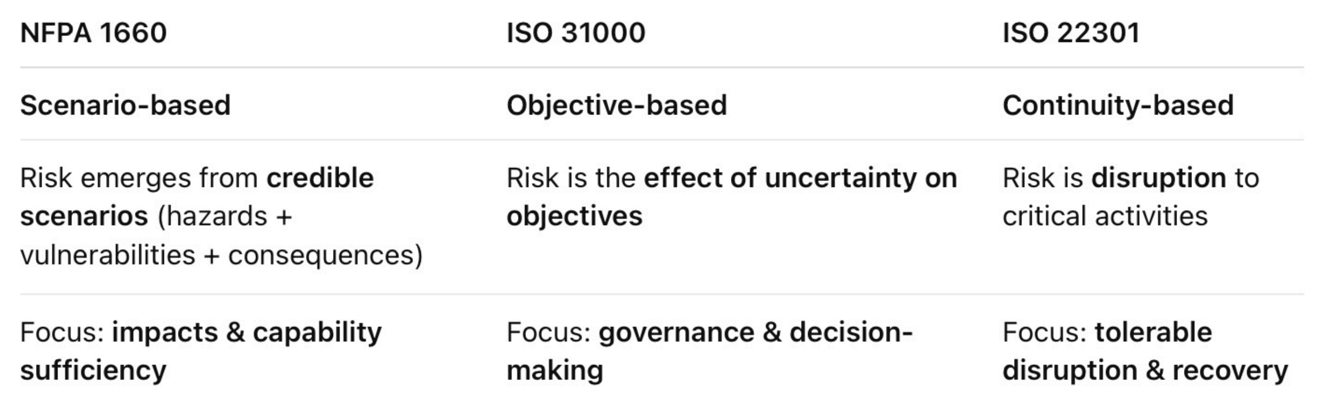
Integrated Gap Analysis Framework

This integrated Gap Analysis Framework cross-maps NFPA 1660, ISO 31000, and ISO 22301, extracts a common set of Key Elements, and then—critically—defines for each element:

- Necessary and sufficient Assessment Criteria (not checklists-for-the-sake-of-it)
- Evidence that should be sought to validate real capability (not paper compliance)



NFPA 1660	ISO 31000	ISO 22301
Scenario-based	**Objective-based**	**Continuity-based**
Risk emerges from **credible scenarios** (hazards + vulnerabilities + consequences)	Risk is the **effect of uncertainty on objectives**	Risk is **disruption** to critical activities
Focus: **impacts & capability sufficiency**	Focus: **governance & decision-making**	Focus: **tolerable disruption & recovery**

Integrated Gap Analysis Framework

(NFPA 1660 × ISO 31000 × ISO 22301)

1. Governance, Leadership & Accountability

Intent (All standards):

Risk, resilience, and continuity must be owned, not delegated to a document.

Assessment Criteria (Necessary & Sufficient)

1. Clear accountability for risk, emergency management, and continuity exists at executive level
2. Roles, responsibilities, and authorities are formally defined and understood
3. Governance mechanisms actively oversee performance and improvement

Evidence to Seek

- Board or executive charters explicitly referencing risk, resilience, BCM, or EM
- Named role holders with position descriptions (not just committee titles)
- Meeting minutes showing decisions, direction, and challenge—not just reports
- Evidence of escalation paths and authority during disruption

2. Context, Scope & Strategic Alignment

Intent:

Capabilities must be aligned to what actually matters to the organization and its environment.

Assessment Criteria

1. Internal and external context is explicitly defined and reviewed
2. Critical objectives, obligations, and value drivers are identified
3. Scope of risk, BCM, and emergency management is justified and bounded

Evidence to Seek

- Context analysis (PESTLE, ecosystem mapping, regulatory landscape)
- Statement of critical objectives and tolerance for disruption
- Documented scope rationale (what is included and excluded, and why)
- Alignment to organizational strategy or mission documents

3. Risk Identification & Hazard Profiling

Intent:

Organizations must understand what could happen before deciding what to do.

Assessment Criteria

1. Hazards and threats are systematically identified (all-hazards approach)
2. Vulnerabilities and exposure are explicitly considered
3. Risk identification is repeatable and reviewed periodically

Evidence to Seek

- Hazard registers or threat catalogues linked to context
- Documentation showing consideration of cascading and compound risks
- Inputs from multiple disciplines (operations, IT, supply chain, people)
- Review history showing updates based on change or experience

4. Risk Analysis, Evaluation & Prioritisation

Intent:

Decision-makers must be able to distinguish important from merely interesting risks.

Assessment Criteria

1. Likelihood and consequence criteria are defined and consistently applied
2. Risk evaluation reflects organizational risk appetite and tolerance
3. Prioritisation supports decision-making and resource allocation

Evidence to Seek

- Defined risk criteria (qualitative or quantitative, but coherent)
- Risk matrix or evaluation logic with documented assumptions
- Evidence of executive acceptance, treatment, or rejection of risks
- Traceability between risks and investment or mitigation decisions

5. Business Impact & Criticality Analysis

Intent:

Understanding impact over time is the bridge between risk and continuity.

Assessment Criteria

1. Critical activities, resources, and dependencies are identified
2. Impacts are analysed across time horizons
3. Recovery requirements are clearly defined and justified

Evidence to Seek

- Business Impact Analysis outputs (activities, impacts, MTPD, RTO/RPO)
- Dependency maps (people, premises, technology, suppliers)
- Evidence of validation with business owners
- Clear rationale for recovery objectives (not inherited defaults)

---

6. Strategy Selection & Treatment Design

Intent:

Responses must be intentional, proportionate, and achievable.

Assessment Criteria

1. Risk treatment and continuity strategies are selected deliberately
2. Strategies are feasible given resources and constraints
3. Trade-offs and residual risks are explicitly acknowledged

Evidence to Seek

- Strategy evaluation or option analysis documents
- Cost–benefit or impact trade-off discussions
- Documented acceptance of residual risk
- Linkage between strategies and identified risks/impacts

7. Plans, Procedures & Operational Capability

Intent:

Plans must work under stress—not just read well in audits.

Assessment Criteria

1. Plans are clear, usable, and role-based
2. Procedures support timely decision-making under uncertainty
3. Plans are accessible when needed

Evidence to Seek

- Crisis, emergency, and continuity plans with clear triggers
- Checklists, decision aids, and escalation protocols
- Evidence of accessibility during outages (offline copies, alternates)
- Feedback from users on clarity and usability

8. Communication, Coordination & Stakeholders

Intent:

Resilience is a networked capability.

Assessment Criteria

1. Internal and external stakeholders are identified and prioritised
2. Communication protocols are defined and tested
3. Coordination arrangements exist with partners and authorities

Evidence to Seek

- Stakeholder communication plans and contact lists
- Pre-scripted messages or communication frameworks
- MOUs, SLAs, or coordination agreements
- Evidence of joint exercises or coordination reviews

9. Training, Exercising & Competence

Intent:

Capability lives in people, not documents.

Assessment Criteria

1. Roles receive appropriate training for their responsibilities
2. Exercises test realistic scenarios and decision-making
3. Lessons learned are captured and acted upon

Evidence to Seek

- Training needs analysis and completion records
- Exercise designs aligned to risk and impact scenarios
- After-action reports with assigned actions
- Evidence of improvement following exercises

10. Monitoring, Review & Continuous Improvement

Intent:

Resilience must evolve as the organization and its risks change.

Assessment Criteria

1. Performance is monitored using defined indicators
2. Reviews are conducted following incidents, exercises, or change
3. Improvement actions are tracked to completion

Evidence to Seek

- KPIs or performance measures linked to objectives
- Management review records
- Change logs and corrective action tracking
- Evidence of program evolution over time

How to Use This as a Gap Analysis

For each Assessment Criterion, rate capability maturity:

- N - Absent – no evidence
- P - Ad hoc – informal or inconsistent
- L - Defined – documented but weakly applied
- F - Operational – consistently applied and tested

The gap is not “non-compliance with a clause”

The gap is the distance between current capability and capability required for your context.