracts determine service credits, termination, notification, audit rights and security obligations. Construction and supply contracts determine design responsibility, defect correction, vulnerability support and delay. Operator and maintenance contracts determine staffing,

monitoring, patching, spares, recovery and indemnity. Financing documents can require insurance, incident notice, compliance, testing and remediation.

The risk-allocation matrix should identify gaps and circular dependencies. A customer may require a recovery time that exceeds the vendor's support commitment. A cyber policy may exclude infrastructure failure. A supplier may limit liability below the cost of a service interruption. The board should decide which residual risks remain with sponsor equity and liquidity.

15. Model an illustrative 48 MW operating campus

Consider a hypothetical 48 MW commissioned campus with contracted revenue of USD 86 million a year. Management assumes an EBITDA margin of 55 per cent, annual cash interest of USD 18 million, scheduled principal of USD 8 million and minimum cash of USD 12 million. These amounts are not market forecasts or project data.

The base case assumes normal service. A contained event reduces billable capacity for six hours, produces service credits and recovery cost, and uses USD 1.6 million of cash. A serious event produces a 36-hour impairment, additional customer remedies, specialist response, hardware replacement and a delayed invoice cycle, using USD 9.5 million. A severe case causes a seven-day service interruption, contract termination at one module, material restoration cost and refinancing delay, using USD 31 million before any insurance recovery.

The model should separate immediate cash outflow, lost revenue, service credits, repair cost, working-capital timing, insurance receipts and longer-term customer effects. Insurance is excluded from the initial liquidity case until coverage, timing and collectability are sufficiently evidenced. The base probability of each event is also excluded from debt sizing unless supported by a qualified risk method.

Table 5. Illustrative resilience and liquidity stress

Assumption or output	Base	Contained event	Serious event	Severe event
service impairment	none	6 hours	36 hours	7 days plus one module termination
immediate cash use	USD 0.0m	USD 1.6m	USD 9.5m	USD 31.0m
insurance receipt in initial liquidity test	USD 0.0m	USD 0.0m	USD 0.0m	USD 0.0m
assumed minimum cash before event	USD 12.0m	USD 12.0m	USD 12.0m	USD 12.0m
additional committed liquidity required	project-specific	project-specific	project-specific	project-specific
tested recovery evidence	required	required	required	required

All amounts and durations are management assumptions for method demonstration only.

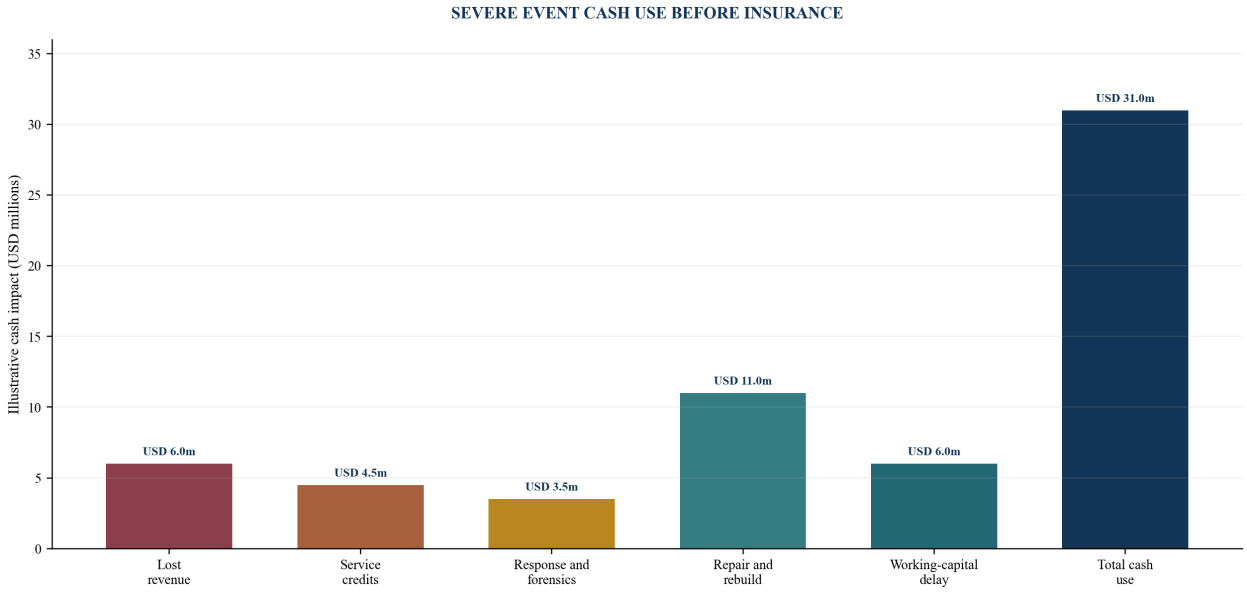
16. Connect resilience to prudent debt capacity

Debt capacity should use a cash-flow model that recognises the tested recovery range and the contractual consequence of service impairment. The lender can apply a downside case, minimum liquidity, debt-service reserve, capex reserve, distribution lock-up and reporting covenant. The exact structure depends on the asset stage, customer contracts, sponsor, jurisdiction and lender policy.

The illustrative model should avoid false precision. A cyber event frequency derived from another sector or portfolio may not describe a specific campus. A recovery time claimed in a policy may not be operationally tested. An insurance limit may not equal a timely cash receipt. The prudent case uses observed test evidence, explicit assumptions and sensitivity ranges.

NIST IR 8286D describes using business impact analysis to connect compromised technology assets to organisational consequences. The financing model applies the same logic to contracted capacity, cash, reserves and debt service. It does not convert a security framework into a credit rating or approval.

Figure 5. Illustrative cyber-physical loss waterfall



Values are management assumptions and exclude insurance receipts from initial liquidity.

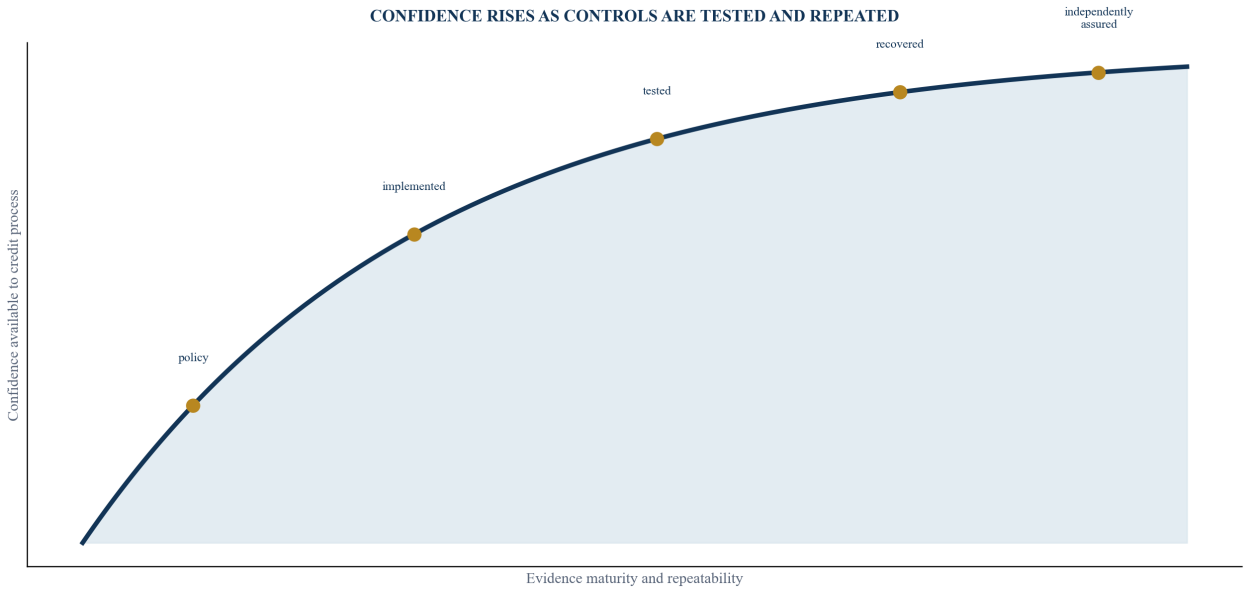
17. Set recovery-linked financing controls

Financing controls should match the evidence gap. During construction, a draw condition can require approved architecture, secured remote access, vendor lifecycle terms, tested backup and closed critical findings. Before operational conversion, conditions can require integrated testing, customer acceptance, insurance and a signed incident plan. During operations, undertakings can require periodic testing, material-incident notice, annual assurance and timely remediation.

Liquidity should cover the period before service and collections recover. A debt-service reserve addresses scheduled debt payments. An operating reserve can address emergency procurement and specialist response. A distribution lock-up can apply when tested recovery exceeds the approved threshold, critical findings remain open or liquidity falls below the agreed floor.

The lender should avoid operating the security programme. Management remains responsible for the asset, controls and incident decisions. The finance documents define evidence, reporting and financial consequences. Qualified technical advisers evaluate the control system and recovery evidence.

Figure 6. Resilience maturity and financing treatment



The curve is conceptual; it is not a pricing model, rating scale or lender commitment.

18. Build the lender and board data room

The data room should let an authorised reviewer trace every material claim. Core folders should include governance, scope, architecture, asset register, critical-service analysis, legal applicability, policies, risk and exception registers, physical security, identity, segmentation, vendor contracts, vulnerability management, logging, incident response, continuity, backups, test results, insurance, customer obligations and remediation.

Evidence needs dates, owners and status. Diagrams should identify the approved version. Test reports should show scope, assumptions, result, deviations and closure. Policies should link to operating records. Sensitive configuration and vulnerability details require controlled access, logging and redaction. A lender does not need unrestricted exposure to information that would increase risk.

The board pack should remain concise. It should show critical services, top residual risks, tested recovery, open high-severity findings, overdue actions, material incidents, reserve sufficiency, upcoming lifecycle events and decisions required. The underlying data room supports verification.

Table 6. Board and lender evidence scorecard

Evidence domain	Minimum decision evidence	Red flag	Accountable owner
governance and applicability	approved appetite, obligations register and responsibility map	no named executive or uncertain entity scope	board risk sponsor and legal
architecture and assets	current zones, conduits, critical assets and dependencies	unknown remote path or unsupported critical controller	engineering and information security
access and physical security	approved roles, remote-support matrix and layered access records	shared permanent privilege or uncontrolled visitor route	security and site operations
detection and response	protected logs, alert playbooks, notification matrix and exercise results	events cannot be traced or authority is unclear	security operations and incident commander
recovery and continuity	protected backups, tested restore, degraded mode and measured recovery	policy objective without successful service restoration	operations and business continuity
finance and insurance	quantified cash stress, reserves, contract remedies and coverage review	insurance assumed as immediate cash or unbounded customer exposure	finance, insurance and commercial teams

Status should be supported by dated evidence and accountable approval.

19. Run a 180-day resilience office

The first 30 days establish scope, authority and facts. The team confirms critical services, asset boundaries, jurisdiction, architecture, remote connections, customer obligations, existing tests, insurance and financing requirements. It creates one risk, exception and evidence register.

Days 31 to 90 close urgent gaps and design the target state. Workstreams address privileged access, vendor paths, segmentation, logging, backups, physical-security integration, incident command, notification and procurement clauses. Finance builds the service-to-cash model and reserve cases. The board approves remediation funding and risk acceptance.

Days 91 to 150 implement and test. The programme performs controlled access, detection, restore, degraded-mode and integrated exercises. Findings receive owners and deadlines. Lender and customer materials are updated with verified evidence.

Days 151 to 180 complete independent review, close critical findings, agree ongoing reporting and prepare the operating assurance calendar. The office should leave behind accountable processes, evidence owners and tested recovery. A dashboard without operating adoption is an incomplete outcome.

20. Convert the framework into an accountable mandate

A mandate can begin with a fixed-scope lender-grade cyber-resilience diagnostic. The output is a critical-service map, evidence-quality assessment, cash-flow stress, red-flag register, remediation sequence and financing data-room plan. Qualified cyber, OT, engineering, physical-security and legal specialists retain responsibility for their disciplines.

The next phase can support transaction execution: coordinating evidence owners, aligning technical findings with the model and credit materials, mapping customer and insurance obligations, managing the data room and tracking conditions to funding. A retained resilience office can maintain the board pack, closure register and test calendar through construction, financing and operational conversion.

Commercial demand, mandate conversion, fee level and timing remain unverified until a client signs an engagement, invoices are issued and cash is collected. Advisory revenue remains zero until those events occur. The useful commercial test is whether a developer, operator, sponsor or lender authorises a paid diagnostic and the follow-on execution scope.

References

[1] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, February 2024, https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final

[2] National Institute of Standards and Technology, Guide to Operational Technology (OT) Security, SP 800-82 Revision 3, September 2023, https://www.nist.gov/publications/guide-operational-technology-ot-security

[3] National Institute of Standards and Technology, Integrating Cybersecurity and Enterprise Risk Management, IR 8286 Revision 1, December 2025, https://csrc.nist.gov/pubs/ir/8286/r1/final

[4] Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals, https://www.cisa.gov/cybersecurity-performance-goals

[5] CISA and international partners, Secure by Demand: Priority Considerations for OT Owners and Operators when Selecting Digital Products, January 2025, https://www.cisa.gov/sites/default/files/2025-01/joint-guide-secure-by-demand-priority-considerations-for-ot-owners-and-operators-508c_0.pdf

[6] European Union, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[7] European Union, Commission Implementing Regulation (EU) 2024/2690, October 2024, https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

[8] UK National Cyber Security Centre, Operational Technology: Secure Connectivity Principles, January 2026, https://www.ncsc.gov.uk/collection/operational-technology/secure-connectivity/introduction

[9] UK National Protective Security Authority, Protective Security Considerations, https://www.npsa.gov.uk/specialised-guidance/secure-business/protective-security-considerations

[10] Cyber Security Agency of Singapore, Cybersecurity Code of Practice for Critical Information Infrastructure, updated December 2022, https://www.csa.gov.sg/legislation/codes-of-practice/

[11] National Cybersecurity Authority, Saudi Arabia, Operational Technology Cybersecurity Controls OTCC-1:2022, updated October 2025, https://nca.gov.sa/en/regulatory-documents/controls-list/otcc/

[12] Dubai Electronic Security Center, Standards and Policies: ICS Security Standard, https://www.desc.gov.ae/regulations/standards-policies/

[13] Australian Cyber and Infrastructure Security Centre, Guidance for the Critical Infrastructure Risk Management Program, March 2025, https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf

[14] Central Electricity Authority, India, CEA Cyber Security in Power Sector Guidelines, 2021, https://cea.nic.in/cyber-security/?lang=en

[15] Indian Computer Emergency Response Team, Directions under section 70B of the Information Technology Act, 28 April 2022, https://cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[16] International Electrotechnical Commission, IEC 62443-2-1:2024 Security program requirements for IACS asset owners, https://webstore.iec.ch/en/publication/62883

[17] International Electrotechnical Commission, IEC 62443-4-1:2018 Secure product development lifecycle requirements, https://webstore.iec.ch/en/publication/33615

[18] International Electrotechnical Commission, IEC 62443-4-2:2019 Technical security requirements for IACS components, https://webstore.iec.ch/en/publication/34421

About the Author

Chennakeshav Adya, Independent Researcher