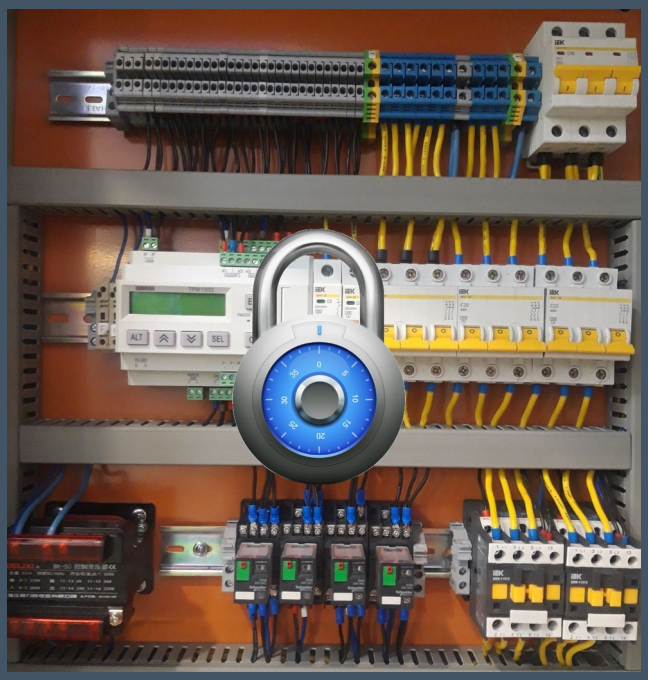
Theme 2

eApplication - Strategic GRC & ERM Framework Coexistence



Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Copyright © 2026 C²S Consulting

Licenced under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain



Table of Contents

1 Participant Team Scenario & Risk List....4
1.1 SCEL Enterprise Profile....4
1.2 Executive Profile & Mandate....5
1.3 Quantitative Threat & Asset Valuation List....5
1.4 Regulatory & Legal Exposure Landscape....6
1.5 OT Operational Realities & Threat Vectors....7
2 Problem Statement & Options....9
2.1 eAPP Ground Rules & Decision Constraints....9
2.2 Central Executive Prompt....9
2.3 Comparative Trade-Off Analysis Matrix....11
2.4 Common Participant Pitfalls & Misconceptions....12
2.5 Strategic Synthesis Statement....12

Theme 2: Strategic GRC, Enterprise Risk Management & Threat Quantification — TBL eApplication Exercise

1 Participant Team Scenario & Risk List

Solasra Clean Energy Limited (SCEL) is a multinational industrial conglomerate operating critical energy and manufacturing infrastructure. The corporation faces intense strategic friction: rapid business expansion and digital transformation have interconnected legacy SCADA networks and IACS with enterprise IT infrastructure. While this convergence optimises operational telemetry and corporate oversight, it exposes critical Programmable Logic Controllers (PLC), safety loops, and manufacturing lines to external cyber threats. Concurrently, SCEL operates across multiple international legal regimes, subjecting executive board members to strict statutory liability. SCEL's executive leadership must establish a comprehensive risk strategy without causing physical plant downtime or exceeding capital budgets.

1.1 SCEL Enterprise Profile

- **Corporate Footprint:** Dual operational facilities, manufacturing plants, and regional corporate hubs operating across the European Union (EU), United Kingdom (UK), United States (US), and India. Systems feature interconnected SCADA/IACS OT environments tied directly into centralised enterprise IT gateways.
- **Governance Mandate:** The board of directors has issued an explicit mandate to implement Enterprise Risk Management (ERM) frameworks across all international business units without reliance on an ISO 27001 Information Security Management System (ISMS) framework.

1.2 Executive Profile & Mandate

Company Profile

Entity: Solasra Clean Energy Limited (SCEL).

Headquarters & Footprint: Irish-headquartered multinational conglomerate operating across Ireland/EU, UK, US, and India.

Infrastructure: Interconnected SCADA networks, IACS, and central enterprise IT gateways.

Board Governance Mandate: Implement ERM frameworks across all international business units without reliance on an ISO 27001 Information Security Management System (ISMS) framework.

1.3 Quantitative Threat & Asset Valuation List

Quantitative financial metrics follow standard industry risk equations:

- Single Loss Expectancy (SLE) = Asset Value (AV) × Exposure Factor (EF)
- Annualised Loss Expectancy (ALE) = SLE × Annualised Rate of Occurrence (ARO)
- Net Cost-Benefit Analysis (CBA) = ALE_{pre} − ALE_{post} − Safeguard Cost

Table 1: Quantitative Threat & Asset Valuation List

Asset Description	AV	EF	SLE	ARO	ALE_{pre}	Safeguard Cost	ALE_{post}	CBA
SCADA Industrial Control Centre	€10,000	0.5	€5,000	0.2	€1,000	€150	€200	+€650
Customer PII DB	€5,000	0.4	€2,000	0.5	€1,000	€200	€300	+€500
Foreign Operations Gateway	€2,000	0.25	€500	1	€500	€100	€100	+€300

Note: Values expressed in thousands of Euros (€ '000).

1.4 Regulatory & Legal Exposure Landscape

Jurisdiction & Regulation	Core Statutory Requirements	Non-Compliance Risk & Penalties
EU GDPR (Regulation 2016/679) & UK Data Protection Act 2018 (UK GDPR)	Regulates personal data processing and cross-border transfers outside the EU/EEA and UK. Governs active workplace electronic monitoring; while employers may monitor employee e-mail to prevent harassment or security breaches, a written policy notifying employees is required to lift their reasonable expectation of privacy.	Severe administrative fines (up to €20M or 4% of global annual turnover) and regulatory enforcement actions by national Data Protection Authorities (DPA).
EU Audit Directive (Directive 2006/43/EC) & Market Abuse Regulation (Regulation 596/2014)	Audit Directive mandates statutory audit standards and corporate governance reporting for Public-Interest Entities (PIE). Market Abuse Regulation strictly prohibits insider trading, unlawful disclosure, and market manipulation.	Statutory sanctions, public censure, loss of public-interest entity auditing credentials, and direct corporate officer liability for reporting failures.
EU Directive (EU) 2026/1021 on Combatting Corruption & UK Bribery Act 2010	Directive (EU) 2026/1021 harmonises public and private bribery offences across EU Member States (including Ireland), establishing EU-wide standards for corruption prevention, integrity policies, and compliance risk assessments. UK Bribery Act 2010 establishes four criminal offences: bribing another person, bribing a foreign public official, failing to prevent bribery, and bribing to retain business advantages. Introduces strict liability for commercial organisations whose employees or associated persons engage in bribery.	Directive (EU) 2026/1021: Severe turnover-based administrative and criminal corporate fines up to 5% of total worldwide turnover or €40 million for bribery offences, alongside exclusion from public tenders, disqualification from business activities, and permit revocation. UK Bribery Act 2010: Unlimited corporate fines and criminal prosecution of executives by the Serious Fraud Office (SFO). Adequate anti-corruption procedures represent the sole statutory defence.

Jurisdiction & Regulation	Core Statutory Requirements	Non-Compliance Risk & Penalties
US Foreign Corrupt Practices Act (FCPA - 1977) & Sarbanes-Oxley Act (SOX - 2002)	FCPA prohibits corrupt payments to foreign officials and requires publicly traded companies to maintain accurate books, records, and adequate internal accounting controls. SOX mandates internal financial controls and audit standards enforced by SEC rulings.	Criminal prosecution by the DOJ/SEC, loss of securities registration, severe corporate fines, and executive imprisonment for accounting failures or foreign bribery.
US Regional & Sectoral Privacy (CCPA, VCDPA, HIPAA, GLBA, COPPA)	CCPA and VCDPA grant consumers rights to access, delete, and opt out of data sales. Sectoral laws mandate protection of health data (HIPAA), financial records (GLBA), credit data (FCRA), and children's online data (COPPA).	State Attorney General civil penalties, mandatory regulatory oversight, statutory damages per breach, and class-action litigation exposure.
Indian Digital Personal Data Protection (DPDP) Act 2023 & POCA 1988 / Companies Act 2013	DPDP Act establishes data processing rules enforced by the Data Protection Authority (DPA); specifically lacks a requirement for explicit consent under certain statutory provisions and exempts government agencies and small businesses. POCA 1988 criminalises bribery; Companies Act 2013 sets governance standards.	High monetary penalties imposed by the Indian DPA for data breaches; criminal prosecution under POCA for corrupt practices in foreign regional hubs.

1.5 OT Operational Realities & Threat Vectors

- **SCADA / IACS Vulnerabilities:** Industrial controllers, legacy PLCs, and SCADA control centres lack basic logical access controls, exposing physical machinery and safety loops to network-borne threats.
- **Phishing & Social Engineering:** Phishing attacks target plant operators and technicians to harvest credentials, enabling lateral movement from enterprise IT into OT control zones.
- **Ransomware & Malware:** Malicious code encrypts critical control systems and historian databases, causing catastrophic plant shutdowns, revenue loss, and physical safety hazards.
- **Denial of Service (DoS) & Network Exploits:** SYNchronise (SYN) floods and Smurf amplification overwhelm operational network gateways, while Man-in-the-Middle (MitM) traffic interception alters unencrypted SCADA control commands.

- **Cyber Terrorism & Reconnaissance:** Organised threat groups and foreign intelligence services conduct systematic server scans to map critical infrastructure vulnerabilities for potential physical sabotage.
- **Human Operator Error:** Configuration mistakes by plant engineers and technicians bypass perimeter firewalls, creating operational gaps that expose physical equipment to external networks.

Having established the quantitative threat List, legal risk landscape, and OT operational vectors, Participant teams must now evaluate the central executive forced-choice problem.

2 Problem Statement & Options

SCEL's Executive Risk Committee has authorised capital allocation for immediate risk treatment. However, severe budget limitations prevent the simultaneous execution of enterprise-wide technical safeguard deployments, comprehensive ERM framework implementations, and complete multi-jurisdictional legal remediations. The board demands a single, prioritised strategy for the next 12 months.

2.1 eAPP Ground Rules & Decision Constraints

1. **Mandatory Single-Option Choice:** Teams MUST select exactly ONE strategic option (Option A, B, C, or D).
2. **No Hybrid Strategies:** Compromise or hybrid proposals (e.g., allocating 50% of capital to Option A and 50% to Option D) are strictly prohibited and will be rejected by the facilitator.
3. **Defend Your Trade-offs:** Selecting an option requires accepting and defending its inherent operational, financial, and legal vulnerabilities during inter-team cross-debate.

2.2 Central Executive Prompt

As SCEL's Chief Risk Officer and Strategic Governance, Risk, and Compliance (GRC) Board, which single comprehensive risk treatment strategy must be prioritised immediately to optimise capital allocation, ensure legal survival, and protect critical OT infrastructure over the next 12 months?

Strategic Options

Option A: Quantitatively Driven Safeguard Deployment

- **Rationale**: Allocates primary capital directly to high-Net CBA technical safeguards. Prioritises SCADA Industrial Control Centre (+€650k Net CBA) and Customer PII Database (+€500k Net CBA) to capture €1.15M net risk reduction. Defers framework overhauls.
- **Vulnerability**: Starves the Foreign Operations Gateway (ARO = 1.00 / 100% annual breach probability). Leaves SCEL completely exposed to strict legal liability under EU Directive 2026/1021, UK Bribery Act 2010, US FCPA, and GDPR workplace monitoring rules.

Option B: Enterprise Risk Governance & ISO 31000 Alignment

- **Rationale**: Standardises the global enterprise around ISO 31000:2018 guidelines across 7 key phases (Scope/Context ➔ Risk Identification ➔ Analysis ➔ Evaluation ➔ Treatment ➔ Review ➔ Reporting). Establishes dynamic Risk Appetite Statements and formal treatment protocols (Transfer, Avoid, Mitigate, Accept).
- **Vulnerability**: ISO 31000 is a high-level process framework providing zero technical baseline controls or OT firewall specifications. PLCs, SCADA networks, and safety loops remain exposed to malware and DoS attacks during governance rollout. Lacks statutory task execution steps for EU/UK anti-corruption or US FCPA/SOX.

Option C: NIST RMF & Operational Control Lifecycle

- **Rationale**: Executes the 7-step NIST Risk Management Framework lifecycle (Prepare ➔ Categorise ➔ Select ➔ Implement ➔ Assess ➔ Authorise ➔ Monitor) using NIST SP 800-53r5 controls for system-level IT/OT security. Ensures deep technical impact categorisation and formal System Authorisation.
- **Vulnerability**: Highly documentation-intensive. Preliminary administrative phases (Steps 1–3) delay physical control installation (Step 4), leaving physical plants vulnerable to active cyber threats. Does not address international anti-corruption mandates (EU Directive 2026/1021, UK Bribery Act 2010, Indian POCA 1988) or labour privacy notifications.

Option D: Legal Compliance & Anti-Corruption Primacy

- **Rationale**: Directs all immediate funding to eliminate criminal corporate liability and personal executive prosecution under EU Directive 2026/1021 (preventing fines up to 5% global turnover or €40M), UK Bribery Act 2010 (adequate procedures defence), US FCPA/SOX, and global privacy laws. Institutes formal written workplace monitoring policies.
- **Vulnerability**: Starves OT engineering security of critical funding. SCADA control centres and PLCs remain unpatched and exposed to physical sabotage. Ignores high-ROI technical risk reductions (Net CBA) and lacks an operational risk identification process like ISO 31000.

Each option represents a distinct, defensible risk management philosophy. Teams must now evaluate the strategic trade-offs and structural vulnerabilities inherent in their selection.

2.2.1 Activity

- Choose one, and only one, option from A, B, C and D above.
- State your primary rationale for choosing this option and how your team plans to defend its structural vulnerabilities during inter-team cross-debate.

2.3 Comparative Trade-Off Analysis Matrix

Strategic Option	Financial ROI / CBA Impact	Regulatory Compliance Posture	OT Operational Resilience	Governance Overhead
Option A: Quantitative Deployment	Maximum Short-Term ROI: Captures + €1.15M net CBA across SCADA and PII assets.	Poor: Leaves strict liability anti-bribery laws and workplace privacy unaddressed.	Moderate: Hardens targeted physical systems; starves Foreign Gateway (ARO = 1.00).	Low: Minimal administrative framework documentation required.
Option B: ISO 31000 Alignment	Variable: Financial returns depend on long-term risk treatment decisions.	Moderate: Establishes organisational criteria; lacks specific statutory compliance execution.	Low-Moderate: Delays OT technical hardening during context setup and analysis.	High: Requires enterprise-wide alignment of risk appetite and criteria.
Option C: NIST RMF Lifecycle	Deferred: Upfront administrative and documentation costs delay financial ROI.	Moderate-High: Excellent technical control compliance; misses anti-corruption law.	Maximum Long-Term: Deep system categorisation, control assessment, and authorisation.	Very High: 7-step lifecycle demands continuous assessment and documentation.
Option D: Legal Primacy	Negative/ Unquantified: Ignores ALE mitigation metrics in favour of legal defence.	Maximum: Eliminates strict corporate liability and criminal executive exposure.	Critical Vulnerability: Physical SCADA networks and PLCs remain exposed to cyber attacks.	Moderate-High: Demands continuous legal auditing, compliance tracking, and policy maintenance.

Having fully evaluated the rationale, trade-offs, and compliance gaps for each option, Participant teams move to the inter-team cross-debate session.

2.4 Common Participant Pitfalls & Misconceptions

1. **Confusing EF with Likelihood (ARO):** Participants frequently confuse the percentage of asset loss (EF) with the annual frequency of threat occurrence (ARO).
2. **Misinterpreting the Foreign Operations Gateway Data:** Teams often overlook that the Foreign Operations Gateway has an ARO of 1.00 (100% annual probability of breach), mistakenly deprioritising it purely because its Net CBA (+ €300,000) is lower than other assets.
3. **Neglecting Strict Liability in Anti-Corruption Law:** Participants often treat legal compliance as a secondary checkbox, failing to recognise that under the Directive (EU) 2026/1021 and the UK Bribery Act 2010, strict corporate liability and severe turnover-scaled fines apply regardless of explicit executive knowledge or intent..
4. **Assuming Positive Net CBA Satisfies Legal Mandates:** Teams incorrectly assume that maximising financial CBA satisfies statutory obligations. A positive CBA does not shield an enterprise or its directors from regulatory fines or criminal prosecution.
5. **Confusing Risk Assessment with Ongoing Risk Management:** Participants often treat risk assessment as a single event rather than an iterative process across Phase 1 (Preliminary), Phase 2 (Critical Area Analysis), and Phase 3 (Organisation-Wide Assessment).
6. **Misunderstanding Privacy Bounds in Workplace Monitoring:** Participants overlook that under EU/UK GDPR, a written policy notifying employees of electronic monitoring is legally required to lift an employee's reasonable expectation of privacy, enabling lawful e-mail monitoring to prevent workplace harassment and security breaches.
7. **Misinterpreting Indian DPDP Act 2023 Provisions:** Participants incorrectly assume the Indian DPDP Act identical to EU GDPR, missing that the DPDP Act specifically lacks an explicit consent requirement under certain statutory provisions and exempts government agencies and small businesses.

2.5 Strategic Synthesis Statement

Effective GRC cannot be achieved through isolated technical spending, passive administrative policy creation, or legal compliance alone. True enterprise resilience requires the integration of quantitative threat modelling, structured governance frameworks, and strict legal compliance to protect critical OT infrastructure, ensure statutory survival, and optimise capital allocation.