MEMO

To: ALFA attendees
From: Philip Maynard, CLO, Tealium Inc.
Re: The Intersection of Seller Due Diligence & an Effective Compliance Program
Date:

Introduction

Seller Due Diligence – the process by which a potential target company in a business combination transaction, or a company seeking a capital raising transaction, examines its own affairs and circumstances so it can quickly, nimbly and accurately respond to a prospective buyer's or investor's (or underwriter's) due diligence request.

This makes perfect sense. In a perfect world, a target, or seller, in a business combination or capital raising transaction, would know everything about itself that the buyer or investor will want to know, and have it readily available.

In a practical world, however, this perfect world may be difficult to achieve in advance of the pressing need of a pending transaction to compel due diligence action. Without a compelling event:

- Why would we spend the money now?
- Where are we going to get the resources/headcount to do this work?
- We don't even know exactly what the buyer/investor is going to ask for?
- This would be a big diversion for management from running the business.
- How are we going to keep the data up to date?

So, is there a way to address these questions and concerns? At a high level, what is the buyer or investor really looking for? They don't want to buy, or invest in, a lot of problems. So, they're looking for risks. They're looking for problems that could pose a risk to the value of their purchase or investment.

So, in the absence of management's willingness to commit resources in advance of a compelling transaction to conduct traditional, self-due diligence, what other organizational structure can a target/seller employee to be well prepared when a compelling event emerges?

Enter the company's corporate compliance program!

Leveraging an Effective Corporate Compliance Program

First, what is a corporate compliance program? Here's my definition:

An compliance program is a broad matrix of personnel, policies, procedures, and controls designed, organized and staffed to carry out the following six pillars:

- Identify the risks faced by the company (think enterprise risk assessment process),
- Creation and implementation of policies and procedures to mitigate or obviate those risks,

- Train the relevant audiences about both the risks and the steps taken to mitigate or obviate those risks (training and enablement),
- Identify risks when they materialize – both proactively (via audit, etc.) and reactively (via effective reporting and controls),
- Investigate and remediate the risk and the resulting damage,
- Improve the program to prevent recurrence of the risk.

Second, what makes a compliance program an EFFECTIVE compliance program? The U.S. Department of Justice tells us in their recent guidelines and in their Principles of Federal Prosecution of Business Organizations. Without getting too far into the weeds, it is a program that answers well three questions:

- Question One – Is the corporation's compliance program well designed?
- Question two – Is the company's compliance program adequately resourced and empowered to function effectively?
- Question three – Does the company's compliance program work in practice?

Third, why have a corporate compliance program, and why make sure it is EFFECTIVE? The short answer is that both management and the board have fiduciary duties to make informed decisions and neither can do so without a compliance program in place. Also, if the company does make a mistake that gets DOJ attention, having an effective compliance program in place can reduce or even eliminate penalties.

Fourth, Compliance is a cross functional activity. Cross functional responsibility is necessary to implement the six pillars throughout the company and to infuse a culture of compliance. There does need to be leaders with sufficient independence, authority, expertise, seniority and executive support to assure cross functional cooperation. Accordingly, it is really a legal necessity to have a properly organized and staffed compliance program.

Fifth, if you want to dig into more detail about what an effective compliance program should be doing, I've attached a Compliance Program Key Activities Matrix, just for fun reading.

Back to Seller Due Diligence

See where this is going? Buyers and Investors want to know what the risks are in the business, and what actions have been taken to mitigate or obviate those risks, so they're not buying unexpected problems. Pick an area where you expect a buyer or investor to look for problems – finance, contracts, InfoSec systems, data privacy compliance, HR systems & policies, third party audits and certifications, etc. Check the Key Activities Matrix.

If you have an effective compliance program, you already are conducting and updating an enterprise risk assessment, you are already creating policies and other ways to mitigate the risks, etc. With a little expansion in scope of your compliance function it is already doing a lot of the work that a one-off due diligence exercise would do, and keeping it updated!

A Word about Data Rooms

If you are subject to U.S. securities laws and you issue equity awards to employees, you're aware of SEC rule 701 that provides an exemption from the registration requirements of the Securities Act of 1933. Once you cross a certain dollar threshold in the value of equity awards granted, which most venture backed companies will do mid-life, the company must provide a disclosure document to those equity award holders and it must be updated periodically. Tealium, and many companies our size, set up a virtual data room to enable viewing of the disclosure documents (including financial statements, description of the business, risk factors, etc.) while preserving confidentiality. (restrict copying, downloading, printing, etc.).

See where I'm going, you've got a good start on a transactional data room that can be swiftly and accurately populated when coupled and aligned with the company's effective compliance program.

Exhibit – Compliance Program Key Activities Matrix

Tealium Corporate Compliance Program – Strategy and Key Activities
From: Phil Maynard, CLO
2024 Template

Legal Department Mission Statement

"The legal department mission is to internally provide professional, timely and useful advice and service, engage and actively manage outside counsel when necessary, implement policies and procedures to mitigate company risks, help protect the Company's intellectual property and promote the company as an innovator and thought leader, and perform all work in the most cost effective manner possible so as to contribute to the company-wide effort to build shareholder value."

Corporate Compliance Program – Long Term Goal

Establish an effective, comprehensive, enterprise compliance program that meets the requirements of applicable law and regulation including the SEC regulations, DOJ guidelines, Federal Sentencing Guidelines and industry expectations for a public company, and establishes Tealium as the most trusted Customer Data Platform.

Pillars of a Corporate Compliance Program

The Six Pillars of an Effective Compliance Program: A broad matrix of policies, procedures, practices and personnel designed to (i) identify the risks faced by the enterprise (including risks of criminal conduct, but not limited to that) (enterprise risk assessment), (ii) mitigate or obviate those risks (create and implement policies & controls), (iii) train the relevant audiences about both the risks and the steps taken to prevent those risks (enablement), (iv) identify the risks when they

materialize (both proactive (audit) and reactive (reporting & controls)), (v) investigate and remediate the risk and resulting damage, and (vi) improve the program to prevent recurrence.

The Three Questions that Must be Answered (because the DOJ is going to ask them)

- **Question One - Is the corporation's compliance program well designed?**
  - Risk Assessment
  - Risk rating and resource allocation
  - Periodic review, audit
  - Policies and Procedures
  - Code of Conduct
  - Comprehensiveness
  - Responsibility for Operational Integration
  - Accessibility
  - Training and Communication
  - Confidential Reporting
  - Investigation Process
  - Third Party Management
  - M&A Activities
- **Question Two – Is the Company's compliance program adequately resourced and empowered to function effectively?**
  - Paper Program v. Effectively Implemented Program
  - Commitment by Senior and Middle Management
  - Autonomy & Resources
  - Outsourced Compliance Functions
  - (Dis)incentives and Disciplinary Measures
- **Question Three – Does the Company's Compliance Program Work in Practice?**
  - The Justice Manual requires prosecutors to assess the adequacy and effectiveness of the company's compliance program at the time of the offense and at the time of the charging decision.
  - Continuous Improvement, Audit, Periodic Testing and Review
  - Analysis and Remediation

Key Activities Matrix

The following matrix is a more granular view of many of the activities that must be undertaken to implement an effective compliance program that meets the six pillars of an effective compliance program, is well designed considering Tealium's specific industry and business, and is adequately resourced and works in practice. Organizational and staffing recommendations follow the matrix.

Key Activity	Description	Responsibility	
Risk Identification			
Enterprise Risk Assessment	Assess and prioritize (risk weighting) compliance risks associated with Tealium's internal and outward facing business activities and services.		

	[add detail re: actions, projects, etc.]		
	Known risk areas include Information Security, Data Privacy, Vendor Management, domestic and international labor & employment practices, financial controls, contract risk & liability management including compliance with contractual covenants, FCPA & anti-bribery laws, export control & sanctions compliance, …		
Inventory risk reduction related policies, procedures and controls	Create comprehensive inventory of corporate policies, procedures and controls (PP&C's) intended to mitigate or obviate the risks identified in the enterprise risk assessment.		
Risk Gap Analysis	Evaluate whether existing PP&C's effectively mitigate the risks they are intended to mitigate. Evaluate whether there are risks that do not have an associated PP&C.		
Create or Update PP&C's	Following Gap Analysis, create or update PP&C's to address gaps, and implement the new and updated PP&C's.		
Periodic Review	Establish calendar of periodic review of Risk Assessment (painting the Golden Gate Bridge) and for review and updating of PP&C's		
ISPMS	Chair the Information Security & Privacy Management System committee and set its agenda and activities. Key purposes/charter of ISPMS include: (i) assuring Tealium as a data processor has information security and privacy policies that are best practices, (ii) periodically review/audit practices to assure operations are conducted in accordance with policies and update policies as appropriate, and (iii) manage compliance and customer audits including ISO 27001, 27701 and SOC 2 type 2 compliance. Critical that these functions be independent of operations.		
Selected Key Compliance Areas & related key activities			
Data Privacy Compliance	Assure privacy policy statements are reviewed and updated periodically to assure accuracy.		
	Regulatory expertise – maintain privacy regulatory expertise, including GDPR and other privacy regulations in locations the Company does business. Advise the business proactively on data privacy requirements.		

	DPA – periodically review and update standard DPA, negotiate edits when necessary. Assure DPA accurately reflects Tealium's data processing and privacy policies.		
	Privacy by Design – assure data privacy considerations are fully considered at the research & development stage of products or services or addition of new subcontractors or the incorporation of new third-party technologies into the Company's products or services.		
	Privacy by Default – Drive a culture of pervasive attention to data privacy rules.		
	Data Privacy Officer responsibilities, including maintaining a compliant location for data subjects to submit requests, and assuring procedures are in place and followed to respond to DSR's. [outline all other DPO duties]		
	Publication of white papers and other communications and participation in programs that demonstrate Tealium as a thought leader on data privacy & security in the Customer Data Platform space.		
	Assure internal and employment policies are regulatorily compliant from an employee data privacy perspective.		
	ROPA – create and manage capability to report on processing activities.		
	Conduct Data Privacy Impact Assessments (DPIA's) as necessary or appropriate. Create policy regarding when DPIA's are needed, and scope of DPIA's.		
	Prepare and maintain data mapping of Tealium processing activities, and make such information available to customers proactively and transparently.		
Information Security	Assure the customer facing DSS is fully consistent with the Company's InfoSec policies and procedures.		
	Review and periodically re-review and update InfoSec policies to assure inclusion of best practices, satisfaction of periodic ISO, SOC2-type 2 and other audit requirements, …		
	Audit management – In conjunction with ISPMS manage, and respond to requests from, outside certification auditors (e.g. ISO 27001, 27701, SOC 2); assure creation of documentation of policy compliance that will be required by auditors beginning 2024.		
	Assure responses to customer audits regarding privacy or security matters are accurate and complete.		

	Assure vendor InfoSec compliance reviews are completed and decisions about adding a new vendor are consistent with the compliance review results and risks.		
	Periodically review to assure InfoSec policies are fully implemented and followed. (see Audit, below)		
	Assure policies and practices are compliant with customer and regulatory requirements, including least privilege, data minimization, data deletion, data retention and regionalization.		
	Periodically review and testing of BCP and disaster recovery plans to assure inclusion of best practices, satisfaction of contractual obligations to customers and others, and accuracy (see Audit, below).		
	Assure implementation of an efficient procedure for InfoSec review of customer information security requirements when necessary, including identification of any policy gaps between customer and Tealium PP&C's.		
	Assure RIF responses regarding privacy and security matters are accurate; periodically review.		
	Lead the activities of the ISPMS (see ISPMS above, Audit below).		
	Data retention & deletion – establish enterprise-wide policy on data retention and data deletion, as both data processor and data controller; periodic audit to assure compliance with policies.		
Labor, Employment & Culture	Periodically review Tealium Code of Conduct and Business Ethics to assure inclusion of industry best practices, and compliance with legal and regulatory requirements.		
	Implement process for review of customer vendor codes of conduct when necessary.		
	Periodically review all Company employee handbooks to assure compliance with local laws and regulations and local custom as appropriate.		
	Periodically review and update Company hiring, on-boarding and off-boarding documentation to best assure compliance with local laws and regulations.		
	Assure Hotline for reporting of suspected policy or legal violations is operational, and properly available and monitored.		
	Assure PP&C's in place to investigate allegations of violations of policy (see Enablement, below).		
	Assure periodic employee compliance attestations are performed and reviewed.		

Financial Controls	Assure appropriate controls are in place to meet financial audit requirements, GAAP requirements, revenue recognition policies, and flag any suspicious payment requests for investigation.		
	Assure contract provisions with customers and vendors have appropriate tax provisions, payment terms and revenue recognition treatment.		
Export Controls	Assure procedures are in place and followed to vet customers and vendors against export control and sanctions lists; procedures are in place to assure products are not made available in violation of prohibited countries or persons lists; periodically confirm whether Tealium products or services are EAR99 or require further licenses.		
Marketing and Corporate Communications	Assure that marketing activities are compliant with data privacy rules and appropriate policies are in place. Assure appropriate policies are in place to assure accuracy of corporate communications (including press releases) and that appropriate executive approvals are obtained and documented.		
Enablement	Train all appropriate audiences on the PP&C's that affect the performance of their responsibilities …		
	[list the core training requirements – e.g. harassment, code of conduct, info security, privacy rules affecting marketing activities, privacy by design/default, etc.		
Reporting and Audit	Assure there are operational and appropriate and regulatorily required methods for reporting of alleged or suspected violations of law or policy, and that those reporting methods are monitored.		
	Implement a calendar for periodically, proactively auditing key policies to assure they remain accurate and are being followed. It is important that the audit function be separate from the part of the organization that is responsible for operating in accordance with those policies.		
Investigation & Remediation	Assure PP&C's exist to quickly respond to, and investigate, any reported allegation of wrong-doing or legal or policy violation. Investigation depends on the nature of the allegation, but should include the		

	equivalent of a root cause analysis. Participate with others to minimize damage and remediate the matter.		
Program Improvement to prevent recurrence	Propose and implement PP&C's improvements to prevent recurrence.		

Organization and Staffing

Compliance is a cross function activity. There does need to be a leader with sufficient independence, authority and seniority, and sufficient executive support, to assure cross functional cooperation. Certain functions can be outsourced under effective and appropriate supervision. However, there is a significant amount of work that will require one or more headcount with appropriate training and experience to effectively carry out the key activities listed above. In particular, the compliance personnel need sufficient expertise to understand the Company's products and services at a deep technical level, experience with auditing compliance with technical PP&C's, and experience with technical audit requirements (such as ISO, SOC2-type 2, etc.).