

Executive Assessment:

SFIA 9 Risk Management [BURM] vs. Emerging Climate Risks

The **SFIA 9 Risk Management skill [BURM]** is defined as *"planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks"*. While the current skill framework covers traditional operational, cybersecurity, financial, and regulatory specialisms, expert industry analysis demonstrates that BURM contains critical structural blind spots regarding emerging IT and digital infrastructure risks driven by climate change.

Traditional BURM Scope vs. Emerging IT Climate Risk Reality

Current SFIA 9 BURM Focus	Emerging IT Climate Risk Realities
Static, historical risk baselines	Non-linear, escalating physical hazards
Facility-bounded operational risk	×11 Upstream supply chain & grid amplification
Scope 1/2 carbon compliance & cybersecurity	93–94% physical risk profile in AI-era compute
Mid-term operational risk management	Multi-decadal asset horizons (15–25+ years)

Key Structural Gaps in SFIA 9 BURM:

- 1. Static Historical Baselines vs. Escalating Physical Hazards:** BURM guidance focuses on routine risk classification and existing governance limits. However, global data centre assessments reveal that digital infrastructure built on historical weather baselines faces severe Value at Risk (MVAR) degradation. Over 8,800 data centres worldwide face escalating exposure to eight acute and chronic climate hazards (riverine/surface flooding, coastal inundation, extreme heat, tropical cyclones, forest fires, extreme wind, freeze-thaw, soil movement). Without forward-looking climate projections, standard IT risk management leaves assets exposed to un-insurability and stranded-asset repricing.
- 2. Inversion of Risk Profile in the AI Era:** Current IT risk practices focus heavily on carbon transition compliance (e.g. Scope 2 renewable procurement) and cybersecurity. Yet, research on AI-era infrastructure shows a complete inversion of risk: on legacy facilities, carbon represents 28% of Climate Value at Risk (ClimVaR) and physical channels 72%; on AI-era assets, physical channels account for 93–94% of enterprise risk, while carbon drops to just 6%. Standard sustainability and risk playbooks that focus on carbon accounting leave over 90% of AI-era compute risk unaddressed.

3. **Omission of Upstream Supply Chain & Interdependency Amplifiers:** BURM treats risk within defined functional or project boundaries. Industry analysis reveals an (x 11) supply chain risk multiplier: 98–99% of business interruption risk for data centres originates upstream in supply chains and shared utilities (power grid congestion, transformer failure, telecommunication cuts, water stress) rather than on-site. Australia’s National Climate Risk Assessment similarly emphasizes that critical infrastructure interdependencies (energy, transport, telecommunications) drive cascading regional failures.
4. **Front-End Design Window vs. Operational Retrofits:** SFIA 9 BURM focuses on managing operational controls and existing processes. However, 40–60% of 2035 global compute capacity will be built in the next five years, with asset horizons spanning 15–25 years for IT facilities and 50+ years for structures. Proactive, front-end climate-informed siting and structural adaptation restore 30–39% of exposed enterprise value at a positive net return, whereas retrofitting legacy facilities costs two to three times more.
5. **Regional Risk Dispersions (e.g. Australia/Oceania):** In Australia, 220 data centres face a projected +478% increase in damage risk by 2100. State-level risks vary drastically: Queensland carries 14.81% High Risk Properties by 2050 (driven by surface flooding), New South Wales (Sydney hub) faces a +347% increase in damage risk, and Victoria faces an +831% surge in damage risk due to coastal inundation. Current BURM skill descriptors lack the granularity to evaluate localized, site-specific physical hazard intensity.

Level-by-Level Assessment of SFIA 9 BURM Responsibilities

SFIA 9 BURM Level Descriptors & Climate Coverage Gaps

Responsibility Level	Current SFIA 9 BURM Descriptor Focus	Identified Climate Risk Deficit
Level 2 (Assist)	Routine data collection & reporting	Lacks physical hazard metrics & climate telemetry
Level 3 (Apply)	Maintains threat/vulnerability records	Omits RCP/SSP climate pathways & downscaled hazard data
Level 4 (Enable)	Medium complexity function/project risk	Ignores cooling stress, thermal limits & grid stress
Level 5 (Ensure/Adv)	Complex operational risk & governance	Misses ClimVaR modelling, siting & ×11 supply chain risk
Level 6 (Initiate)	Enterprise risk appetite & policy	Lacks systemic stress testing & insurance withdrawal
Level 7 (Set Strategy)	Vision, strategy & capital allocation	Ignores 15–25yr climate horizons & multi-trillion risk

- **Level 2 (Assist):**
 - *Current Definition:* Assists in collecting and reporting data to support risk management activities under routine supervision.
 - *Climate Gap:* Lacks requirements to record physical environmental stressors, temperature anomalies, localized flood exposure, or environmental site data.
- **Level 3 (Apply):**
 - *Current Definition:* Undertakes basic risk management activities; maintains documentation of risks, threats, vulnerabilities, and mitigation actions.
 - *Climate Gap:* Focuses on traditional threat registers. Fails to incorporate forward-looking climate projections (e.g. RCP 2.6 vs RCP 8.5 pathways), local hazard maps, or infrastructure design baselines.
- **Level 4 (Enable):**
 - *Current Definition:* Carries out risk management within a specific function, technical area, or project of medium complexity; assesses impact/probability and mitigation strategies.
 - *Climate Gap:* Evaluates risks within immediate project perimeters. Fails to account for ambient cooling degradation (where each +1°C ambient increase elevates cooling costs by 2–4%), component thermal derating, or local power grid vulnerabilities.
- **Level 5 (Ensure, advise):**
 - *Current Definition:* Plans and implements complex risk management activities within a technical area, project, or programme; establishes reporting mechanisms aligned with governance.
 - *Climate Gap:* Lacks requirements to model Enterprise Value at Risk (ClimVaR), evaluate front-end climate-informed site selection, or perform supply chain cross-dependency audits (x 11) business interruption multiplier).
- **Level 6 (Initiate, influence):**
 - *Current Definition:* Plans and manages organisation-wide risk management processes; aligns with business risk appetite and governance frameworks.

- *Climate Gap*: Ignores macro-level insurability risks (where insurance premiums are projected to triple or quadruple by 2050 with market withdrawals), systemic power grid failures, and cascading cross-sector disruptions across energy, transport, and telecommunication networks.
- **Level 7 (Set strategy, inspire, mobilise):**
 - *Current Definition*: Establishes organisation-wide risk management strategy and risk appetite in alignment with strategic objectives; allocates resources.
 - *Climate Gap*: Fails to mandate multi-decadal asset horizon risk governance (15–25+ years) or capital allocation strategies that prioritize proactive front-end adaptation to protect enterprise valuation across \$1.0–\$3.7 trillion global AI compute assets.

Research Reference Sources (containing some alarming numbers):

1. [The Economics of Climate Risk and Resilience for AI-Era Capital](#) [Schneider Electric June 2026]
2. [2025 Global Data Centre Physical Climate Risk and Adaptation Report](#) [XDI June 2026]
3. [Australia's National Climate Risk Assessment Report](#) [Australian Government Climate Service Sept 2025]