

# Business Continuity & Risk Management

Gary Pennington

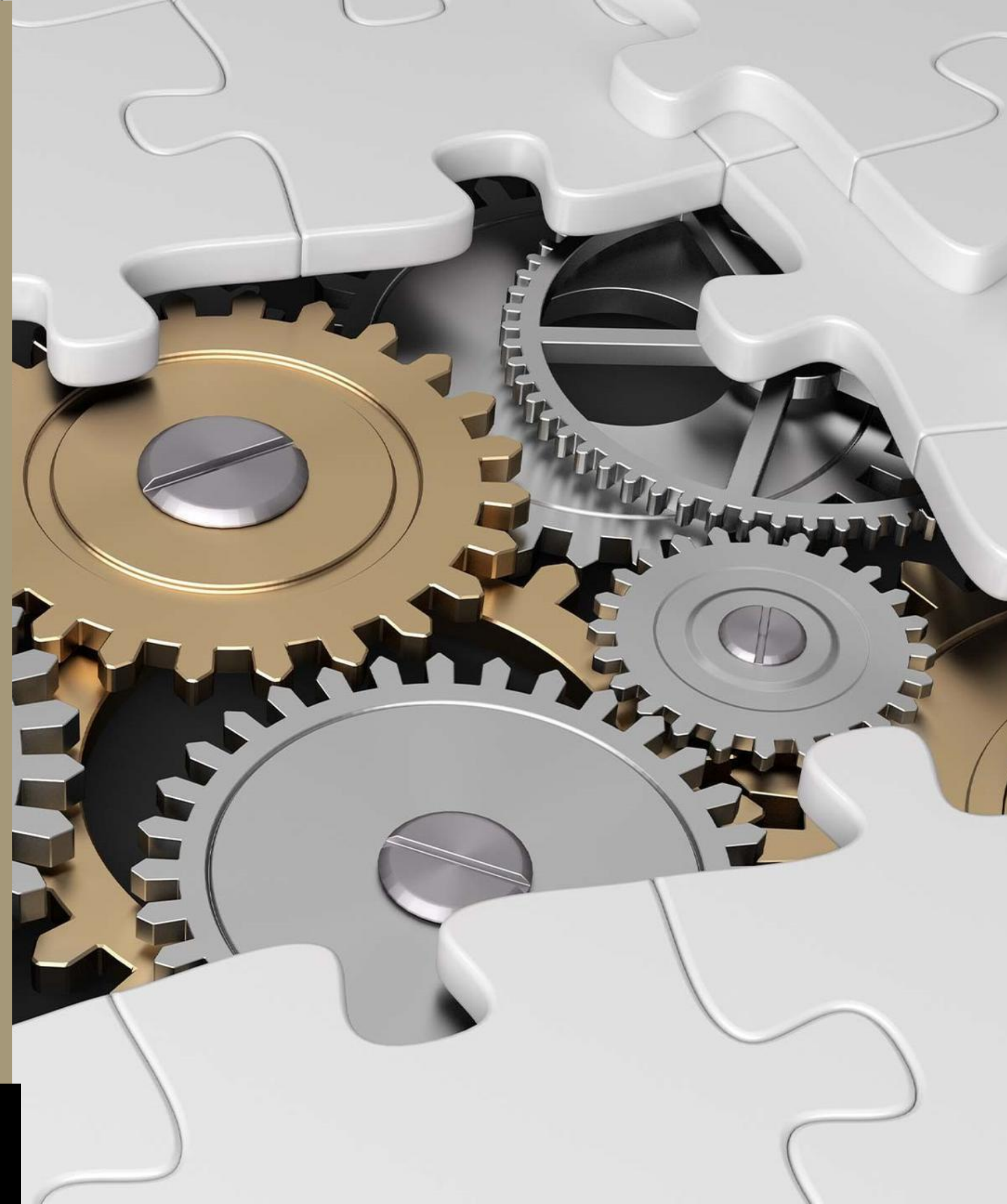


**ALCHEMI**  
ADVISORY GROUP

# DISCUSSION GUIDE

---

- Getting Started with Business Continuity
- Doing what's Important





40 Percent of businesses never  
reopen after a disaster.

25 Percent of the businesses that  
reopen will fail within one year.

*Based on 2018 FEMA study*



# Where Do You Start?

## **Identify what assets and resources are critical to deliver products and services to customers**

- Those components of your business you must have to do what you do including:
  - ✓ Facilities
  - ✓ Systems & Infrastructure
  - ✓ People
  - ✓ Critical Vendors
- Perform a Risk Assessment to identify where your risks lie
- Perform a Business Impact Analysis to identify what part of your business will be impacted in various scenarios.

# Developing a Plan

## **Identify Interdependencies**

- Internal systems and business functions
- Third Party Service Providers

## **Create a Plan to React to Interruptions in Critical Services**

- Be nimble and flexible to adjust to unforeseen events
- Identify who is responsible for critical areas
- Have a robust contact tree of internal and external parties
- Communicate, Train & Test
- Remediate based on lessons learned

# Create a Company Nerve Center

## **Issue Identification and Management**

- Single source of truth for issue resolution and ensuring resources are available where needed

## **A Business Continuity Plan that identifies critical assets**

- Identify what is critical to restore and how soon you need it back

## **Portfolio of actions across all work streams**

## **Leadership Alignment**

- Alignment of leaders on defining responsibilities, accountability and allocation of resources
- Roundtable exercise to identify any weak areas

# Protect Your Workforce

## 2-Way Outreach

- Multi Channel Communications
- Confidential feedback / reporting channels
- Escalation criteria / Call Trees

## Work from Home Support

- Infrastructure Setup and Support (e.g. VPN support, Virtual Conferencing Support, Broadband & Security Issues)

## Contractor Management

- Policy Alignment
- Contractor Safety
- Resource Availability for Outside Contractors
- Confidentiality Concerns

## Issue Management

- Issue Response Expectations
- Defined Owners and Available Resources

## On- Site Work Norms

- Social Distance Standards
- Preventative Measures
- Flexible Work Hours
- Health Checks

## Outside Stakeholder Engagement

- Availability of Information & Artifacts



# Engage With Customers

## Define Communication Channels

- Identify multiple trusted methods of communication to interact with customers.
- Use targeted communication where necessary to engage with specific impacted customer groups (e.g. Geographic specific, Customer specific (commercial vs residential, etc.)

## Customer Outreach

- Fact Based Reporting on issues as they arise
- Situational communications to educate & facilitate where necessary

# Stress Test Your Financials

## Liquidity Considerations

- Identify alternate arrangements if payment systems fail
- Identify emergency borrowing access
- Procedures to secure, deliver & distribute cash
- Emergency authorization procedures

## Financials Stress Testing

- Evaluate different scenarios and identify working capital requirements

# Verify Your Third-Party Providers Are Stable

## Supplier Engagement

- Supplier Validation “Trust but Verify”
- Security of Information
- Infrastructure Weaknesses
- Backups and Redundancies
- New Supplier Qualifications

## Logistics

- Logistics Capacity & Alternative Sourcing
- Logistics Capacity
- Import & Customs

# Final Thoughts

- Prepare a Risk Assessment & Identify Possible Threat Scenarios
- Prepare a plan that identifies critical assets and infrastructure to deliver services.
- Identify Responsible Internal and External Individuals
  - Maintain an Active Call Tree
- Perform a desktop exercise to identify shortfalls in the Business Continuity Plan