Compliance as a Catalyst for Reducing Risk

Dave Schmoeller, Director of Program Architecture and Product Solutions, Reciprocity
TODAY’S SPEAKER

Dave Schmoeller
Director of Program Architecture and Product Solutions, Reciprocity

1. Diverse auditing career spanning 25 years including 13 years as Chief Audit Executive
2. Enabling Reciprocity’s customers for 6+ years through Customer Success, Sales, Product Marketing, and Product Strategy
3. Resides in Perdido Key, FL and enjoys beach time with the family
AGENDA

● Challenges in the Marketplace Putting Risk into Business Context

● Simplifying the Journey to Risk by Leveraging Compliance

● Tools and Mindshift to Risk
THE PANDEMIC HIGHLIGHTED THE NECESSITY OF RISK MANAGEMENT

- Acceleration in digital strategy and transformation efforts (to survive)
- Exposed gaps and accepted risks in operational risk planning
- Demand for the ability to track and monitor risk is at an all-time high
CIO’S TOP THREE GRC PROGRAM CHALLENGES

- Limited resources/budget: 41.67%
- New or changing regulations: 18.75%
- Tracking and maintaining compliance: 14.58%
POLLING QUESTION #1

What is your biggest GRC challenge?
Now more than ever, companies depend on the trust of customers, partners and employees to stay competitive and achieve sustainable growth.
TRUST IS THE NEW HUMAN CURRENCY FOR DOING BUSINESS

DRIVES

Customer loyalty
62% buy trusted brand exclusively over competitors

COSTS

- A lack of trust costs global brands $2.5 trillion per year.
- Brands that broke customer trust due to scandals lost 20-56 percent of their market capitalization.

BUYING DECISIONS

81% of customers cite ‘brand trust and doing what is right as decisive factor for buying decisions.

Sources:
- Deloitte: HX in Uncertainty Survey, May 2020,
- Deloitte: The chemistry of trust Part 1: The future of trust
- Social Media Week, February 2018;
- Edelman Trust Barometer Special Report, June 2019
69% of companies across industries & geographies report an increase in threats to their business.

9% of boards are extremely confident that they are protecting their organization from cyber attacks.

Earning & keeping trust is a struggle.
INFORMATION SECURITY LEADERS MUST…

Stay compliant as regulations change

See, understand, act on risk

Communicate business impact

…to build a cyber risk program that enables the business
BUILDING A **ROADMAP** FOR IT SECURITY MANAGEMENT

- **Prioritized** risk leads to better compliance and more importantly, better security
- **Build** a strategic cyber risk roadmap to manage your InfoSec programs leveraging compliance frameworks
- Take a ‘**risk first**’ approach to transition from compliance to risk management.
STRATEGY DRIVES RISK AND COMPLIANCE

DEFINE
- GTM Strategy
- Risk Profile

INVEST
- People
- Tools

ACT
- Assess & Analyze
- Oversight
- Reporting
COMPLIANCE FIRST, LEADS TO RISK

INCEPTION POINT

Compliance frameworks hold all organizations to the same standards.

CYBER RISK PROGRAM

Leverage compliance activities to start thinking about cyber risks.

BE STRATEGIC

Companies need to do things differently to create a strategic roadmap for IT Security.
BUILD A BETTER INFOSEC PROGRAM

A Cyber risk platform provides **better visibility** into your organization’s risk posture

- Think differently about your business activity and how it incurs risk
- Understand and monitor the controls that mitigate those risks
- Enable continuous monitoring, better visibility, and actionable insights
- Share information seamlessly between risk and compliance
THINK SECURITY AND COVERAGE

Think Strategy not Tactics

- Don’t just check boxes, understand business strategy
- Get buy in at an executive level
- Have the right foundation to ensure success
CONTROLS AND RISK: TWO SIDES OF THE SAME COIN

Controls
- Helping Things Go Right
- Preventing Bad Things from Occurring
- Detecting When Things go Wrong

Risks
- What Can Go Wrong?
- Adverse Impacts to the Organization?
What is your primary role at your organization?
RISK PROGRAM OVERVIEW

Source: “Getting Started with Risk Management” (ISACA circa 2018)
IMPLEMENTING A RISK PROGRAM

● Planning  Vision, Risk structure and overall project plan
● Involvement For leaders and participants
● Analysis  Industry and organizationally focused risk identification
● Remediation Control Gap Identification and remediation strategies
● Preparedness Business Impact and Disaster Recovery development and testing
PLANNING

- Risk Goals and Structure
  - What to accomplish
  - Leverage Compliance

- Governance
  - Communication plans
  - Risk Committee

- Project Planning
  - Implementation
  - Future scalability
INVolVEMENT

- **Education**
  - Risk practices
  - Identification
  - Remediation and controls

- **Roles and Responsibilities**
  - Organizational/Departmental
  - Executives
  - Champions
IDENTIFICATION & ANALYSIS

● Risk Structure – Standardizing Risk Metrics
  ○ Risk target and calibration

● Risk Identification – Building the Registers
  ○ Leverage Compliance and Controls
  ○ Risks
  ○ Threats
  ○ Vulnerabilities
  ○ Incidents

● Risk, Vulnerability and Threat Ratings
  ○ Quantification & Evaluation
NOT QUICKLY IDENTIFYING RISKS COSTS MONEY

$9.0M
Average cost of a data breach in the US

$7.7M
Average cost of insider-related cyber breach for SMBs

287 days
Average time to identify and contain a breach

Source: IBM and Ponemon Institute's 2021 "Cost of Data Breach Report"
BETTER DECISIONS ON RISK

GAPS

- Residual Risk greater than Risk Appetite / Target
- Controls not in place or not operating effectively

PRINCIPLES

- Accept No Unnecessary Risk
- Make Risk Decisions at the Appropriate Level
- Weigh Benefits and Costs to Reduce Risks
- Anticipate and Manage Risk by Planning & Preparedness
PREPAREDNESS & RESPONSE

- Process and System Review
  - Disaster recovery
  - Crisis management
  - Breach notification documents
  - Vulnerability controls
- Simulations
- Share results
CONTINUITY PLANNING

- Past Performance May Not Reflect Future Events
- Communication Plan
- Physical and Remote Access Sites
- Everyone is a “Risk Steward”
INFOSEC BEST PRACTICES

- Implement Risk Accountability - risk is everyone’s responsibility
- Champion Risk from the Top
- Conduct Risk Assessments Timely
- Quantify and Prioritize Risks
- Implement Risk Treatments including Strong Controls
Be Prepared! Questions Boards will Definitely Ask

- How did this (incident) happen?
- Are we 100% secure?
- What happened at XYZ Company?
- Resource allocation?
  - Are we spending enough?
  - Why are we spending too much?
- What keeps you up at night?
What is your Board or Executive team’s biggest interest in IT risk and information security?
GRC TOOLS — WHEN TO USE

Challenges:
- Continuously changing risk landscape
- Complexity and redundancy
- Constrained resources
- Broadening stakeholder expectations driving Go-to-Market
- Reporting and monitoring on risk programs
- Tasks and repetition increase, and process & information becomes decentralized
BE MORE STRATEGIC WITH RISK IN BUSINESS CONTEXT

- Enable risk-guided, strategic business decisions
- Keep teams connected
- Know you are on the right track
- Give time back to the team
USE COMPLIANCE TO IMPROVE RISK MANAGEMENT

- Go beyond checking the box for compliance
- Deliver quick wins
- Start fast and stay smart
- Connect your teams
- Free your teams
CONNECTING COMPLIANCE AND CYBER RISK MANAGEMENT

Automatically map current compliance program data to the secure controls framework’s (SCF) catalogue of 32 cyber risks

Leverage expert-provided inherent and target residual risk scores as a starting baseline
MINDSHIFT TO THINK RISK FIRST

Every business activity involves risk, so prioritizing risk is critical

- The ability to view and measure risk at a holistic level is not enough
- Identifying and categorizing risks as they relate to a business activity is critical to understanding, quantifying and reducing those risks
RISK IS EVERYONE’S RESPONSIBILITY

Minimizing Risk Requires a Culture Change

● Compliance frameworks map industry or company security requirements into sets of actionable controls that can identify and mitigate associated risks

● Encourage ownership throughout the organization

● Metrics, KPIs, and Dashboards help promote transparency and accountability

● Communicate in context of your business goals
Visit reciprocity.com

- Sign-up for our GRC Weekly Digest email to keep up on events, news, reports and more
- Our Resource Center is available 24/7 with articles, guides, webinars and more, filtered to your industry or framework preferences
- Learn about Reciprocity® ROAR Platform and schedule a demo
QUESTIONS?
Sign-up for our GRC Weekly Digest email to keep up on events, news, reports and more

Our Resource Center is available 24/7 with articles, guides, webinars and more, filtered to your industry or framework preferences

Learn about Reciprocity® ROAR Platform and schedule a demo
THANK YOU