THE BAZZ GLOBAL

Cybersecurity Resilience Framework

Risk-Aligned Deployment and Institutional Uplift System

Version 1.0 — August 2026

Bazz Global LLC

A vendor-neutral, outcome-based operating framework for resource-constrained essential-service organizations

R • A • D • I • U • S

Recognize | *Align* | *Deploy* | *Inspect* | *Uplift* | *Share*

Publication Notice

Bazz RADIUS is a voluntary cybersecurity resilience and institutional-capacity framework developed by Bazz Global LLC. It is designed to help organizations translate recognized cybersecurity outcomes into prioritized, verified, locally sustainable operating practices. It does not replace NIST, CISA, sector regulation, contractual requirements, or professional judgment. It is not a certification standard and does not guarantee that cyber incidents will be prevented.

The framework is intentionally outcome-based and vendor-neutral. Organizations may use existing technologies, service providers, and control libraries so long as they can demonstrate the RADIUS outcomes with reliable evidence. Sector profiles and implementation targets must be tailored to legal, safety, operational, procurement, labor, privacy, and technical constraints.

Version 1.0 is designed for local governments and special districts, K–12 school systems, community and rural healthcare organizations and their business associates, and small and midsized manufacturers and supply-chain firms. It can be extended to other essential-service and critical-infrastructure communities through additional profiles.

Executive Summary

Cybersecurity frameworks often define what good outcomes look like. Resource-constrained organizations can still struggle with the next question: what should be done first, who owns it, how should limited funds be allocated, how can effectiveness be proven, and how can capability remain after outside assistance ends? Bazz RADIUS addresses that implementation gap.

RADIUS stands for Risk-Aligned Deployment and Institutional Uplift System. The framework converts mission consequence into a closed-loop resilience cycle: recognize essential services and failure consequences; align a minimum viable resilience baseline to those consequences; deploy the highest-value safeguards in time-bounded sprints; inspect whether controls actually work; uplift local personnel so the capability becomes institutional; and share de-identified lessons so one organization's improvement can benefit a wider community.

The design draws from the outcome orientation of the NIST Cybersecurity Framework, the prioritization logic of CISA Cybersecurity Performance Goals, the lifecycle risk-management approach of the NIST AI Risk Management Framework, the management-system discipline reflected in ISO/IEC 42001 implementation materials, and practical AI audit concepts in the attached compliance materials. RADIUS does not claim ownership of those underlying standards. Its contribution is the integration, sequencing, validation, capability-transfer, and community-learning architecture described in this publication.

RADIUS Function	Purpose	Primary Question	Principal Output
R — RECOGNIZE	Mission and public-consequence mapping	What must continue, what can fail, and who is affected?	Mission Dependency & Consequence Map
A — ALIGN	Minimum Viable Cyber Resilience baseline	What is the smallest coherent set of outcomes that materially reduces consequence?	Current/Target Resilience Profile
D — DEPLOY	Risk-reduction-per-dollar control sprints	What should be implemented first, by whom, and by when?	90-Day Resilience Sprint Plan
I — INSPECT	Continual assurance and operational validation	Do safeguards work in practice and under pressure?	Evidence Register & Validation Report
U — UPLIFT	Institutional capability transfer	Can local personnel sustain, operate, and improve the safeguards?	Resilience Champion & Runbook Package
S — SHARE	Cohort learning and community uplift	What can be safely reused across comparable organizations?	De-identified Benchmark & Sector Playbook

1. Foundations of the Bazz RADIUS Framework

1.1 Design Objective

The objective of Bazz RADIUS is to improve measurable cyber resilience and continuity where cyber failure can affect populations, public services, supply chains, or connected institutions. The framework is optimized for organizations that cannot maintain separate full-time teams for security engineering, governance, audit, incident response, business continuity, third-party risk, privacy, and compliance.

1.2 Seven Design Principles

Principle	Meaning
Mission before machinery	Begin with services, people, dependencies, and consequences before inventorying technical weaknesses in isolation.
Minimum viable resilience	Establish a coherent baseline that can be afforded, operated, and verified; then mature it over time.
Risk reduction per dollar	Sequence remediation by consequence, threat exposure, exploitability, dependency, feasibility, and cost rather than checklist order.
Evidence over assertion	A documented policy is not treated as effective until implementation evidence or operational testing supports the outcome.
Recovery is a control	Backup existence is insufficient; recoverability, restoration priority, and decision readiness must be demonstrated.
Capability must transfer	Each engagement should leave behind trained people, ownership, runbooks, and repeatable evidence practices.
Learning should compound	De-identified lessons, benchmark patterns, and reusable playbooks should improve later implementations and, where appropriate, noncustomers.

1.3 Intended Audience

RADIUS is intended for executive leaders, governing boards, technology leaders, security and risk professionals, internal auditors, compliance teams, business-continuity leaders, service owners, procurement teams, and designated Resilience Champions. It is also designed to support external assessors and funding or oversight bodies that need clear evidence of progress without requiring a single technology stack.

2. RADIUS Architecture

RADIUS uses three interacting layers: the Core, Profiles, and Capability Levels. The Core defines universal outcomes through six functions. Profiles tailor those outcomes to a sector, mission, and organization. Capability Levels describe the repeatability and institutionalization of implementation without equating maturity with absolute security.

Layer	Description	Use
Core	Six functions, categories, and outcomes that form the resilience lifecycle.	Provides a common operating language.
Profiles	Current and Target outcomes selected for a specific mission, sector, threat context, and resource envelope.	Creates a prioritized implementation scope.
Capability Levels	Four levels describing whether practices are ad hoc, repeatable, managed, or adaptive.	Supports realistic progression and governance reporting.
Evidence Model	Required evidence classes and confidence ratings for claimed outcomes.	Prevents paper compliance and enables independent review.
Community Learning	De-identification, aggregation, benchmarking, and reusable playbooks.	Extends learning beyond a single engagement.

2.1 Capability Levels

Capability Level	Definition
Level 1 — Reactive	Practices are largely informal, person-dependent, or event-driven. Evidence is incomplete.
Level 2 — Repeatable	Priority practices are documented, assigned, and performed on a defined cadence.
Level 3 — Managed	Practices are measured, validated, integrated with governance, and linked to mission outcomes.
Level 4 — Adaptive	The organization uses trend evidence, exercises, incidents, threat intelligence, and peer learning to continuously adjust controls and priorities.

3. The Bazz RADIUS Core

The Core is the heart of the framework. Each function contains categories and outcome statements. Organizations may map these outcomes to NIST CSF 2.0, CISA CPGs, sector requirements, ISO/IEC standards, contractual controls, or internal policies. RADIUS adds implementation logic and evidence expectations rather than replacing those source authorities.

R — RECOGNIZE

Establish the mission context and consequence model before selecting safeguards. The unit of analysis is the essential service and the people or systems that depend on it.

ID	Category	RADIUS Outcome
R.MS	Mission Services	Essential services, critical business processes, service owners, acceptable downtime, and minimum operating conditions are documented.
R.BN	Beneficiaries & Consequences	Patients, students, residents, employees, suppliers, partner agencies, customers, and other affected groups are identified; consequence scenarios are documented.
R.AD	Assets & Data	Assets, applications, data, identities, operational technology, and facilities supporting essential services are identified and prioritized.
R.DP	Dependencies	Upstream/downstream systems, cloud services, utilities, vendors, business associates, suppliers, and single points of failure are mapped.
R.TE	Threat & Exposure	Relevant threats, internet exposure, known vulnerabilities, identity attack paths, and likely failure modes are evaluated.
R.RP	Restoration Priorities	Recovery sequence, minimum service levels, dependencies, and decision authorities are established.

A — ALIGN

Build a Minimum Viable Cyber Resilience baseline that is coherent, affordable, and proportionate to the organization's highest-consequence risks.

ID	Category	RADIUS Outcome
A.GV	Governance	Cybersecurity roles, risk ownership, policies, escalation thresholds, exceptions, funding decisions, and governing-body reporting are established.
A.ID	Identity & Access	MFA, privileged access, joiner/mover/leaver processes, service accounts, remote access, and least privilege are prioritized.
A.VM	Vulnerability & Configuration	Asset visibility, secure configuration, patching, vulnerability remediation, unsupported technology, and exception handling are baselined.
A.DP	Data Protection	Data classification, encryption, retention, backup, recovery, and sensitive-data handling are aligned to mission consequence.
A.LD	Logging & Detection	Priority logs, alert ownership, time synchronization, endpoint/network visibility, and escalation pathways are established.
A.IR	Incident & Recovery	Incident roles, communications, legal/regulatory triggers, continuity procedures, backups, restoration, and exercises are integrated.
A.SC	Supply Chain	Critical suppliers and technology providers are risk-tiered; contractual, access, incident notification, and continuity expectations are defined.
A.WF	Workforce	Role-based awareness, phishing resilience, privileged-user training, and Resilience Champion responsibilities are defined.

D — DEPLOY

Turn prioritized gaps into accountable implementation. RADIUS favors short, evidence-based control sprints over static multi-year remediation lists.

ID	Category	RADIUS Outcome
D.PR	Prioritization	Remediation is ranked using consequence, exposure, exploitability, dependency, cost, feasibility, and time-to-risk-reduction.
D.SP	Sprint Planning	High-value changes are grouped into approximately 90-day sprints with scope, owner, due date, evidence, dependencies, and acceptance criteria.
D.OW	Ownership	Every action has an accountable owner and executive sponsor; unresolved items have escalation and exception paths.
D.CH	Change Execution	Changes follow appropriate testing, approval, rollback, safety, and operational-change controls.
D.RS	Resource Strategy	Controls are selected with explicit consideration of staffing, licensing, implementation effort, grant/funding options, and sustainability.

D.CL	Closure	A task closes only when implementation evidence is accepted and, where appropriate, retesting confirms the intended outcome.

I — INSPECT

Determine whether safeguards operate as intended. Validation includes evidence review, technical verification, exercises, and restoration testing.

ID	Category	RADIUS Outcome
I.EV	Evidence Assurance	Evidence is current, attributable, complete, reproducible where practical, and tied to the claimed outcome.
I.EX	Exposure Validation	External exposure, vulnerabilities, configuration weaknesses, and attack paths are periodically re-evaluated.
I.AC	Access Validation	MFA, privileged access, inactive accounts, role changes, and access reviews are tested.
I.RC	Recovery Validation	Backups are restored on a defined cadence; recovery time and recovery point performance are measured against mission needs.
I.TT	Tabletop & Simulation	Decision-makers exercise realistic scenarios, including communications, vendor dependencies, service degradation, and recovery.
I.ME	Measurement	Current-to-target profile movement, closure aging, exposure reduction, test results, and capacity metrics are reported.
I.CI	Continuous Improvement	Incidents, exercises, audit findings, near misses, and threat changes update the risk register, profile, and next sprint.

U — UPLIFT

Transfer capability so resilience becomes an institutional practice rather than a consultant-dependent activity.

ID	Category	RADIUS Outcome
U.RC	Resilience Champion	At least one local employee is designated, trained, and empowered to coordinate routine resilience activities.
U.RB	Runbooks	Role-specific runbooks cover recurring governance, incident, recovery, evidence, and escalation tasks.
U.TR	Role-Based Training	Executives, administrators, service owners, technical staff, and general users receive training relevant to their decisions and exposures.
U.TT	Train-the-Trainer	Local personnel receive reusable materials and guided practice to reinforce capability after intensive support ends.
U.KT	Knowledge Transfer	Architecture decisions, exceptions, vendor dependencies, lessons learned, and evidence locations are transferred and maintained.
U.SU	Sustainability	The organization establishes cadence, budget ownership, staffing coverage, succession, and periodic reassessment for priority practices.

S — SHARE

Convert safely reusable lessons into community value through de-identified benchmarks, profiles, playbooks, and feedback.

ID	Category	RADIUS Outcome
S.DI	De-identification	Shared information is screened to remove customer identifiers, sensitive technical details, regulated data, and exploitable information.
S.BM	Benchmarking	Comparable outcome measures are aggregated to identify recurring gaps, realistic improvement ranges, and implementation patterns.
S.CP	Community Profiles	Common priorities across a sector or cohort are expressed as reusable current/target patterns while preserving local tailoring.
S.PB	Sector Playbooks	Sanitized implementation sequences, evidence examples, exercise lessons, and decision aids are packaged for reuse.
S.DS	Dissemination	Appropriate findings are shared through briefings, workshops, publications, partner networks, or public resources.
S.FL	Feedback Loop	Peer results and external lessons are incorporated into RADIUS profiles, measures, training, and future sprints.

4. RADIUS Implementation Method

Phase	Purpose
Phase 0 — Charter	Define sponsor, scope, essential services, legal constraints, evidence access, confidentiality, and success criteria.
Phase 1 — Recognize	Conduct mission workshops, dependency mapping, asset/data correlation, consequence analysis, and exposure review.
Phase 2 — Align	Create Current and Target Profiles; select Minimum Viable Cyber Resilience outcomes; approve exceptions and funding priorities.
Phase 3 — Deploy	Execute 90-day control sprints. Track owner, due date, evidence, cost, blockers, exception, and retest status.
Phase 4 — Inspect	Validate implementation through evidence, scanning, access tests, tabletop exercises, and restoration tests.
Phase 5 — Uplift	Train the Resilience Champion and role owners; deliver runbooks, cadence, escalation paths, and evidence templates.
Phase 6 — Share & Rebaseline	De-identify eligible findings, update sector benchmarks/playbooks, capture lessons, and establish the next Target Profile.

4.1 Risk-Aligned Prioritization Model

RADIUS prioritization is designed to be transparent rather than mathematically absolute. Each candidate action is scored on a 1–5 scale across six factors. Weighting may be adjusted by sector, but the rationale must be documented. Safety, legal, and mission constraints can override the numerical score.

Factor	Illustrative Weight	Question
Mission/Public Consequence	25%	How severe is the service, safety, privacy, economic, or community consequence if the weakness is exploited?
Threat Exposure	20%	How exposed is the weakness to realistic threat actors or failure conditions?
Exploitability/Likelihood	15%	How feasible is exploitation or failure given current controls?
Dependency Amplification	15%	Could failure propagate through vendors, systems, locations, partners, or supply chains?
Time-to-Risk-Reduction	10%	How quickly can the action materially reduce exposure or improve recovery?
Feasibility & Sustainability	15%	Can the organization implement, operate, fund, and maintain the safeguard?

Illustrative Priority Score = weighted risk-reduction value ÷ normalized implementation burden. The score is a decision aid, not a substitute for expert judgment. Actions required by law, patient/student safety, or immediate active exploitation may be elevated regardless of calculated rank.

4.2 The 90-Day Resilience Sprint

Sprint Field	Required Content
Outcome	Specific RADIUS outcome and mapped source control/outcome.
Owner	Named accountable individual and executive sponsor.
Baseline	Current state and evidence date.
Action	Concrete implementation steps and dependencies.
Acceptance Criteria	Observable condition required for completion.
Evidence	Configuration, report, ticket, screenshot, log, test result, policy approval, or other proof.
Exception	Risk acceptance authority, compensating control, expiration, and review date.
Retest	Method, date, tester, result, and residual risk.
Benefit Link	Essential service and consequence reduced by the change.

5. RADIUS Evidence and Assurance Model

RADIUS distinguishes design, implementation, and operating evidence. An organization should not receive full credit for an outcome merely because a policy exists. Evidence confidence is rated so decision-makers can distinguish asserted, observed, tested, and sustained outcomes.

Confidence	Definition	Example
E0 — Asserted	Claim exists but reliable evidence has not been reviewed.	Interview statement only.
E1 — Documented	Design or policy evidence exists.	Approved MFA policy or backup standard.
E2 — Implemented	Configuration or transaction evidence shows implementation.	Identity-provider settings; backup job history.
E3 — Validated	Independent test or exercise demonstrates intended operation.	MFA bypass test; successful restoration; tabletop action log.
E4 — Sustained	Repeated evidence across time demonstrates continued operation and improvement.	Quarterly access tests; recurring restore success; aging trend improvement.

5.1 Minimum Evidence Rules

- Evidence must be attributable to a system, process, owner, and date.
- Screenshots should be supported by source context where feasible; configuration exports, logs, tickets, or system reports are preferred for repeatability.
- Sensitive evidence must be handled according to customer classification, legal, privacy, and contractual requirements.
- Control exceptions require an owner, rationale, compensating measure where feasible, expiration/review date, and residual-risk acceptance.
- Validation must avoid unsafe testing on clinical, educational, public-safety, or operational-technology systems without authorization and appropriate safeguards.

6. Measurement and Outcome Reporting

RADIUS measures progress against an organization's verified baseline rather than promising universal percentage reductions. Targets are prospective operating commitments and must be adjusted to sector constraints and the integrity of available evidence.

Measure	Definition
Mission coverage	% of essential services with documented owner, dependency map, restoration priority, and target profile.
Critical finding closure	% and aging of critical/high-priority findings closed with accepted evidence and retest where required.
External exposure	Count and age of validated high-risk internet-exposed weaknesses; recurrence rate.
Identity protection	% of privileged and remote-access accounts protected by phishing-resistant or appropriate MFA; stale account rate.
Recovery readiness	% of mission-critical services with tested backup/restoration; observed RTO/RPO versus target.
Exercise readiness	Scenario objectives achieved; decision latency; unresolved actions; repeat finding rate.
Profile improvement	Movement from Current to Target Profile by RADIUS category and capability level.
Local capability	Number of trained Resilience Champions; runbook completion; local execution of recurring tasks.
Third-party resilience	% of critical vendors risk-tiered with incident notification, access, continuity, and evidence expectations.
Community reuse	Number of de-identified lessons, playbooks, benchmark contributions, workshops, or external reuse events.

7. Sector Profiles

Sector Profiles tailor the Core to mission consequence. They are not separate frameworks. Each profile emphasizes dependencies, evidence, and scenarios that matter most to the sector while preserving the same RADIUS lifecycle.

7.1 K–12 Education Profile

- Student information systems, learning platforms, identity services, transportation, payroll, communications, special-education records, and safety systems should be treated as mission dependencies.
- Priorities commonly include MFA, privileged access, exposed services, immutable or isolated backups, incident communications, vendor access, phishing resistance, and restoration of instructional and administrative services.
- Exercises should test ransomware during instruction, loss of identity services, parent communications, student-data exposure, and recovery sequencing.

7.2 Community & Rural Healthcare Profile

- Clinical availability, patient safety, scheduling, pharmacy, laboratory, imaging, billing, claims, identity, medical devices, and business associates must be mapped to care continuity.
- Validation should emphasize access control, segmentation where appropriate, backup/restoration, downtime procedures, third-party dependencies, vulnerability management, logging, and incident escalation.
- Testing must be coordinated to avoid unsafe impact on patient care and regulated systems.

7.3 Local Government & Special District Profile

- Public safety support, utilities, billing, permitting, public records, courts, benefits, communications, elections-related dependencies where applicable, and emergency operations should be mapped to residents and partner agencies.
- Priority safeguards should account for shared services, aging infrastructure, third-party managed systems, remote administration, identity, backup/recovery, and public communications.
- Exercises should include ransomware, vendor compromise, loss of communications, public-information pressure, and continuity of essential resident services.

7.4 Manufacturing & Supply-Chain Profile

- Production, ERP, warehouse, engineering, supplier connectivity, logistics, operational technology, remote vendor access, and safety dependencies should be mapped to production and downstream customers.
- RADIUS distinguishes enterprise IT from OT safety and availability constraints; changes to production systems require engineering and safety governance.
- Priorities include identity, segmentation, remote access, vulnerability exposure, backups, recovery sequencing, vendor dependencies, incident isolation, and manual workarounds.

8. RADIUS AI Governance and AI Risk Overlay

Organizations increasingly use predictive, generative, embedded, and vendor-provided AI. The attached NIST AI RMF emphasizes that AI risks can be systemic or localized and organizes risk management through GOVERN, MAP, MEASURE, and MANAGE. The attached ISO 42001 implementation material similarly emphasizes a structured AI management system, risk assessment, policy development, implementation, and continuous improvement. RADIUS incorporates those concepts as an overlay so AI use is connected to the organization's mission, cybersecurity, vendor, privacy, and resilience practices rather than treated as a separate technology island.

RADIUS AI Outcome	Required Practice
AI Inventory & Ownership	Maintain an inventory of approved AI use cases, models, embedded AI capabilities, owners, vendors, data classes, and business purpose.
AI Risk Classification	Classify use cases by consequence, autonomy, sensitive data, external impact, security exposure, and reliance on third parties.
AI Governance	Define approval, prohibited/restricted uses, human oversight, accountability, change control, exception, and incident responsibilities.
AI Security & Privacy	Assess data leakage, prompt/instruction risks, model or agent access, secrets, insecure integrations, supply-chain risk, logging, and privacy obligations.
AI Validation	Test intended behavior, failure modes, access boundaries, output reliability where relevant, monitoring, and escalation before and after deployment.
Third-Party AI	Require appropriate transparency, security evidence, incident notification, data-use terms, retention expectations, and change notification from vendors.
AI Auditability	Preserve sufficient evidence to reconstruct approval, data/use constraints, risk decisions, tests, changes, incidents, and control operation.
AI Continuous Improvement	Use incidents, hallucination/error patterns, security findings, regulatory changes, user feedback, and model/vendor changes to update controls.

The AI overlay is deliberately technology-neutral. It does not certify model safety or replace specialized model evaluation. Its purpose is to ensure that AI-enabled services are governed, mapped to mission consequences, measured with appropriate evidence, and managed within the same resilience lifecycle as other digital dependencies.

9. Governance and Roles

Role	RADIUS Accountability
Governing Body / Executive Sponsor	Approve risk appetite, target profile, major exceptions, funding priorities, and resilience reporting.
Service Owner	Define mission requirements, acceptable downtime, dependencies, and operational acceptance criteria.
Technology/Security Lead	Coordinate technical implementation, evidence, vulnerability management, detection, and response.
Risk/Audit/Compliance	Challenge assumptions, assess evidence quality, track exceptions, and support independent validation.
Resilience Champion	Coordinate cadence, maintain runbooks/evidence, facilitate exercises, track actions, and sustain local capability.
Procurement/Vendor Management	Embed security, access, notification, continuity, and evidence requirements in third-party relationships.
Bazz Global / External Facilitator	Facilitate RADIUS assessment, prioritization, sprint design, validation, capability transfer, and de-identified learning subject to engagement scope.

10. Standard RADIUS Deliverables

- RADIUS Charter and Scope Statement
- Mission Dependency & Public-Consequence Map
- Current RADIUS Profile and Target RADIUS Profile
- Minimum Viable Cyber Resilience Baseline
- Risk-Aligned Priority Register
- 90-Day Resilience Sprint Plan
- Control Evidence Register
- External Exposure and Vulnerability Validation Summary
- Access Assurance Review
- Incident/Recovery Readiness Assessment
- Tabletop Exercise After-Action Report
- Backup and Restoration Validation Record
- Resilience Champion Training & Runbook Package
- Executive Resilience Scorecard
- De-identified Cohort Benchmark (where consented and appropriate)
- Sector Playbook / Community Learning Brief

11. Organizational Adoption Roadmap

An organization may adopt RADIUS as a complete program or use it to structure an existing cybersecurity initiative. Adoption should begin with a bounded set of essential services rather than an enterprise-wide attempt to document every technology at once.

Time Horizon	Recommended Outcome
Days 0–30	Charter; identify essential services and owners; map highest-consequence dependencies; collect baseline evidence; identify urgent exposures.
Days 31–60	Approve Current/Target Profiles and Minimum Viable Cyber Resilience baseline; select first sprint; assign owners and funding.
Days 61–90	Implement priority safeguards; begin evidence register; close urgent gaps; train Resilience Champion.
Days 91–180	Validate access, exposure, recovery, and incident readiness; complete tabletop; execute second sprint; address exceptions.
Months 7–12	Demonstrate sustained evidence; refine profile; mature vendor and AI overlays; contribute de-identified lessons where authorized.
Year 2+	Expand scope, increase capability level, automate evidence where appropriate, and use peer benchmarks and incident lessons for adaptive improvement.

12. Community Learning, Confidentiality, and Responsible Sharing

The SHARE function is designed to create broader value without creating new security or privacy risk. No customer-specific information should be published merely because it is useful for benchmarking. Sharing requires consent, de-identification, minimum aggregation thresholds where appropriate, and review for exploitability and regulated information.

- Remove names, addresses, IP addresses, domain names, account identifiers, system identifiers, unique incident details, regulated personal data, and other customer-identifying information unless explicitly authorized.
- Do not publish technical details that materially increase exploitability of an unresolved weakness.
- Separate benchmarking datasets from customer evidence repositories and apply access controls and retention rules.
- Use cohort statistics only when comparability and sample size support a meaningful interpretation; disclose limitations.
- Distinguish observed results from inferred or estimated effects. Do not claim that a control prevented an incident without supportable causal evidence.

13. Conceptual Crosswalk to Recognized Frameworks

This crosswalk is conceptual and intended to aid adoption. It is not an assertion of one-to-one equivalence or certification. Detailed mappings should be validated against the current authoritative publications and sector requirements.

RADIUS	NIST CSF 2.0 Emphasis	NIST AI RMF Analogy	Management-System Emphasis
RECOGNIZE	Identify; Govern context	MAP	Context, scope, interested parties, risk identification
ALIGN	Govern; Protect; Detect; Respond; Recover target outcomes	GOVERN + MAP	Risk treatment planning, policy, objectives
DEPLOY	Implementation of selected outcomes	MANAGE	Operational planning and control
INSPECT	Measure performance across CSF outcomes	MEASURE + MANAGE	Monitoring, internal review, corrective action
UPLIFT	Govern roles and workforce; continuous improvement	GOVERN	Competence, awareness, documented responsibilities
SHARE	Community Profiles; improvement	GOVERN + MANAGE learning	Continual improvement and organizational learning

14. RADIUS Assessment and Scoring Protocol

RADIUS reporting should separate Outcome Status from Evidence Confidence. A high maturity score with weak evidence is not treated as equivalent to a validated outcome. Each category receives an implementation status and an evidence confidence rating.

Implementation Status	Definition
0 — Not Addressed	Outcome is not implemented or evidence shows material absence.
1 — Initiated	Partial activity exists but ownership, coverage, or consistency is insufficient.
2 — Implemented	Outcome is substantially implemented for defined scope.
3 — Validated	Outcome is implemented and has been tested or independently validated.
4 — Sustained/Adaptive	Outcome is repeatedly evidenced, measured, and improved over time.

Executive reporting should show: (1) mission services covered; (2) high-consequence gaps; (3) sprint commitments and aging; (4) validated versus merely documented outcomes; (5) recovery and exercise results; (6) exceptions and residual risk; (7) capability transfer; and (8) changes since the prior reporting period.

15. Replication and Scalable Adoption Model

RADIUS is designed for replication through a standardized Core plus modular sector profiles, hybrid remote/on-site delivery, cohort-based training, reusable evidence packages, local Resilience Champions, and de-identified playbooks. This structure is intended to reduce the incremental effort required for later implementations without forcing identical controls on dissimilar organizations.

A multi-organization cohort can share orientation, training, exercise design, benchmark definitions, and sanitized lessons while preserving institution-specific risk decisions and confidential evidence. This creates a practical mechanism for regional and cross-state adoption by school systems, healthcare organizations, municipalities, manufacturers, and other essential-service institutions with similar constraints.

Appendix A — Minimum Viable Cyber Resilience (MVCR) Baseline

The MVCR baseline is a starting profile, not a universal compliance checklist. The following outcome families should ordinarily be considered before an organization declares a minimum viable resilience posture. Sector or legal requirements may require additional controls.

Outcome Family	Minimum Viable Expectation
Governance	Named executive sponsor; risk owner; incident authority; exception process; recurring executive reporting.
Inventory & Mission	Essential-service inventory; critical assets/data; vendor dependencies; restoration priorities.
Identity	MFA for privileged/remote/high-risk access; lifecycle process; privileged account separation; stale account review.
Vulnerability & Configuration	Supported systems; prioritized patching; secure configuration; external exposure review; documented exceptions.
Endpoint/Network Protection	Appropriate endpoint protection; segmentation or access boundaries; remote administration controls; logging.
Data & Backup	Sensitive-data handling; protected backups; restoration testing; retention and recovery ownership.
Detection & Escalation	Priority logs/alerts; monitored channels; incident thresholds; after-hours escalation.
Incident Response	Roles; communications; legal/regulatory triggers; containment; vendor coordination; evidence preservation.
Recovery & Continuity	Service restoration order; tested recovery; manual workarounds; crisis communications.
Third Parties	Critical vendor inventory; access controls; incident notification; continuity expectations; evidence review.
Workforce	Role-based awareness; phishing/social engineering resilience; Resilience Champion; periodic exercises.
AI Use	Approved-use inventory; ownership; sensitive-data rules; vendor AI risk; human oversight; auditability where AI is material.

Appendix B — RADIUS Record Templates

B.1 Priority Register

ID	Service	Gap	Consequence	Priority	Owner	Due	Evidence	Retest	Status

B.2 Evidence Register

Outcome ID	Evidence Source	Date	Owner	Confidence	Result / Limitation

B.3 Resilience Champion Monthly Cadence

- Review open high-priority actions and exceptions.
- Confirm identity/access changes and privileged account issues.
- Review new critical vulnerabilities and external exposures.
- Confirm backup jobs and scheduled restoration tests.
- Review critical vendor or AI-use changes.
- Update incident contacts and escalation pathways.
- Capture lessons and prepare executive dashboard.

References and Source Basis

Source	Framework Use
NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023.	Used for lifecycle risk concepts, trustworthy AI characteristics, and GOVERN/MAP/MEASURE/MANAGE orientation.
AuditBoard / A-LIGN, Effective AI Governance: Confronting AI Risks with ISO 42001 Compliance.	Used for AI management-system concepts, implementation phases, risk assessment, policy development, operational implementation, and continuous improvement.
InfoSec Compliance Now 2025, Demystifying AI Audits: A Practical Guide to Compliance.	Used for practical AI audit, third-party AI risk, compliance, visibility, and auditability concepts.
NIST CSF 2.0, NIST Cybersecurity Framework 2.0	Establishing governance, defining target outcomes, implementing security practices, measuring performance, and continuously improving through community profiles and workforce management.

Appendix C — Evidence of Development and Adoption Readiness

For evidentiary use, this framework should be supported by contemporaneous records showing genuine development and implementation activity. The existence of a polished framework demonstrates a defined methodology; it does not by itself prove market adoption, historical implementation, or national impact. Bazz Global should preserve version history and collect objective implementation evidence as pilots occur.

- Version-controlled framework files showing dates and substantive revisions.
- Board/member approval or internal adoption memorandum for Bazz Global use.
- Pilot engagement scopes, statements of work, or letters of intent that expressly reference RADIUS.
- Completed Current/Target Profiles, sprint plans, evidence registers, and after-action reports from authorized pilots, appropriately redacted for filing.
- Resilience Champion training materials, attendance records, and competency checks.
- Independent expert review of the framework's technical design and applicability, with the expert identifying materials actually reviewed.
- De-identified before/after metrics and limitations from pilots; no unsupported causal claims.
- Evidence of external presentations, workshops, partner interest, citations, downloads, or organizational reuse where they actually occur.
- Sector playbooks and benchmark reports generated from consented, sufficiently aggregated data.