Entrepreneur & Family BUSINESS COUNCIL

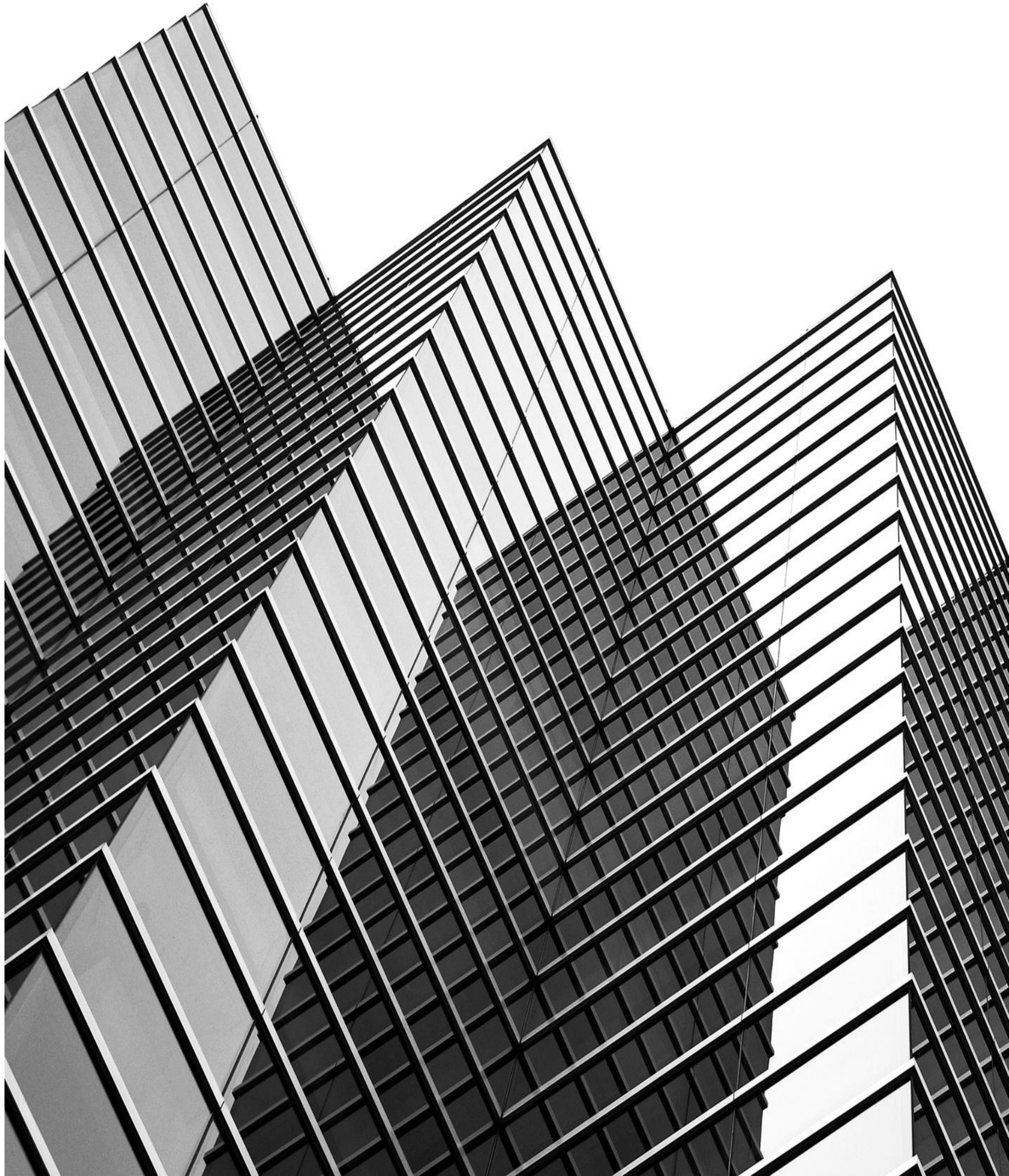
Module 7

# Legal and Regulatory Compliance

# Module 7: Legal and Regulatory Compliance

SUBTITLE

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus at lacus in purus laoreet bibendum. Integer vulputate, sapien sit amet interdum malesuada, mauris magna aliquet nulla, sed tempor erat tortor vitae sem.




**Jon Pisani**

**PSM Partners**

jpisani@psmpartners.com


# Presenter Intro

Jon Pisani is a Solution Architect at PSM Partners with close to Two (2) decades of cybersecurity experience. Jon focuses his efforts on helping organizations and business owners identify gaps within their infrastructure and design roadmaps to allow businesses to smoothly and efficiently upgrade.

# Understanding Cybersecurity Standards

| Standard / Framework | Primary Industries / Use Cases | IT Infrastructure Areas Impacted |
|---|---|---|
| **NIST Cybersecurity Framework (CSF)** | Broad — government contractors, critical infrastructure, and private sector seeking best practices | Network security, endpoint protection, identity management, incident response, continuous monitoring |
| **CMMC (Cybersecurity Maturity Model Certification)** | Broad — government contractors, critical infrastructure, and private sector seeking best practices | Access control, data protection, system security planning, auditing, incident response, endpoint management |
| **SOC 2 (System and Organization Controls)** | Common — SaaS providers, cloud service providers, financial and healthcare tech firms | Data storage, application security, access control, change management, monitoring and logging |
| **ISO/IEC 27001** | Common — Global standard across all industries — especially finance, healthcare, and tech | Risk management, information security policies, physical security, encryption, access management |
| **GDPR (General Data Protection Regulation)** | Common — Any organization handling EU citizen data | Data storage and retention, consent management, encryption, audit trails, access logs |
| **HIPAA (Health Insurance Portability and Accountability Act)** | Niche — Healthcare organizations, medical billing, insurance | Data storage, email systems, access control, backup/recovery systems, mobile device security |
| **PCI DSS (Payment Card Industry Data Security Standard)** | Niche — Retail, e-commerce, hospitality, financial services | Network segmentation, encryption, access control, firewall configuration, monitoring systems |
| **FedRAMP (Federal Risk and Authorization Management Program)** | Niche — Cloud service providers working with U.S. federal agencies | Cloud infrastructure, encryption, identity management, incident reporting, continuous monitoring |

# Policy Governance

- **Business Continuity** – Plan to keep operations running during disruptions.
- **Disaster Recovery** – Ensure systems and data can be restored after cyber or physical disasters.
- **Incident Response** – Pre-plan who does what in the event of a security incident. Speed matters. Perform a table-top exercise.
- **IT Security Policies** – Written rules for employees (e.g., password management, phishing awareness). Determine compliance framework if applicable.

# Building an Effective BCDR Plan

- **Know what matters most –** Identify the core business functions that must stay operational (e.g., payroll, customer communication, sales platforms).
- **Document “Plan B” processes –** Define how the company will continue serving customers if systems go offline or a facility is unavailable.
- **Test before you need it –** Conduct at least one tabletop or live recovery test per year. Small tests expose major gaps.
- **Don’t overlook people –** Ensure staff know their roles and who to contact in an emergency — plans are useless if only one person understands them.

# Building an Effective SIRP

- **Plan before the panic** – Define clear steps for detecting, containing, and recovering from security incidents (e.g., ransomware, data breach).
- **Assign roles and responsibilities** – Who investigates, who communicates with customers, and who makes the call to shut down systems?
- **Practice scenarios** – Regular exercises make teams faster and calmer during real events.
- **Focus on communication** – Have prepared messaging for employees, clients, and possibly the media.

# Building Effective IT Security Policies

- **Set clear expectations, not technical rules** – Policies like Acceptable Use, Data Retention, and Change Management help employees understand what's okay, what's risky, and how to protect company assets

- **Think of policies as "guardrails," not "roadblocks."** – They create consistency and accountability across the business, reducing mistakes and confusion.

- **Keep policies simple and enforceable** – One-page summaries or checklists are more likely to be read and followed than long legal documents.

- **Train and revisit annually** – A policy that sits in a drawer helps no one. Schedule refreshers and update them as technology and regulations change.

# Building Effective IT Security Policies

- **Prioritize what affects people the most:**
  - **Acceptable Use Policy (AUP)** – Defines how employees can use company devices, email, and internet safely.
  - **Data Retention Policy** – Ensures data is kept as long as legally or operationally required — and deleted when it’s no longer needed.
  - **Change Management Policy** – Helps IT and vendors make system updates without disrupting business operations or causing security gaps.

# Presenter Contact Info

**NAME NAME**
**COMPANY**
email@email.com

**NAME NAME**
**COMPANY**
email@email.com

**NAME NAME**
**COMPANY**
email@email.com

**NAME NAME**
**COMPANY**
email@email.com