Regulatory Risk Management
Compliance Controls Assessment Program

Steve Koslow

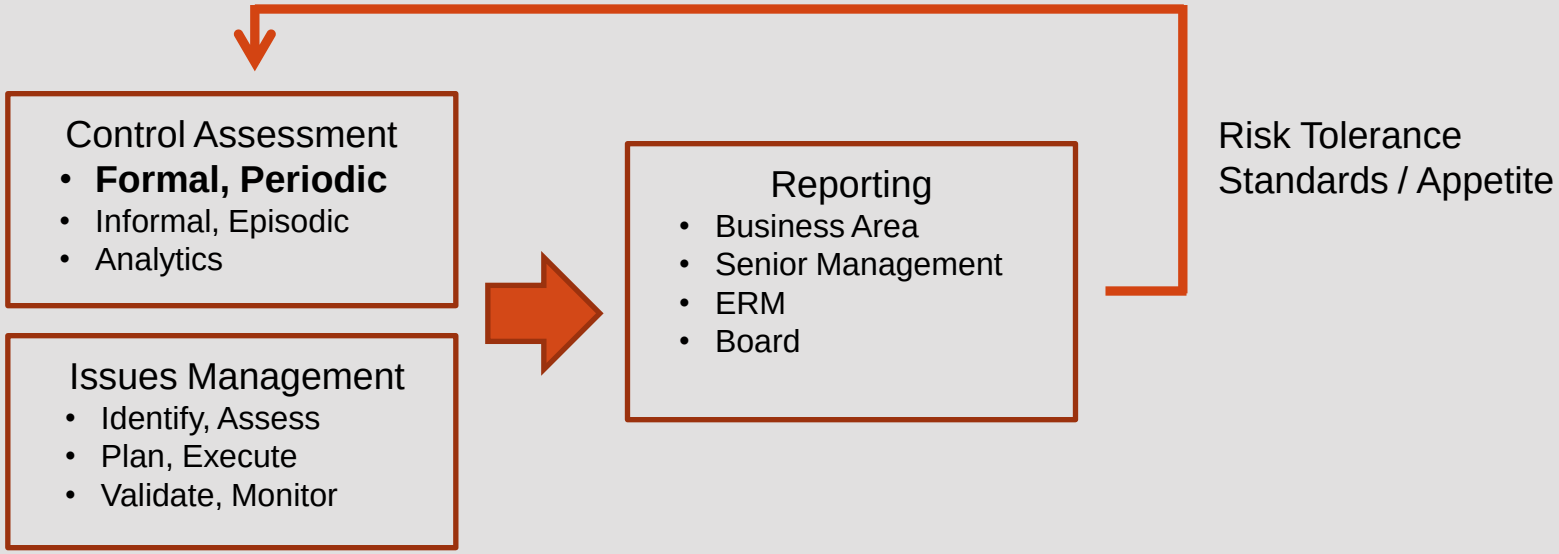
CUNA Mutual Group

SVP, Chief Ethics & Compliance Officer

Compliance Oversight Objectives

- To assess, monitor, and report on the design and execution of existing regulatory compliance controls.
- To ensure requirements of applicable model regulations, state and federal standards, regulatory examinations, or company-specific standards are met.
- To support and validate the remediation of compliance issues due to materialized risks.
- To help ensure business operations and core functions design and execute controls that align with risk tolerance levels.
- To report on the extent to which our controls manage our risk to expected risk tolerance levels.

Compliance Oversight – General Framework



Compliance oversight is composed of two integrated components that identify, assess, and manage compliance risk to meet the organization's risk appetite expectations.

1) **Compliance Controls Assessment** – Periodic and proactive assessment of whether compliance-related controls are reasonably designed and effectively executed.
2) **Issues Management** – On-going process to manage remediation of materialized compliance risks.

Formal, Periodic Control Assessment

Methodology:

- Determine the regulatory standard and core risk based on regulations, examination findings, articulated regulatory intent, and internal standards. (Inherent Risk)
- Analyze, test, and document the business or functional area's design and execution of compliance controls to manage identified risks. (Residual Risk)
- Identify and rate control deficiencies that may benefit from modification or enhancement. (Risk Rating)
- Where risk tolerance is in question, escalate to appropriate leaders for business decision to remediate or accept. (Risk Tolerance)
- Assist in the development of management action plans to enhance controls and/or ensure transparency in the acceptance of modified risk tolerance levels. (Mitigation)

Controls Assessment Framework - Example

Product / Service Function

Regulatory Framework
e.g. NAIC

Category /Sub-Category

ASSESSMENT SCOPE Risk Universe* (NAIC Model Regulations)	
General Management	**Sales**
Privacy	Licensing Appointments
Records Mgmt	Licensing Terminations
Disaster Recovery	Compensation
New Law Review	Producer Oversight
Vendor Mgmt	Suitability/Replacements
Claims	**Marketing**
Claims Handling Practices	Advertising
Settlement Practices	E-commerce
Anti-Fraud	Do Not Contact
Subrogation	
Underwriting / Rating	**Policyholder Servicing**
Rating Practices	Anti-Fraud
Filed Forms/Endorsement	Billing/Collection
Underwriting	Premium Refunds
Declination/Termination	Implementation/Servicing
	Reinsurance
Regulatory Reporting	**Complaint Handling**
Source Identification	Response Handling
Data Collection & Accuracy	Data Trending
Reporting Mgmt	

- Assessed where applicable. Note that additional categories will be used for business areas subject to non-NAIC regulation (e.g. International).

Controls Assessment Tool

Regulatory Requirement → Risk → Questions

Source	Citation	Model Regulation or Standard Language	Core Risks	Control Assessment Question
NAIC	40 s 8 B (3)	**(B)** In addition to the practices prohibited in [insert reference to state law equivalent to the NAIC Unfair Trade Practices Act], the following acts and practices are prohibited: **(3)** Cold Lead Advertising. Making use directly or indirectly of any method of marketing that fails to disclose in a conspicuous manner that a purpose of the method of marketing is solicitation of insurance and that contact will be made by an insurance agent or insurance company.	1. Controls of outbound marketing practices do not adequately address regulatory standards for proper consumer contact.	What is the process that reasonably ensures that unsolicited communications with customers include proper disclosure?
NAIC	40 s 14 M	**(M)** An agent who makes contact with a consumer, as a result of acquiring that consumer's name from a lead-generating device, shall disclose that fact in the initial contact with the consumer. An agent or insurer may not use names produced from lead-generating devices that do not comply with the requirements of this regulation.		What process is in place to ensure business areas provide proper disclosure when contacting customers through outbound marketing channels?
TCPA	47 CFR 64.1200(a)(1) iii	No person or entity may: **(1)** Initiate any telephone call (other than a call made for emergency purposes or made with the prior express consent of the called party) using an automatic telephone dialing system or an artificial or prerecorded voice, **(iii)** To any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call.		What process is in place to ensure TPA's or vendors follow applicable policies and procedures for DNC?

Reporting Assessment Scoring - Illustration

				Inherent Risk				Residual Risk		
Control Category	Control Sub-Category	Expected Control	Exhibited Control	Likelihood Rating	x Severity Rating =	Risk Score	x Mitigation Factor =	Risk Score	Mitigated Risk Level
Marketing	Do Not Contact	1. Outbound Marketing Training 2. Marketing sales Scripts	1. Outbound Marketing Training 2. Marketing sales Scripts	2	3	6	0.25	1.5	Low
Marketing	Do Not Contact	1. Outbound Marketing Training 2. Approved disclosure statements	1. Outbound Marketing Training	3	5	15	0.5	7.5	Low
Marketing	Do Not Contact	1. Periodic review of business marketing practices 2. Periodic review of vendors/TPA's business practices	None	3	4	12	1	12	Moderate

4	Risk Control Category	Marketing	Risk Rating Level	Moderate

Assessed Standard, Risk, and Control: An assessed standard included Section 64.1200 (d)(5) of the Telephone Consumer Protection Act which specifies that, "in the absence of a specific request by the subscriber to the contrary, a residential subscriber's do-not-call request shall apply to the particular business entity making the call (or on whose behalf a call is made), and will not apply to affiliated entities unless the consumer reasonably would expect them to be included given the identification of the caller and the product being advertised". E&C reviewed the presence and design of controls to address the risk of improper consumer contact through outbound marketing practices. Controls and processes should reasonably ensure that Company subsidiaries and affiliates follow applicable DNC policies and procedures.

Current State: No process has been established to determine which affiliates, or their vendors, should base their consumer contacts upon the contact preference recognized and used by the Company. Additionally, no process is in place to identify which subsidiaries or affiliates may have a need for program support and training related to DNC or to determine compliance with company policy or federal regulations related to Do-Not-Contact.

Cause and Impact: Resources to review business marketing practices of affiliates and subsidiaries, or their vendors, across all possible business channels and operations for compliance with Do-Not-Contact regulations. Insufficient controls to monitor affiliate and subsidiary business practices for compliance with DNC regulations and company policy could result in an increase in complaints or fines ranging up to $500 per call violation.

Management Action Plan & Anticipated Completion Date:

Reporting Assessment Results - Illustration

- Aggregated residual risk status of control environment by NAIC Category for a business area with multiple product lines.

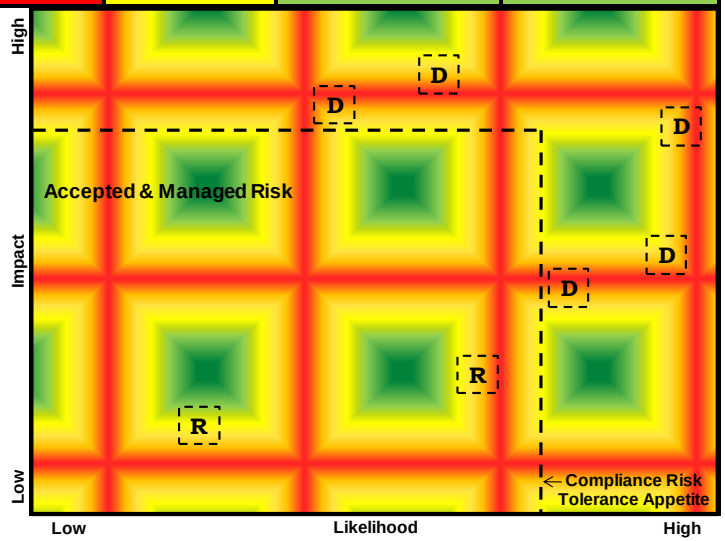
	Product Family							
	General Management	Underwriting and Rating	Claims	Marketing	Complaint Handling	Sales	Policyholder Servicing	Regulatory Reporting
Product A								
Product B								
Product C								

Three categories are used to rate and prioritize identified risks presented by the state of a control environment:

High – Risk controls are deficient and require remediation.

Moderate – Risk controls may be deficient and may require remediation or an acceptance of increased risk tolerance.

Low – Risk controls are adequate. However, the business may want to consider recommended improvements.



R = Recommendation; D = Deficiency

Thank You!