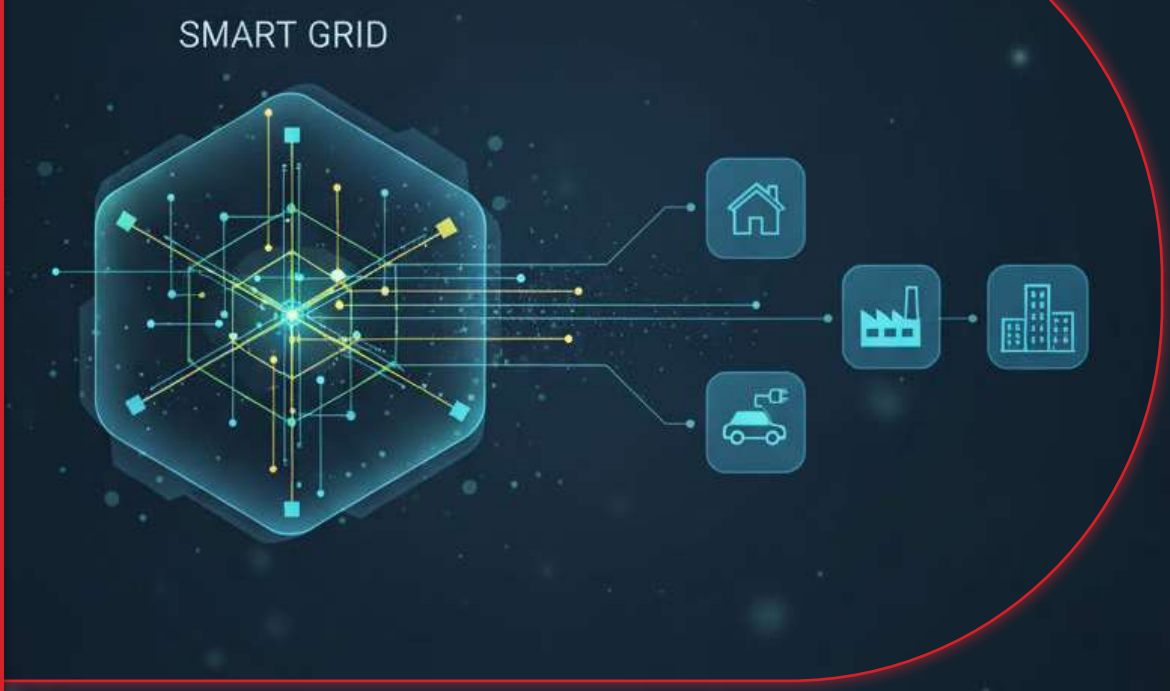
SOFTENGER
Strive to Excel

Grid Modernization Readiness Checklist



for Utility IT Leaders

Executive Summary:-

Grid modernization has shifted from a long-term transformation initiative to an immediate operational and risk-management priority for U.S. utilities. As grids become more distributed, digital, and interconnected, IT infrastructure decisions now directly affect reliability, security, and regulatory exposure.

This checklist enables utility IT leaders to:

- ☑ Objectively assess grid modernization readiness across infrastructure, cloud, security, and operations
- ☑ Identify gaps that increase outage duration, cyber risk, or compliance exposure
- ☑ Support internal justification for deeper evaluations, phased modernization, and budget prioritization

This is intentionally designed as a vendor-neutral self-assessment to support informed planning and executive alignment.

Who This Is For

- CIOs and Heads of Infrastructure
- IT Directors responsible for grid-facing platforms
- IT leaders supporting OT operations, cybersecurity, and compliance teams

Assessment Method

Yes

Fully implemented, operational, and consistently enforced

Partial

Implemented but incomplete, manual, or inosistently applied

No

Not implemented; represents moderation gap

Important: "Partial" responses often introduce the highest hidden risk, especially during outages, audits, or cyber incidents.

Scoring Guidance

- **80–100% Yes:** Strong foundation; focus on optimization and resilience tuning
- **50–79% Yes:** Moderate risk; targeted modernization required
- **Below 50% Yes:** High risk; modernization should be prioritized

Section 1. Grid Visibility & Digital Monitoring Readiness

Objective: Assess real-time observability across grid systems

- Real-time visibility across generation, transmission, and distribution
- Substations equipped with digital sensors and IEDs streaming telemetry
- AMI data integrated into enterprise analytics platforms
- IT teams can access telemetry without manual extraction
- Monitoring enables proactive fault detection (not just alerts)

Why It Matters

Limited visibility directly increases outage duration, slows restoration, and reduces operational confidence during grid events.

Section 2. IT Infrastructure Resilience & Availability

Objective: Validate infrastructure readiness for grid-critical workloads

- Grid-supporting systems designed for high availability and fault tolerance
- Documented RTO/RPO targets for control, monitoring, and analytics platforms
- DR and failover capabilities tested at least annually
- Infrastructure performance aligned with grid SLAs
- Redundancy across network, compute, and storage layers

Reference Benchmarks (Typical)

System Category	RTO	RPO
Control & Monitoring Systems	Minutes to < 1 hour	Near-zero to minutes
Operational Data Platforms	< 1 hour	Minutes
Analytics & Visibility Systems	1–4 hours	Minutes to hours

Section 3. Hybrid IT & Cloud Readiness

Objective: Assess maturity of hybrid infrastructure strategy

- Defined hybrid IT reference architecture (edge, data center, cloud)
- Latency-sensitive workloads intentionally retained on-prem or at the edge
- Cloud workloads governed by security, compliance, and cost controls
- Workload placement based on performance, regulation, and resilience
- Workloads can move across environments without disruption

Common Risk:

Unstructured cloud adoption often introduces latency, compliance gaps, and cost overruns—especially for grid-facing systems.

Section 4. IT–OT Integration & Governance

Objective: Evaluate coordination between IT and OT environments

- IT and OT environments segmented but securely integrated
- OT–IT data flows documented and continuously monitored
- Shared governance across IT, OT, and cybersecurity teams
- Clear ownership, escalation paths, and decision rights
- Changes to grid-facing systems centrally governed

Maturity Signal:

Clear IT–OT responsibility models reduce outages, incident confusion, and recovery delays.

Section 5. Cybersecurity & NERC CIP Alignment

Objective: Assess security posture for modern, connected grids

- Zero Trust architecture implemented or actively planned
- Continuous vulnerability monitoring across IT and OT assets
- SOC integration for both IT and OT security events
- NERC CIP controls operationalized—not just documented
- Incident response and recovery plans tested jointly

Risk Highlight:

Weaknesses in IT infrastructure frequently become entry points into OT environments, amplifying operational and regulatory risk.

Section 6. Automation & Operational Maturity

Objective: Measure ability to operate grid infrastructure at scale

- Automated patching, monitoring, and remediation
- Alerts prioritized using analytics or AI correlation
- Remote incident resolution without on-site dependency
- True 24x7 monitoring coverage
- Continuous performance and availability optimization

Section 7. Compliance, Audit & Reporting Readiness

Objective: Ensure infrastructure supports regulatory and audit requirements

- Infrastructure controls mapped directly to NERC CIP requirements
- Audit evidence produced quickly and consistently
- Logs retained, protected, and monitored per mandates
- Compliance embedded into infrastructure design

Common Readiness Gaps Across U.S. Utilities

Across U.S. energy and utilities organizations, several recurring readiness gaps emerge during grid modernization assessments:

Visibility gaps
between OT telemetry and IT analytics platforms

Automation limited
to monitoring, not remediation

"Partial" DR capabilities
that exist on paper but are untested or manual

Unclear IT–OT ownership
especially during incidents

Hybrid IT sprawl,
where cloud adoption outpaces governance

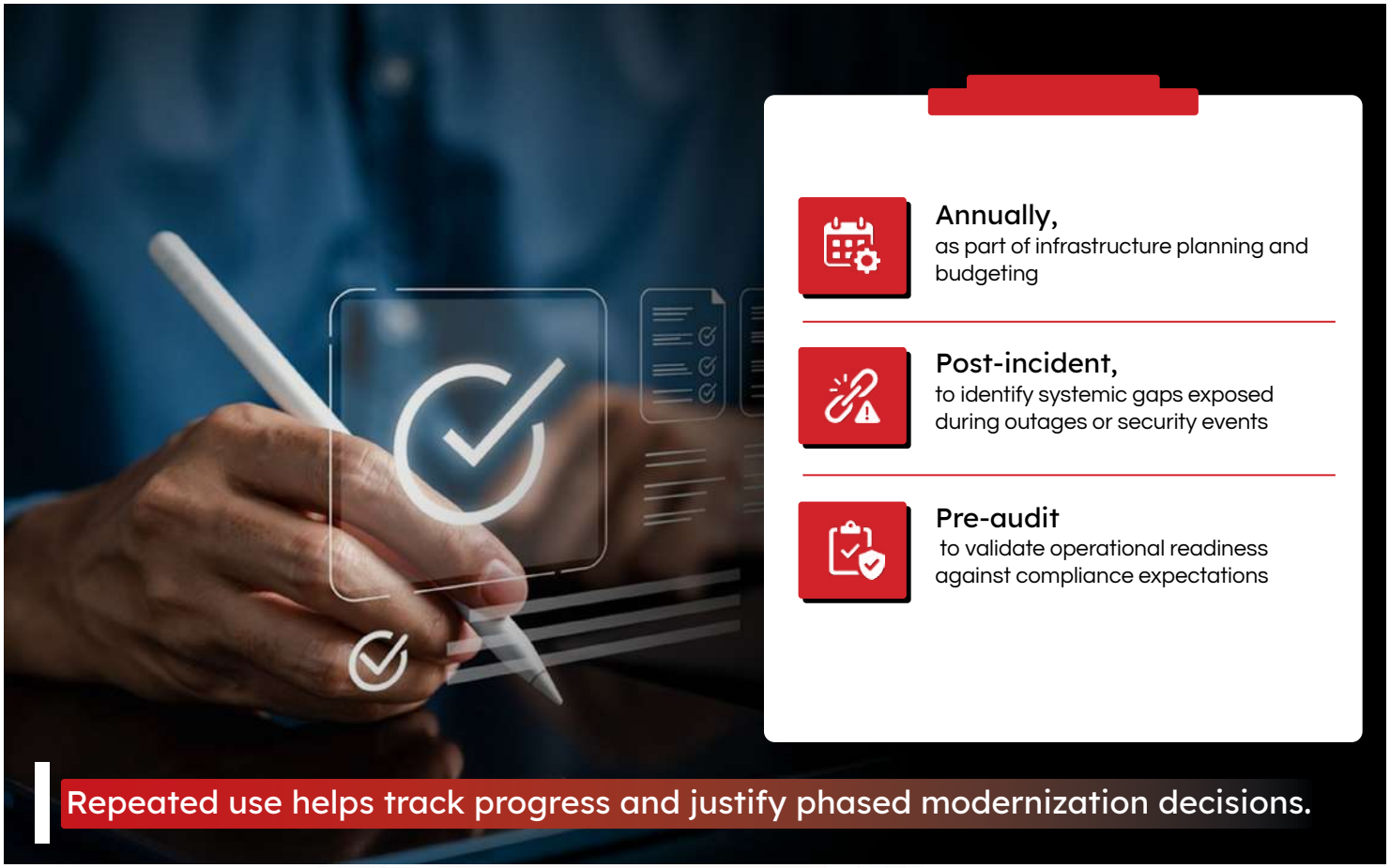
Compliance controls
documented for audits but not operationalized

Individually, these gaps may seem manageable. Collectively, they compound risk during outages, cyber incidents, or regulatory scrutiny—often exposing weaknesses only when stakes are highest.

Readiness Summary & Risk Profile

How and When to Reuse This Checklist

This checklist is most effective when used:



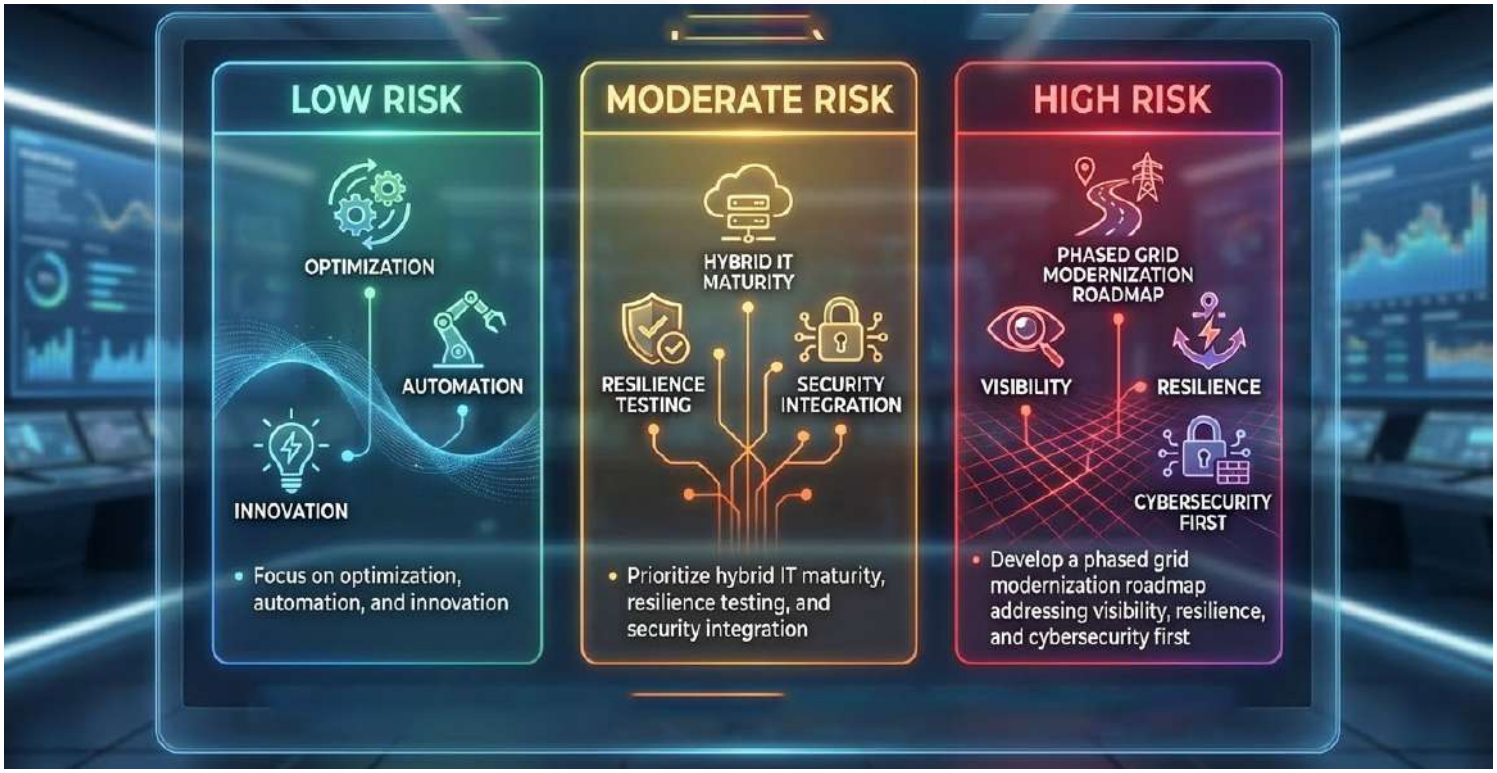
Annually,
as part of infrastructure planning and budgeting

Post-incident,
to identify systemic gaps exposed during outages or security events

Pre-audit
to validate operational readiness against compliance expectations

Repeated use helps track progress and justify phased modernization decisions.

What to Do Next



SOFTENGER
Strive to Excel

Request a 30-minute **Grid Modernization Readiness** Review with an **Infrastructure Specialist.**

This session is designed to validate findings, surface blind spots, and support confident next-step planning—without obligation.

Book a Consultation Call