



# Resilient Systems

Decentralised Security for Smart Cities and Critical Infrastructure

ACCREDITATION ALIGNMENT

# NAAC Alignment Note

IQAC and Accreditation Teams

Prepared for institutional planning, program evaluation, and strategic conversations with ATRISI.

---

# NAAC Alignment – Resilient Systems

## *Decentralised Security & Infrastructure Intelligence*

### NAAC Criteria Mapping Table

NAAC Criterion	Key Focus Area	Program Alignment	Evidence Generated
Criterion 2	Teaching–Learning & Evaluation	Systems thinking, infrastructure mapping, applied resilience learning	Architecture templates, system maps, workshop artifacts
Criterion 3	Research, Innovations & Extension	Infrastructure intelligence, cyber-physical systems, predictive risk models	Research problem statements, resilience models, applied research frameworks
Criterion 6	Governance, Leadership & Management	Institutional resilience planning, IT/OT integration, risk governance	Policy drafts, resilience strategy inputs, governance frameworks
Criterion 7	Institutional Values & Best Practices	Responsible infrastructure management, safety, ethical AI usage	Risk awareness documentation, resilience best practices

---

## Detailed Mapping (Slide 2 Equivalent)

### Criterion 2: Teaching–Learning & Evaluation

- Introduction to **systems thinking in infrastructure**
- Applied learning through:
  - Smart city / campus case studies
  - OT + IT integration scenarios
- Shift from:
  - Conceptual cybersecurity → **applied resilience design**
- Hands-on outputs:
  - Infrastructure topology mapping
  - Security zone design
  - Risk identification models

Outcome:

Participants move from “learning security” → **designing resilient systems**

---

### Criterion 3: Research, Innovations & Extension

- Exploration of emerging domains:
  - Smart cities
  - Critical infrastructure
  - Cyber-physical systems
- AI-enabled research thinking:
  - Signal → Risk → Intelligence → Action
- Example research direction:
  - Vegetation risk intelligence using satellite imagery
  - Predictive outage modeling
- Focus on:
  - **Research** → **real-world impact**

Evidence Generated:

- Research blueprints
  - Problem statements for infrastructure resilience
  - Applied innovation frameworks
- 

### Criterion 6: Governance, Leadership & Management

- Institutional readiness for:
  - Cyber + OT integration
  - Smart infrastructure adoption
- Leadership-level awareness:
  - Risk governance
  - Distributed system accountability
- Development of:
  - Resilience policies
  - Incident response frameworks
  - Infrastructure governance models

Outcome:

Institutions move from reactive management → **proactive resilience governance**

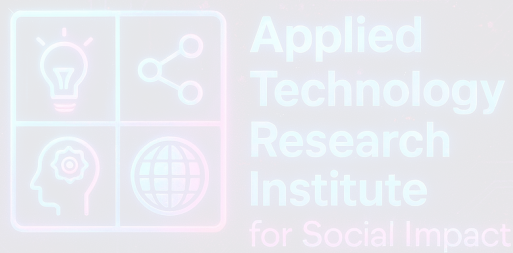
---

## Criterion 7: Institutional Values & Best Practices

- Responsible use of:
  - AI in infrastructure
  - Data from sensors, surveillance, and systems
- Awareness of:
  - Systemic risks (not just cyber threats)
  - Environmental + physical dependencies
- Establishing:
  - Resilience as a core institutional value
  - Best practices for infrastructure safety and continuity

Outcome:

Institutions adopt **resilience as a cultural and operational principle**



“This program contributes to institutional quality enhancement by enabling participants to design, govern, and implement resilient infrastructure systems aligned with NAAC criteria.”