SQUIRE PATTON BOGGS

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

The Value of Regular Independent Compliance Assessments

The Continual Improvement Journey

April 27, 2022

Your Presenters

SQUIRE PATTON BOGGS

Corinne Hodges

CEO, Association of Women's Businesses

E chodges@awbc.org

Colin R. Jennings

Partner, Cleveland

E colin.Jennings@squirepb.com

Adele Navarrete

Senior Corporate Counsel, LMI

E anavarrete@lmi.org

Ericka A. Johnson

Senior Associate, Washington DC

E ericka.johnson@squirepb.com

SQUIRE PATTON BOGGS

AGENDA

- Recent Trends
- Applicable Government Guidelines
- Overview of Compliance Assessments
- Key Elements of Compliance Assessment
- Testing and Monitoring
- Practical Application: Cybersecurity Risks

SQUIRE PATTON BOGGS

Recent Trends

Robust M&A Market, Pandemic Environment, Heightened Focus on ESG, and Sanctions and Cybersecurity Risks from Russia-Ukraine Invasion

Robust Mergers and Acquisitions

SQUIRE PATTON BOGGS

- Trends for 2021/2022
  - Global M&A hit new highs in 2021
  - Deals exceeded 62,000 globally in 2021
  - Deals up an unprecedented 24% from 2020
- Fueled by:
  - Intense demand for technology
  - Digital and data-driven assets
  - Pent-up deal-making demand from 2020
- Most indications point to another supercharged year for 2022, despite some dampening as a result of factors such as the Russia-Ukraine conflict.

Associated Risks and Considerations During Mergers and Acquisitions

SQUIRE PATTON BOGGS

- There are risks associated with acquiring/merging with another organization.
- Organizations should consider, among others, the following:
  - Strength of acquired organization's compliance program
  - Existing gaps/risks of acquired organization
  - Overlap of jobs central to compliance
  - Gaps in jobs central to compliance
  - Existing gaps/risks of third party vendors of acquired company

Evolving Pandemic Environment

SQUIRE PATTON BOGGS

- Impact on compliance culture
- Transitions to remote or hybrid working arrangements, or back to office
- Adjustments to changing mandates related to Covid-19
  - Masks, vaccines, large groups or gatherings, etc.
  - Navigating CDC and local recommendations

Heightened Focus on Environmental, Social, and Governance (ESG)

SQUIRE PATTON BOGGS

- Increasingly, environmental disclosures are required and are beginning to impact compliance programs
  - EU disclosure requirements
  - US disclosure requirements coming
- Companies should be wary of “greenwashing” as well
  - Public scrutiny
  - Regulatory scrutiny

Sanctions and Cybersecurity Risks from Russia-Ukraine Invasion

SQUIRE PATTON BOGGS

- The Treasury Department's Office of Foreign Assets Control imposed additional sanctions on "key enablers of the invasion"
  - Sanctioned entities include Russian defense companies, members of the Russian State Duma, and head of Russia's largest financial institution.

- Biden-Harris Administration released statement warning of potential malicious cyber activity against US companies in response to economic sanctions imposed on Russia.
  - Companies are urged to execute security measures to protect data and for technology companies to bolster their products

Current Regulatory Landscape

SQUIRE PATTON BOGGS

- Regulation continues to be aggressive and far reaching
  - The DOJ has called for “law enforcement to be aggressive in pursuing corporate wrongdoers.”
  - Past enforcement actions demonstrate the DOJ takes a broad view over corporations with a US nexus to be within its jurisdiction.
- Investigations and audits have been lengthy and may have wide-ranging consequences
  - Investigations can take years, resulting in criminal fines, punitive damages, civil liability, suspension or debarment, and even loss of export privileges.
- Agencies are working together to conduct parallel investigations

SQUIRE PATTON BOGGS

Applicable Government Guidelines

Considerations for Benchmarking

Legal Framework

SQUIRE PATTON BOGGS

- **U.S. Sentencing Commission's Federal Sentencing Guidelines for Organizations (effective 1991)**
- U.S.S.G. § 8B2.1, Effective Compliance and Ethics Program
  - Main sentencing standard for organizations in the U.S.
- There are aggravating and mitigating factors that the DOJ can consider when pursuing an appropriate punishment (U.S.S.G. Ch. 8, intro. comment)
  - Aggravating factor: The organization's involvement in or tolerance of criminal activity
  - Mitigating factor: Whether the organization has an effective compliance and ethics program

Legal Framework

SQUIRE PATTON BOGGS

- **Principles of Federal Prosecution of Business Organizations in the Justice Manual of the DOJ (JM 9-28.000)**
  - Describes the factors that prosecutors should consider in determining whether to bring charges against an organization
  - These include, among others:
    - Pervasiveness of the wrongdoing, including the complicity of the organization (JM 9-28.500)
    - The corporation's history (JM 9-28.600)
    - The adequacy and effectiveness of the corporation's compliance program (JM 9-28.800)
    - An organization's voluntary disclosure (JM 9-28.900)
    - An organization's remedial actions (JM 9-28.1000)

Legal Framework

SQUIRE PATTON BOGGS

- **DOJ and SEC's Resource Guide to the U.S. Foreign Corrupt Practices Act** (updated 2020, guided by JM 9-28.000 and FCPA Corporate Enforcement Policy JM 9-47.000**)**
  - Addresses a wide range of topics related to proper corporate ethics and compliance
  - The Guide also articulates factors that the DOJ and SEC consider when deciding whether to open an investigation or bring charges
- **DOJ Criminal Division's Evaluation of Corporate Compliance Programs** (updated 2020, guided by U.S.S.G. §§ 8B2.1, 8C2 and JM 9-28.000)
  - The DOJ will consider three fundamental questions when examining an organization's compliance program:
    - Is the corporation's compliance program well designed?
    - Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?
    - Does the corporation's compliance program "work" in practice?

2020 Update to the DOJ Guidance

SQUIRE PATTON BOGGS

- In June 2020, the DOJ issued several changes to its guidance document “Evaluation of Corporate Compliance Programs.”
- The updated guidelines offer even more detail on how prosecutors will evaluate the effectiveness of corporate compliance programs.
- The 2020 changes to the Guidance emphasize that:
  - Having a compliance program in place is not enough. It has to work.
  - Compliance programs shouldn’t be “snapshots” but dynamic and updated to respond to new circumstances.
  - An “off the shelf” compliance program that merely exists on paper will not benefit a company that is under investigation.

Legal Framework

SQUIRE PATTON BOGGS

- **Treasury Department's Framework for OFAC Compliance Commitments (2019)**
  - OFAC strongly recommends the establishment of a sanctions compliance program when conducting business with foreign entities.
  - Such a program should consist of at least five basic components:
    - Management commitment
    - Risk assessment
    - Internal controls
    - Testing and auditing; and
    - Training
  - Annex to Appendix A to 31 C.F.R. Part 501, OFAC's Economic Sanctions Enforcement Guidelines provides an OFAC Risk Matrix used to evaluate compliance programs

Legal Framework:
Additional Guidance from Administrative Agencies

SQUIRE PATTON BOGGS

- Federal Acquisition Regulations ("FAR") (FAR 52.203-13 / 48 CFR 3.1002-3.1004)
  - Civilian Agency Acquisition and Defense Acquisition Regulation Councils finalized rules placing certain compliance program requirements on federal government contractors
- Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (2019, guided by JM 9-28.800 and DOJ's Guidance on Evaluation of Corporate Compliance Programs)
  - DOJ's Antitrust Division will now consider company's compliance program in determining whether to bring charges and how to seek to resolve alleged antitrust violations
- Federal Energy Regulatory Commission ("FERC") Policy Statement on Enforcement (Docket No. PL08-3-000, par. 57-60 (May 15, 2008))
  - FERC will consider compliance programs when determining remedies for violations of statutes, orders, rules and regulations that FERC administers

Potential Criminal and Civil Liability

SQUIRE PATTON BOGGS

- U.S.S.G. § 8C2 provides that measurement of organizational guilt may impact fines assessed, taking into account victim's loss and company's gain.
  - In 2019, the DOJ implemented a policy that allows prosecutors to adjust criminal fines that would produce a significant adverse collateral consequence that, while severe, may not necessarily threaten the organization's continued viability.
- 15 U.S.C. §§ 78dd-1 and 78ff, FCPA penalties for companies
  - $2-$25 million fine per violation or twice the gain
  - $21,663 civil penalty per anti-bribery provision violation
  - Debarment, denial of export license, disgorgement of profits
- 31 C.F.R. pt. 501, OFAC may refer cases to DOJ for criminal investigation, issue civil penalties, or issue cautionary letter or take no action.
- 31 U.S.C. § 3730, False Claims Act violations for government contractors
  - Treble damages and penalties (up to additional $21,526.80 per claim)
  - Lawsuits filed by private citizens
- FAR Subpart 9.4 provides for suspension and debarment

SQUIRE PATTON BOGGS

Overview of Compliance Assessments

Overview of Compliance Assessments

SQUIRE PATTON BOGGS

- Importance of a compliance risk assessment
- The U.S. Department of Justice's 2020 Guidance
  - Plans are not one-size fits all
  - Risks change over time
  - The starting point is to understand and evaluate risk (data analytics/metrics)
  - Devote appropriate resources
  - Continuous improvement is expected

Compliance Maturity Model

SQUIRE PATTON BOGGS

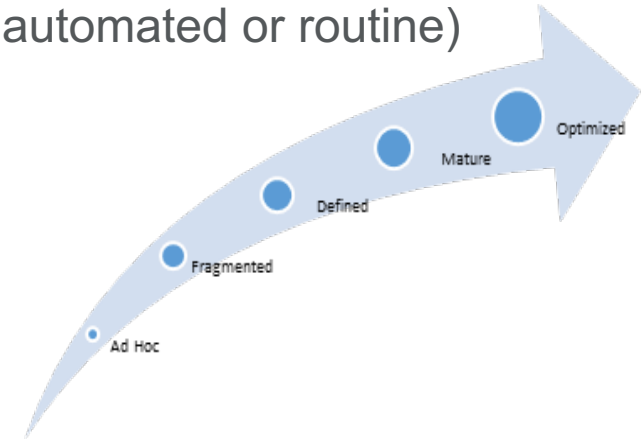
Ad hoc (procedures are informal, incomplete and inconsistently applied) ⟶

Fragmented (some compliance controls, but not consistent or widespread) ⟶

Defined (compliance controls documented and standardized) ⟶

Mature (compliance procedures integral part of the business and periodic reviews conducted to assess effectiveness of the program) ⟶

Optimized (regular review and feedback to ensure continuous improvement and elements are often automated or routine)



Risk Assessments Maturity Stages

SQUIRE PATTON BOGGS

Ad Hoc	Fragmented	Defined	Mature	Optimized
• Compliance risks may be identified, but not as a result of a formal process • A compliance risk assessment has not been completed and risk is not formally documented • Risk identification is reactionary or by happenstance	• Employees may be aware of and consider various compliance risks • Risk assessments may not be conducted regularly • Risk assessments may not cover all areas	• Processes have been implemented for risk identification, assessment, and reporting • A formal risk management process has been adopted • Risk assessments are informed by past misconduct, compliance violations, audits and corrective actions • Some automation exists for risk management process • Risk assessments result in updates to policies, procedures, and internal controls	• All formal processes for compliance risk management have been implemented throughout the organization, and are formally documented through a risk register or other means • All risks are assessed at least annually • Mitigation plans are monitored by risk owners and reviewed by external department (e.g., compliance, audit, legal) • Results of risk management process reported annually to executive leadership and Board	• Compliance, Risk Management, and Audit have integrated risk management processes that are improved continuously through ongoing monitoring. Risks are specific to functional areas • Executive management and Board regularly review risk program and provide leadership for key strategic and institutional risks • Automation supports risk management processes, where appropriate

SQUIRE PATTON BOGGS

Key Elements of a Compliance Assessment

Key Elements of a Compliance Assessment:
Developing the Assessment

SQUIRE PATTON BOGGS

- Involve Compliance Personnel
  - Include Internal Audit, Human Resources, and Legal
  - Develop clear mapping within compliance of responsible parties for key risk areas
- Consider whether to hire a third-party to conduct assessment
  - At a minimum, beneficial for first assessment and periodically
  - Provides independent and objective perspective

Key Elements of a Compliance Assessment:
Identifying Compliance Risks

SQUIRE PATTON BOGGS

- Define compliance risks for your organization
  - Compliance risks are “those risks relating to possible violations of applicable laws, regulations, contractual terms, standards, or internal policies where such violation could result in direct or indirect financial liability, civil or criminal penalties, regulatory sanctions, or other negative effects for the organization or its personnel”
  - Compliance risks vary by industry, region, and organization
  - Examples include criminal misconduct, uncertainty in financial markets, operational failures, third party risks, natural disasters, reputational harms, and other legal liabilities

Key Elements of a Compliance Assessment:
Identifying Compliance Risks

SQUIRE PATTON BOGGS

- A compliance risk assessment will shed light on the full range of risk exposure, including the likelihood that a risk event may occur, the reasons it may occur, and the potential severity of its impact
- An effectively designed compliance risk assessment helps organizations prioritize risks, map them to the applicable risk owners and/or locations, and effectively allocate resources
- Leverage the following methodologies to identify compliance risks:
  - Surveys
  - Investigation data and lessons learned
  - Training data
  - Internal audit results
  - Industry trends
  - Hotline report data

Example Compliance Risk Assessment Survey

SQUIRE PATTON BOGGS

- Survey should contain a listing of compliance risks the company has faced in the past, expected to face in the future, or are attempting to avoid by proscribing actions or behaviors through the Code of Conduct.
- Request survey takers to provide a relative ranking for each risk item by inputting a ranking within the following two scales:
  - Impact; and
  - Likelihood

Key Elements of a Compliance Assessment:
Prioritize Risks

SQUIRE PATTON BOGGS

- Prioritize identified ethics and compliance risks using common rating scale
  - Ex: low, medium, high
  - Ex: numbering system
- Develop a rating matrix or heat map
  - Heat maps are effective visuals to show hot spots of risks more likely to occur and having the most impact

	Likelihood										
Low Medium High	5										
	4										
	3										
	2										
	1										
		1	2	3	4	5	6	7	8	9	10
		Minor			Moderate				Severe		
		Severity									

Key Elements of a Compliance Assessment:
Remediation and Action Plans

SQUIRE PATTON BOGGS

- Identify existing measures that address compliance risks and evaluate whether to:
  - Improve controls
  - Monitor and consider additional mitigation controls
  - Continue existing controls
- Evaluate how to address the compliance risks
  - Reject the risk
  - Accept the risk
  - Transfer the risk
  - Mitigate the risk
- Develop remediation plans and mitigation controls
  - Create remediation plans for high priority risks
  - Improve mitigation controls to reduce likelihood of adverse events

Key Elements of a Compliance Assessment:
Proper Reporting and Implementation of Results

SQUIRE PATTON BOGGS

- Communicate Results & Take Action
  - Determine proposed action plan and how/who to report results
  - Use a reporting mechanism that works best for your audience
  - Update the risk assessment based on newly identified risks or other problems with the compliance program (assessment should be dynamic)
- Tailor Compliance Program Based on the Assessment
  - Update compliance policies and procedures on the basis of the risk assessment
  - Allocate company resources based on risk
  - Apply greater scrutiny to high-risk transactions, partners in high corruption index countries, etc.

Key Elements of a Compliance Assessment:
Board and Management Oversight

SQUIRE PATTON BOGGS

- Tone from the top
- Directors have a general duty of oversight for the Compliance Program
  - Stay informed about content and operation of compliance and ethics program and exercise reasonable oversight
  - Respond to “red flags,” which demonstrate a sustained and/or systematic compliance failure
- Expectations of compliance officer, senior management, and GC
  - Compliance function must have direct access to the board of directors or the audit committee
  - Provide periodic updates of compliance and ethics program, including results of program risk assessments
  - Use results of assessments to develop and support strategic plans and road maps

SQUIRE PATTON BOGGS

Testing and Monitoring

Testing and Monitoring Maturity Stages

SQUIRE PATTON BOGGS

Ad Hoc	Fragmented	Defined	Mature	Optimized
• Monitoring of compliance risks is informal, inconsistent, and sporadic, if it takes place at all	• Monitoring of compliance program elements and risk may exist, but may not cover all aspects	• Monitoring of compliance program covers all relevant program elements and risks, and is informed by past misconduct and audit findings	• Monitoring of compliance program covers all program elements and compliance risks	• Monitoring is coordinated and integrated into Compliance, Audit, and Risk Management functions
• Guidance on monitoring for compliance risk is not formally documented or provided	• Some guidance provided on monitoring and review, but not fully documented	• Some metrics exist for monitoring, but may not be fully developed or for all risk areas	• Monitoring is fully documented and includes ongoing monitoring by risk owners and independent monitors (e.g., compliance, audit, legal, consultant)	• Formal integrated monitoring plans are developed annually
• Audit (internal or third-party) in areas of compliance risk areas is not performed or inconsistently performed	• Reviews, audits, and interviews of employees and third parties on compliance are often reactionary, following misconduct	• Some measurement of corporate culture of ethics and compliance exists, but may not be formal, routine, or conducted enterprise-wide	• Monitoring results with corrective action plans are presented to executives and Board	• Monitoring plans are reviewed annually by executives and Board
		• Regular audit performed for key compliance risk areas, with audit results and findings reported to senior leadership and Board	• Metrics are defined for all monitoring risk areas, including metrics for measuring corporate culture of compliance with ethics and laws	• Metrics for monitoring activities are developed, reported, and utilized to drive continuous improvement in the compliance program
		• Following violations, root-cause analysis occurs but is ad hoc	• Audit function is reviewed regularly to ensure appropriate resources and funding	• Automation used when possible
			• A formal documented process for root-cause analysis exists	• Procedures to independently evaluate past misconduct through root-cause analysis are followed consistently

Importance of Monitoring

SQUIRE PATTON BOGGS

- Day-to-day process used by management to identify emerging risks
- Valuable way to evaluate effectiveness, efficiency, and consistency of operational controls
- Monitoring and auditing can overlap
  - Monitoring
    - Typically performed by business or compliance
    - Real-time identification of problems
    - “Detective” control
  - Auditing
    - Independent of management
    - Formalized method for audit process
    - “Preventative” control

Use of Metrics

SQUIRE PATTON BOGGS

- DOJ Guidance (2020) asks whether company has implemented metrics to collect information and help detect misconduct
  - Do the metrics inform compliance program?
  - Is there continuous access to operational data across functions?
  - Do compliance and control personnel have sufficient access to relevant sources of data?
  - Any impediments that limit access to data?
  - Are there timing metrics to ensure responsiveness?
- Common metrics applied to reporting and investigations
  - Source of allegations and reporting channels
  - Percentage of substantiated, unsubstantiated, insufficient information
  - Percentage of escalated cases
  - Subject matter of violations (business, geography, employee level)
  - Disciplinary actions and mitigating controls implemented
  - Days to resolution

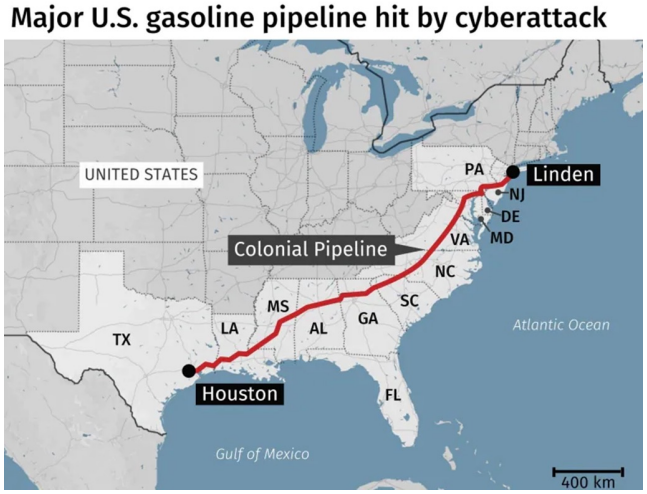
SQUIRE PATTON BOGGS

Practical Application

Appropriately Assessing Your Organization's Cybersecurity Risk Profile

Colonial Pipeline Ransomware Attack

SQUIRE PATTON BOGGS



Robust Regulatory Environment under the Biden Administration

SQUIRE PATTON BOGGS

- Biden Executive Order on Improving the Nation's Cybersecurity
- DOJ's Cybersecurity Enforcement Initiatives for Government Contractors
- OFAC Updated Sanctions Guidance for Virtual Currency Industry
- Cyber Incident Reporting for Critical Infrastructure Act
- 72- hour breach notification rule for Banks
- Proposed SEC Rules

Trends in Cybersecurity Enforcement

SQUIRE PATTON BOGGS

- U.S. Regulators across all industries are increasingly leveraging their authority to enforce cybersecurity regulations.
  - U.S. Securities & Exchange Commission (“SEC”)
    - Sanctioned eight broker dealer and/or investment advisory firms for failures in their cybersecurity policies and procedures that resulted in email account takeovers exposing the personal information of thousands of customers and clients at each firm. Penalties ranged from $200,000 - $300,000. (August 2021).
  - NY Department of Financial Services (“NYDFS”)
    - Fined Residential Mortgage Services, Inc. (“RMS”) a $1.5 million penalty to New York State for failing to report a cyber breach exposing New York residents' private data. (March 2021)

Trends in Cybersecurity Enforcement

SQUIRE PATTON BOGGS

- Continued
  - U.S. Health and Human Services (“HHS”)
    - Fined health insurer, the Lifetime Healthcare Companies, $5.1 Million to settle data breach affecting over 9.3 million people (January 2021).
  - U.S. Department of Justice (“DOJ”)
    - Announced the launch of its Civil Cyber-Fraud Initiative aimed at combating “new and emerging cyber threats to the security of sensitive information and critical systems” specifically targeting accountability of cybersecurity obligations for federal contractors and federal grant recipients, by way of the False Claims Act (October 2021).

Step One: Identify the Risk

SQUIRE PATTON BOGGS

- Identify which compliance standards apply to your organization.
- A cybersecurity framework is, essentially, a system of standards, guidelines, and best practices to manage risks that arise in the digital world.
- There are many different frameworks:
  - The US National Institute of Standards and Technology (NIST) Framework
  - The Center for Internet Security Critical Security Controls (CIS)
  - The International Standards Organization (ISO) frameworks ISO/IEC 27001 and 27002

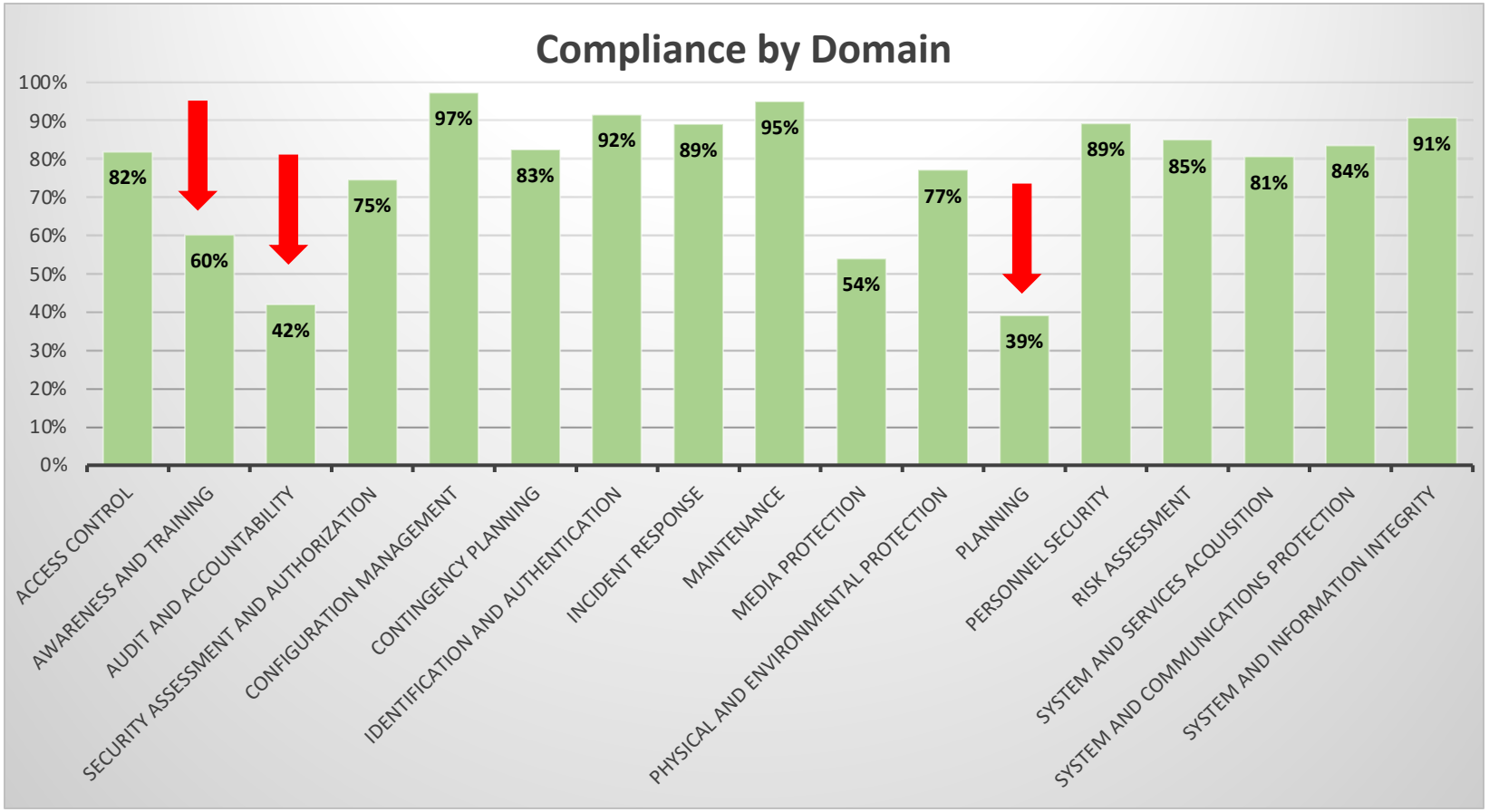
Step One: Identify the Risk

SQUIRE PATTON BOGGS

- Begin by documenting your key workflows, information systems, and transactions
- Are there areas in your key functions and systems that suggest non-compliance with regulatory or industry standard requirements?

Example NIST Family of Controls

SQUIRE PATTON BOGGS



(NIST SP 800-171)

Step Two: Map potential risks to possible outcomes and affected parties

SQUIRE PATTON BOGGS

- **Planning**
  - Possible outcome: ineffective response to a cybersecurity incident; failure to meet notification obligations; reputational harm; and litigation and/or enforcement action.

- **Awareness & Training**
  - Possible outcome: company experiences a Business Email Compromise ("BEC") after an employee opens a phishing email, resulting in fraudulent wire transfers to threat actors.

- **Audit & Accountability**
  - Possible outcome: Ransomware attack resulting from a failure to actively monitor logs and designate accountability for the same.

Step Three: Prioritize the most severe risks and determine control measures

SQUIRE PATTON BOGGS

- The process of implementing compliance programs, or beefing up the program you have, can be overwhelming
- Resources are precious and limited
- Prioritize all the identified risks by the severity of their outcomes
- Address the most severe first

- **Example: Planning (39%)**
  - Possible outcome: ineffective response to a cybersecurity incident; failure to meet notification obligations; reputational harm; and litigation and/or enforcement action.

Step Four: Implement controls and validate through testing

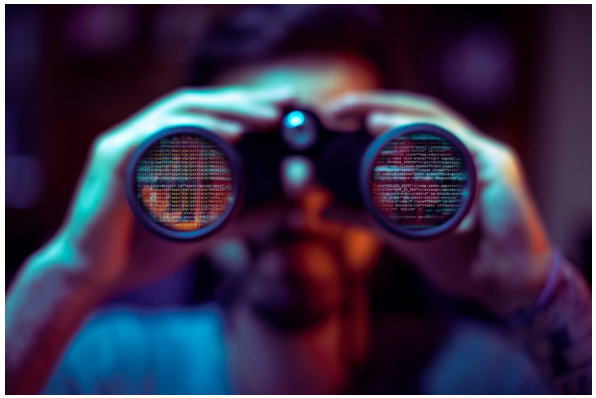
SQUIRE PATTON BOGGS

- Once you've determined what must be done to mitigate your compliance risks, implement those steps.
- A compliance function is only as good as its ability to prevent risk exposure.
- Thus, testing to validate your controls is an important next step before proceeding to another risk.
- **Example: Planning (39%)**
  - Implement control: implement an Incident Response Plan tailored to your organization's operational needs and enforcement/litigation risks.
  - Testing: conducting annual tabletop exercises to test the strength of the response

Step Five: Routinely re-evaluate risks, test controls, and update as needed

SQUIRE PATTON BOGGS

- Don’t forget that a corporate compliance program should be a permanent, ongoing part of your business.
- As your business grows, your risks change; legislation affecting your business does too.
- Moreover, unmonitored, unenforced controls tend to be discontinued after a while.
- Therefore, you should routinely monitor your controls, re-test them periodically, and re-evaluate them as the business grows and laws change.



Template: Cybersecurity Scorecard

SQUIRE PATTON BOGGS

Cybersecurity Lifecycle	Selected Metrics	Green (At or Better Than Expected)	Yellow (Outside Expected)	Red (Well Outside Expected)
Identify Monitored potential cybersecurity threats or risks, such as malicious sites and criminal actors, fraudulent attempts to trick users via phishing, etc.	**External Threats**			
	Overall New Threat Information Being Monitored			
	Watchlist of Groups Actively Targeting Similar Companies/Industry			
	Real Phishing Campaigns Against Company			
	Internal Threats			
	Personnel with Admin Access			
	Employee Phishing Test Pass Rate			
	Systems Scanned for Security Vulnerabilities			
	Internet-Facing			
	Corporate Data Centers			
	Extreme and High Open Vulnerabilities			
Protect Measured effectiveness of technical controls and processes.	Real Phishing Emails Blocked			
	Malware Blocked			
	New or Potential High Risk Compliance Issues			
Detect Investigated potential cybersecurity events such as malware, phishing, etc.	Investigation of Events			
Respond Coordinated response to new cybersecurity incidents. All incidents are classified on a severity scale of one being the lowest impact and four being the highest impact.	New Incidents			

Questions?

SQUIRE PATTON BOGGS