

Mastering Business Continuity: ISO 22301 Strategies for Real-World Resilience

PECB Webinar
October 2025



THINK RISK

Introduction

- Experience of webinar hosts
- Webinar etiquette
- Key Learning Objectives
- Technical Material
- Start and Finish Times
- Questions

Introduction – *Michael Hannam*

- **Experienced senior leader across heavy industries for more than 35 years in Transport & Logistics, Mining (gold, diamonds, coal, bauxite, and iron ore), Oil & Gas, Marine, and manufacturing environments (EPC/M).**
 - The majority of his career has been in production and operational roles transforming and developing teams and leading HSSEQ at a senior level globally.
- **Remote geographical and regional responsibilities have included locations throughout Australia, Southeast Asia, China, Europe, the GCC, Southern Africa , New Zealand and North and South America.**
 - Mick has supported businesses by establishing comprehensive Training and Health, Safety, Security, Environment and Quality (HSSEQ) programs while ensuring crisis management and business continuity are intrinsically adopted into day-to-day operations.
- **Held senior executive roles with:**
 - Yinson Production – Global Head of Safety, Major Projects
 - Milaha Shipping and Logistics – Executive Manager – Corporate HSSEQ
 - Otraco International – Head of HSEQ, Global Operations and CEO of the Registered Training Organisation (RT051112)
 - Bridgestone Mining Solutions Australia – International Zero Harm Leader
 - HSSEQ General Manager (Asia Pacific) – Actuant Energy
 - National HSSEQ and Business Services Leader – TAMS Group
 - Health and Safety Manager – Contractor Safety – Rio Tinto Iron Ore - Pilbara Operations
 - Mining Superintendent – AngloCoal, Callide Coalfields.



Introduction – Mathew Jones

- **Chief Operation Officer, Think Risk International (2022 – Present)**
 - Oversee the offshoring team, and providing emergency response arrangements globally for Think Risk International
 - Managed the Audit and Compliance Department
 - Managed the Open-Source Intelligence Capability.
- **Head of Security and Emergency Response, Yinson Production (2023 – Present)**
 - Oversee security and emergency response initiatives for Yinson Production globally
 - Oversee all Medical Evacuation planning and execution globally.
- **Director of Audit and Compliance, Lockforce Consultancy (2008 – 2022)**
 - Led Audit and Compliance Department and developed systems and processes for business compliance
 - Managed the Open-Source Intelligence Capability.
- **Private Security (2004 – 2008)**
 - Team Leader for a Personal Security Detail (PSD) in Iraq
 - Regional Security Manager for Basra, leading a team of 45 personnel to secure election materials for the Iraq elections
 - Conducted anti-piracy operations in the Gulf of Aden.
- **Full-Time SAS (1993 – 2004) & SAS Reserves (2004 – 2006)**
 - Conducted combat operations in East Timor, Solomon Islands, Afghanistan, and Iraq
 - Conducted domestic counter-terrorism operations.
- **Qualifications**
 - *MSc in Business Continuity, Security & Emergency Management*
 - *Postgraduate in Security and Risk Management*
 - *Adv. Dip in Project Management*
 - *Adv. Dip Occupational Health and Safety*
 - *Certified Lead Auditor in Quality Management System*
 - *Certified Lead Auditor in OHS Management Systems*
 - *Lead Auditor in ISO 45001, ISO 28000, ISO 22301, ISO 27001, ISO 14001, ISO 9001*



Webinar Etiquette

-  Please ensure your microphones and webcams are off.
-  Feel free to ask questions in the chat as we go through the presentation.
-  You will also have **15 minutes** at the end for open Q&A.
-  The Slide Deck and Presentation will be shared with all confirmed participants after the webinar.
-  Mat and Mick will be available after the session to answer any additional questions – their contact details will be shared at the end of the presentation.

Key Learning Objectives

By the end of this webinar, you will:

- Understand the principles of **Business Continuity** and its importance to organisational resilience
- Gain practical knowledge of how to conduct a **Business Impact Assessment (BIA)** to identify critical activities and dependencies
- Learn the structured process for **developing a Business Continuity Plan (BCP)** that reflects real operational needs
- Understand how to **test, validate, and maintain** the continuity plan through ongoing exercises and updates.



Agenda

1. **What is Business Continuity and why do we need it?**
2. **Introduction to Business Impact Assessments (BIA) and Business Continuity Plans (BCP)**
3. **Phase 1: BIA Development**
 - Define the scope and objectives of the BIA
 - Identify Critical Activities and Dependencies
 - Assess Impact and Recovery Requirements
 - Prioritise Activities for Recovery
 - Validate and Maintain information in the BIA
4. **Phase 2: Writing the BCP**
 - Define BCP Objectives & Scope
 - Develop Response and Recovery Strategies
 - Document the Plan Structure and Content
 - Review, Validate and Approve the Plan
5. **Phase 3: Testing & Maintenance of the BCP**
 - Test & Exercise the BCP
 - Maintain & Improve the BCP
6. **Questions & Answers**
7. **Feedback Form**

What is Business Continuity?

Business Continuity is fundamentally about keeping essential business operations running during and after a disruption whether it's a cyberattack, natural disaster, power outage, or supply chain breakdown. It focuses on:

- Identifying critical functions that must be maintained or restored quickly to minimise financial, legal, and reputational impact
- Minimising downtime by preparing contingencies and workarounds
- Maintaining trust with customers, regulators, and stakeholders by ensuring service delivery even in adverse conditions.



Example: A bank experiencing a system outage must still ensure customers can access their funds or make transactions through alternative means (e.g., call centers or branch services).

What is Business Continuity? *(cont.)*

These ISO standards will provide you with a framework to work with and put processes in place.

- ISO 22301 – Business continuity management systems
- ISO 22313 – Societal security – Business continuity management systems – Guidance
- ISO 22317 – Business continuity management systems – Guidelines for business impact analysis (BIA)
- ISO 22320:2011 – Societal Security – Emergency Management – Requirements for Incident Response
- ISO/PAS 22399:2007 – Societal Security – Guideline for Incident Preparedness and Operational Continuity Management
- ISO 22316 – Societal Security – Organisational Resilience – Principles and Guidelines
- ISO/TS 22331:2018-Security and resilience – Business continuity management systems – Guidelines for business continuity strategy, and
- ISO 22398 – Societal Security – Guidelines for Exercises.

Why Do We Need a BCP?

- **Minimise Downtime:** A BCP helps ensure that essential business functions can continue during and after a disruption, reducing the time it takes to return to normal operations
- **Protect Assets:** By having a plan in place, companies can safeguard their physical and digital assets, including data, equipment, and facilities
- **Maintain Customer Trust:** Consistent service delivery, even during crises, helps maintain customer confidence and loyalty
- **Compliance and Legal Requirements:** Many industries have regulations that require businesses to have a BCP. Compliance with these regulations can prevent legal issues and fines.



Why Do We Need a BCP? (cont.)

- **Financial Stability:** A well-executed BCP can mitigate financial losses by ensuring that revenue-generating activities continue and by reducing the costs associated with downtime and recovery
- **Employee Safety and Morale:** A BCP includes measures to protect employees during emergencies, which can boost morale and ensure their well-being
- **Reputation Management:** Effective continuity planning can enhance a company's reputation by demonstrating resilience and preparedness
- **Competitive Advantage:** Companies with robust BCPs are often better positioned to recover quickly from disruptions, giving them an edge over competitors who may struggle to respond effectively.

In essence, a BCP is vital for ensuring that a company can withstand and recover from unexpected events, thereby securing its long-term success and stability.

Definitions and Terms

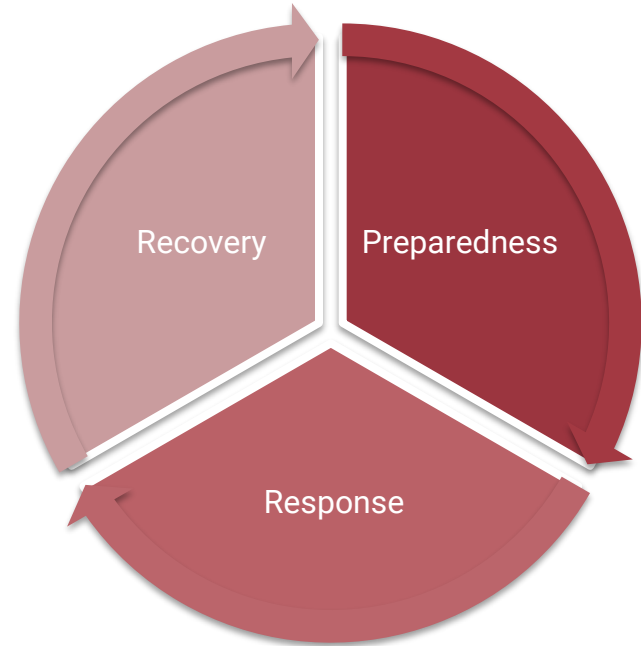
- **Business Continuity Management (BCM)** – A holistic management process that identifies potential threats to an organisation and the impacts to business operations. It provides a framework for building organisational resilience and the capability for an effective response. *(Source: ISO 22301:2019)*
- **Business Continuity Plan (BCP)** – Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following a disruption. *(Source: ISO 22301:2019)*
- **Business Impact Analysis (BIA)** – The process of analysing the effect of a disruption on business functions, including the determination of time-critical activities and the resources required for continuity and recovery. *(Source: ISO/TS 22317:2021 – Guidelines for Business Impact Analysis)*

Preparedness, Response, and Recovery

Business Continuity isn't just about reacting to crises; it is about building proactive capacity across the organisation.

- **Preparedness**
 - Training staff on roles and responsibilities
 - Documenting business continuity plans
 - Conducting Business Impact Analyses and risk assessments
 - Running simulations and tabletop exercises.
- **Response**
 - Immediate actions taken to contain or manage an incident
 - Activation of BCPs, communication protocols, and emergency roles.
- **Recovery**
 - Gradual restoration of operations to pre-defined levels (RTO - Recovery Time Objectives and RPO - Recovery Point Objectives)
 - Reviewing and learning from the event to strengthen future response.

This cycle ensures an organisation can respond quickly, effectively, and recover strategically.



What Business Continuity *Is Not*



✗ Just an IT Disaster Recovery (ITDR) Plan

- ITDR focuses narrowly on restoring technology systems, like servers, networks, or databases. It's a subset of BCM
- BCM covers the whole organisation, including HR, Finance, Operations, Legal, etc.

✗ A Crisis Management Plan (CMP)

- CMP guides how leaders make decisions and coordinate during a crisis
- It involves strategic oversight, resource coordination, and situational control
- CMP activates the BCP but is not the BCP.

✗ A Crisis Communication Plan (CCP)

- CCP defines how and what to communicate during a disruption—internally and externally
- It includes media handling, customer updates, and stakeholder messaging
- It supports both CMP and BCP but does not replace either.

ISO 22301 BCM Lifecycle

This diagram illustrates the core components of a Business Continuity Management System (BCMS) under ISO 22301. At the center is Leadership, Planning and Support, which drives the BCM process through commitment, resources, and oversight. Surrounding it are four key lifecycle stages:

1. **Business Impact Analysis & Risk Assessment** – Identify critical functions and assess how disruptions affect operations.
2. **Business Continuity Strategy** – Develop practical strategies to maintain or recover those critical functions.
3. **Business Continuity Procedures** – Document clear response and recovery steps in a usable continuity plan.
4. **Exercise and Test** – Regularly validate and improve the plan through testing and training.



How Do We Develop a BCP?

Three-Phase BCM Process

PHASE 1 BIA DEVELOPMENT

- Define BIA Objectives & Scope
- Identify Critical Activities & Dependencies
- Assess Impact and Recovery Requirements
- Prioritise Activities



PHASE 2 WRITING THE BCP

- Define BCP Objectives & Scope
- Develop Response and Recovery Strategies
- Document the Plan Structure and Content
- Review, Validate and Approve the Plan



PHASE 3 TESTING & MAINTENANCE

- Test & Exercise the BCP
- Maintain & Improve the BCP

Phase 1

Developing the BIA

- Defining the scope and objectives of the BIA
- Identify Critical Activities and Dependencies
- Assess Impact and Recovery Requirements
- Prioritise Activities for Recovery
- Validate and Maintain information in the BIA.

Step 1: Define Scope & Objectives

This step sets the foundation for the BIA by clearly defining what will be assessed, why it's being done, and who should be involved.

- Clarify the purpose of conducting the BIA (e.g., prioritise recovery planning, comply with ISO 22301)
- Define the scope: which departments, sites, or services are included
- Align with the organisation's strategic objectives and risk appetite
- Identify regulatory, customer, or contractual drivers for continuity
- Determine the timeframe and expected outputs of the assessment
- Assign ownership: nominate a BIA lead and sponsor
- Communicate purpose and expectations to all stakeholders involved.



Step 2: Identify Critical Processes

Map how each time-critical activity runs and what it relies on, so impact and recovery targets are realistic.

Dependency Register					
Activity name, owner, purpose, peak periods	People key roles, minimum staffing, single points of failure	Technology apps, data, interfaces, access needs	Facilities location, utilities, workspace / equipment	Third Parties suppliers, SLAs, alternates	Workaround manual steps, temp tools/docs
Order Processing	Order Fulfilment Team	ERP System	Main Warehouse	Shipping Provider	Manual orders in spreadsheet; local courier
Customer Support	Call Centre Staff	CRM Platform	Office Workstations	Telecom Service Provider	Redirect calls to mobile phones
Payroll	Payroll Officer	Payroll Software	Head Office	External Payroll Bureau	Manual calculation with spreadsheet

Step 3: Rate the Dependencies

Rating the dependency

Dependency Rating Table	
Level	Description
Low	Minimal reliance on this resource. Loss has little to no effect; work can continue with minor inconvenience.
Moderate	Some reliance; an outage causes delays or minor disruption, but workable alternatives exist.
High	Significant reliance; loss would cause major disruption. Only limited short-term workarounds are available.
Critical	Essential for continuous operation; loss would have immediate and severe consequences. No viable workaround exists.

Note: Use current state, not ideal state. Calibrate with process owners.

Step 4: Assess Impact & Set Recovery Targets

This step helps you understand how long your business can tolerate downtime and what recovery goals must be set to minimise damage.

- Evaluate impact over time (e.g., 0–4 hrs, 4–24 hrs, 1–3 days)
- Assess across impact categories: financial, legal, reputational, customer
- Assign impact severity ratings using a standard scale
- Determine Recovery Time Objective (RTO): acceptable downtime per activity
- Determine Recovery Point Objective (RPO): acceptable data loss tolerance
- Define Maximum Acceptable Outage (MAO), if applicable
- Justify ratings to support transparent decision-making.



Step 4: Assess Impact & Set Recovery Targets

(cont.)

Quantify consequences over time and set RTO/RPO/MAO so strategies match business tolerance.

- **Time buckets:** 0–4h, 4–24h, 1–3d, 3–7d (customise as needed)
- **Impact lenses:** financial, regulatory/legal, customer, operational, reputation
- **Score & justify:** use a consistent 1–4 scale with short rationale
- **Set targets:** RTO (downtime), RPO (data loss), MAO/MTD (outer limit)
- **Cross-check with dependencies:** high-rated dependencies often drive shorter RTOs.

Time				
Impact Over Time	0-4 Hours	4-24 Hours	1-3 Days	3-7 Days
Financial	1	1	2	3
Regulatory	1	2	2	4
Customer	1	2	3	4
Operational	1	2	4	4
Reputation	1	2	4	4

Step 5: Prioritise Activities

With impacts assessed, prioritisation ensures that the most critical operations are restored first during a disruption.

- Rank activities based on combined impact, urgency, and dependency ratings
- Use MAO, RTO, and dependency scores to build a recovery priority list
- Group activities into tiers (e.g., Immediate, <24h, <72h)
- Identify processes requiring immediate attention during a disruption
- Consider cross-functional interdependencies so sequencing makes sense
- Align with customer, regulatory, and strategic expectations
- Document prioritisation decisions and rationale to guide Phase 2: BCP Development.

Step 5: Prioritise Activities *(cont.)*

This example shows how to document a process, its dependencies, potential impacts over time, and when it becomes unacceptable to be offline (MAO). Use this format to keep your BIA data clear, consistent, and ready to inform your continuity plan.

Process	Dependencies		Impact Scenario	Impact Category	Impact of Disruption	Description of Impact	4H	24H	3D	7D	MAO	Critical System or Service (Yes / No)
	Internal	External										
Order Processing	Order Fulfilment Team	ERP Vendor	ERP system unavailable due to software failure	Operational / Customer / Financial	Orders cannot be processed, inventory not updated, shipments delayed	Backlog of orders, loss of customer trust, potential financial penalties	1	1	2	3	3D	Y
Customer Support	Call Centre Staff	Utility Provider	Power outage at main office	Operational / Customer / Reputational	Call center operations halted; no access to CRM or phone systems	Delayed responses to customer inquiries, reduced service levels, reputational harm	1	2	3	4	3D	N

Step 6: Validate & Maintain

The BIA must remain accurate over time. This step ensures that findings are reviewed, approved, and updated regularly.

- Review BIA findings with process owners and management
- Validate accuracy of Recovery Time Objectives (RTO) / Recovery Point Objectives (RPO) and dependencies
- Adjust for changes in business structure, systems, or risk landscape
- Formalise sign-off and store the approved BIA securely
- Integrate BIA results into BCP development
- Set a regular review cycle (e.g., annually or after major changes)
- Communicate updates to all relevant teams and departments.



Phase 2

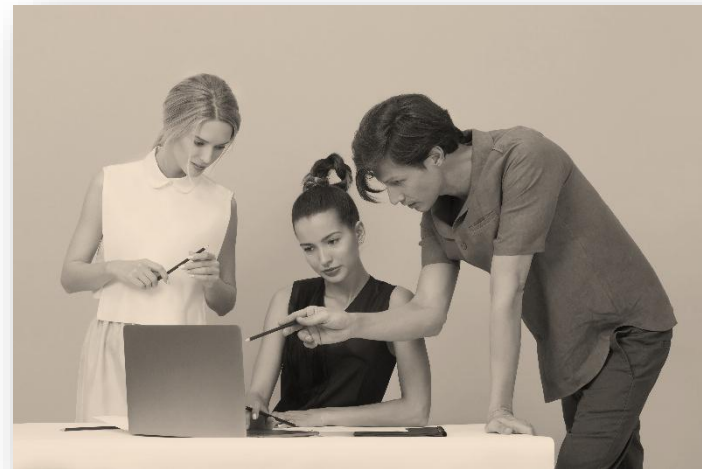
Establishing the BCP

- Defining BCP Objectives & Scope
- Develop Response and Recovery Strategies
- Document the Plan Structure and Content
- Review, Validate and Approve the Plan.

Step 1: Define BCP Objectives & Scope

The first step in BCP development is to clearly outline what the plan aims to achieve, who it covers, and under what circumstances it is activated.

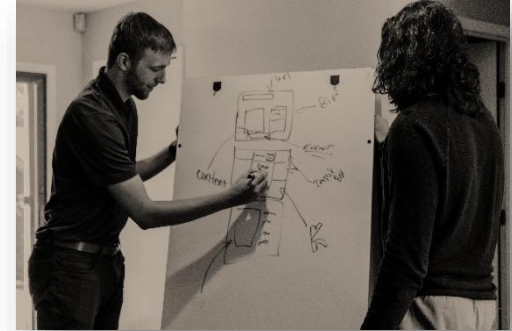
- Define the purpose: ensure continuity of essential operations during disruption
- Establish the scope: site-specific, department-specific, or enterprise-wide
- Identify the BCP owner and plan coordinators
- Clarify triggers for plan activation (e.g., IT outage, facility loss, staff unavailability)
- Determine applicable recovery timeframes (from BIA)
- Ensure alignment with the organisation's risk appetite and resilience strategy
- Coordinate with crisis and emergency management protocols.



Step 2: Develop Response & Recovery Strategies

This step focuses on selecting practical strategies that enable the organisation to maintain or quickly restore critical functions identified in the BIA.

- Define alternate methods to perform critical processes (manual workarounds, alternate suppliers)
- Identify backup facilities, remote work options, or relocation strategies
- Document procedures for partial or full loss of systems, staff, or infrastructure
- Align response strategies with recovery time objectives (RTOs) from the BIA
- Consider internal and external dependencies (e.g., IT, logistics, vendors)
- Integrate cybersecurity, safety, and regulatory requirements into strategies.



Step 3: Plan Structure & Content

The BCP should be well-organised, accessible, and easy to follow under pressure. This step focuses on assembling the plan components into a usable format.

- Create plan sections: introduction, activation criteria, roles & responsibilities, response actions, recovery steps
- Include contact lists (internal, external, emergency services)
- Insert Job Action Sheets or role-specific checklists
- Add communication protocols (internal announcements, stakeholder updates)
- Include resource lists (equipment, software, templates)
- Reference dependency and prioritisation data from the BIA
- Ensure formatting is clean and printable (digital and physical copies).



Step 4: Review & Approve the Plan

Once the BCP is drafted, it must be validated by relevant stakeholders to ensure it is accurate, realistic, and operationally sound.

- Conduct a walkthrough of the plan with process owners and BCP team
- Confirm alignment with BIA outputs and current operational practices
- Review contact details, location specifics, and supplier arrangements
- Identify any gaps, unrealistic timelines, or resource assumptions
- Secure executive approval and assign plan ownership
- Prepare the plan for distribution and training.



Phase 3

Testing & Maintenance of the BCP

- Testing & Exercising the BCP
- Maintaining & Improving the BCP.

Step 1: Testing & Exercising the BCP

Testing validates the practicality of your business continuity strategies and reveals gaps in procedures, communications, or awareness before a real incident occurs.

- **Tabletop Exercises:** Simulate disruptions through structured discussions; useful for validating procedures and decision-making
- **Walkthroughs:** Review the plan step-by-step with staff to check understanding and identify gaps
- **Simulation Drills:** Practice live response scenarios (e.g., power outage, cyberattack) to test recovery actions under pressure
- **Communication Cascade Tests:** Confirm accuracy of contact lists and escalation procedures
- **Test Timing:** Conduct at least annually or after major changes
- **Record & Review Outcomes:** Document lessons learned and improvement actions
- **Link Testing to Improvement:** Feed test results into plan updates and team training.

Step 2: Maintaining & Improving the BCP

A business continuity plan is only effective if it reflects current realities. Maintenance ensures the BCP remains aligned with your organisation's people, systems, and structure.

- **Schedule Regular Reviews:** At least annually or after significant organisational or operational changes
- **Assign Ownership:** Each plan should have a designated owner responsible for upkeep
- **Update Critical Information:**
 - Contact lists
 - Dependencies
 - Recovery strategies
 - System configurations.
- **Revisit RTOs and Dependencies:** Check they still reflect business priorities
- **Audit and Compliance Checks:** Ensure the plan meets internal and external requirements
- **Version Control:** Track changes, approvals, and distribution of updated plans
- **Reinforce Organisational Awareness:** Include continuity responsibilities in onboarding and refresher training.

Next Steps in your BCM Journey

From Awareness to Action: What Comes Next?

- Strengthen your Continuity Capabilities with ISO 22301
- Contact Think Risk International for further assistance in your own BCP – Mick@thinkrisk.com.au

Key Takeaways

✦ ***What You've Learned:***

- The purpose and structure of Business Continuity Management (BCM) aligned with ISO 22301
 - How to conduct a Business Impact Assessment (BIA) to identify critical functions, impacts, and dependencies
 - The steps to develop a practical Business Continuity Plan (BCP) using BIA outputs
 - The importance of testing, training, and maintaining your BCP for real-world readiness
 - How BCM strengthens resilience, trust, and operational reliability across your organisation.
- ✓ You now have a roadmap to start or improve your business continuity journey.

Why ISO 22301 Certification Matters

- ISO 22301 is the global standard for Business Continuity Management Systems (BCMS)
- Helps organisations prepare for, respond to, and recover from disruptions
- Adds credibility with customers, regulators, and partners
- Improves risk management, governance, and compliance posture
- Enables competitive advantage in procurement, audits, and strategic partnerships.

Certification demonstrates not just preparedness—but leadership in continuity and resilience.

How We Can Support Your ISO 22301 Journey

 **Professional Training.**  **Globally Recognised.**

- Accredited training on ISO 22301 at Foundation, Lead Implementer, and Lead Auditor levels
- Learn from certified experts with real-world BCM experience
- Flexible delivery: instructor-led, online, or hybrid
- Certification exams and internationally recognised credentials
- Tools, templates, and guidance to implement and audit BCMS effectively.

PECB-certified professionals are trusted worldwide for their continuity and risk expertise.

Next Steps

Turn Today's Learning into Certified Capability

- Explore PECB's ISO 22301 course catalogue at www.pecb.com
- Enroll in an upcoming ISO 22301 Foundation or Implementer course
- Contact Think Risk International at PECB@thinkrisk.com.au for training or corporate certification
- Use this webinar as a springboard to formalise your skills
- Consider aligning your team or organisation to international continuity standards.

The best time to prepare for disruption is before it happens, and with the right training, you can lead that change.



Questions?



- Any final questions about today's content?
- Need help deciding which PECB course is right for you?
- Want more resources on BCM, BIA, or ISO 22301?

Feedback Form

We'd love your feedback! Please scan the QR code to share your thoughts on today's webinar and the hosts—it'll help us improve future sessions.



Contact

- Website: www.thinkrisk.com
- Phone: +61 407 016 340
- Email: Mick@thinkrisk.com.au
and PECB@thinkrisk.com.au

PECB CONNECT

- events@pecb.com