TOP 5 Strategies CISOs Must Champion in CCM for Regulated Communications

Safeguarding Regulated Communications

Critical strategies every CISO should prioritize to stay compliant and customer-centric.

Insights from our CISO, Sasan Hamidi

STRATEGY 01

Governance Across the Communication Lifecycle

Start with Strong Governance

- Ensure governance from data intake to archiving
- Apply encryption, version control, and approval workflows
- Use audit trails for full traceability
- Align controls with business objectives

QUOTE:

"Security should be an enabler — not a bottleneck."

STRATEGY 02

Align Platforms with Regulatory Mandates

Technology Built for Compliance

- Design systems to meet CCPA, HIPAA, SOC 2, FINRA, etc.
- Enforce retention policies, customer consent, and access control
- Use agile platforms like **OSG JourneyConnect®**

KEY POINT:

Build to meet today's rules and adapt for tomorrow.

STRATEGY 03

Implement Role-Based Controls & Policy Enforcement

People & Permissions Matter

- Enforce role-based access control
- Regular permission audits
- Train teams on compliance and threat detection

OUTCOME:

Reduces risk of misuse and strengthens security culture.

STRATEGY 04

Multichannel Delivery with Centralized Oversight

Consistency Across All Channels

- Track and log every message sent
- Maintain traceability across email, print, SMS, and more
- Store delivery metadata for audit-readiness

REMINDER:

Multichannel ≠ Loss of Control

STRATEGY 05

Use Intelligence to Monitor Risk & Adapt

Proactive Risk Detection with AI

- Leverage real-time analytics from **OSG JourneyConnect Orion**
- Identify delivery issues and emerging compliance risks
- Turn insights into continuous improvements

RESULT:

Act before small issues become major problems.

CISO Takeaway

By championing these 5 strategies, CISOs can safeguard communications, stay compliant, and ensure trust in every communication touch-point.

osgconnect.com