Regulatory Compliance in Software Development: a Grounded Theory Study Interview Guide

Background and Purpose

Society uses laws, regulations, and security standards to embed ethical norms into engineering systems, including software systems. However, this process is not free. Large multinational organizations spend on average about $5.5 million USD annually to comply with regulation at the state, federal, and international levels [1]. For non-compliance, the average cost of remediation is about $14.82 million USD [1]. None of these figures address the value of ethics and reputational costs to organizations in regulated domains. We conducted a systematic literature review of research on regulatory and security standard compliance and found that academic research directly connecting regulatory and security standard compliance to the later stages of the SDLC is rare [2]. In particular, we did not find any academic research examining software practitioners' perceptions of regulatory and security standard compliance as part of the software development process. The interview guide you are reading now is the result of our efforts to address this gap.

This interview study has three goals: (1) understanding the state-of-the-art for regulatory and security standard compliance in software; (2) understanding practitioner perceptions of regulatory and security standard compliance; and (3) given that some regulations have been around for more than a decade, identifying whether and how perceptions have changed or matured as a response. This study targets software practitioners in the industry with different experience levels and backgrounds ranging from 5 to 30 years of experience operating in regulated domains (e.g., healthcare, data protection and privacy, finance, and public administration). Initial drafts of this interview guide were pilot tested by interviewing six software practitioners. After analyzing feedback from our participants, we produced the final guide and a coding scheme—both seen below. A more detailed description of our methodology is within the associated paper for this artifact [3]. Researchers seeking to replicate or adapt this interview guide may wish to consult appropriate research methods and source materials [4, 5].

How to use the interview guide

We structured the interview guide into five sections. Each section includes the questions asked to the participant as well as our rationale for asking the question and the data we hoped to collect. The first section is the Participant's Background or Demographics. The second section, the Participant's organization, examines the participant's role in their current organization. It sets up the next two sections, which detail the Participant's Experience with Software Development Life Cycle (SDLC) (Section 3) and the Participant's Experience with Regulatory or Security Standard Compliance (Section 4). The third section focuses on the software development process and the decision factors and influences that affect development. The fourth section is where we dive into regulatory and security standard compliance within the software industry, asking questions like what regulations they must comply with, how compliance fits within their software development process, and if there are challenges and benefits to compliance. The last few questions within this section, for the most part, are end-of-interview questions. We asked questions about recent events that may affect the compliance landscape, final thoughts regarding compliance, and wishes or thoughts of what the participant might like to see as far as research or updates within the Software community regarding compliance. The last section is the Summary section to capture any additional data, recruit additional candidates for the interview study, and thank the participant for their time and inputs.

When using this interview guide, keep three things in mind. First, this is a semi-structured interview guide. We chose a semi-structure interview format to ensure consistent coverage of demographics, software development life cycle, and regulatory and security standard compliance while allowing the participants and researchers to add to the discussion or ask additional questions during the interview.

Second, the coding scheme and details outlined below give a general idea of the type of data expected during the interview. However, do not share the details of the coding scheme or the coding schemes relationship to the questions. These details are shown in gray under each question, and they are only included to help the researcher when analyzing data resulting from a completed set of interviews. All boldfaced elements of the guide are intended to guide a live interview and can be shared with participants. During the interview, aside from prompting for details, examples, and descriptions from the participants and making sure the participants stay on topic, we should allow the participants to talk and not give them any material that could bias their answers. Remember, the goal is to capture participants' perceptions, thoughts, and opinions.

Third, try to keep to the general structure and flow of the questions as outlined in the interview guide. The researcher (i.e., the interviewer) or the participant may have to clarify or expand on specific points. However, keeping to the general structure of the questions will ensure consistency amongst the different interviews and that the analysis of data is comparable.

History of the Interview Guide

This Interview Guide has gone through 10 version prior to its use in the Interview Study. Version 10, completed in late October 2020, was the version used in the interview study. The Interview Guide below is version 11. The difference between versions 10 and 11 are:

1. The inclusion of Rationale and Type of Data included under each question and highlighted in grey. We included this to help someone attempting to replicate or reproduce these results.
2. The adding of sections 4.11 and 4.12 to the interview guide. Section 4.11 and 4.12 were asked during the interview as opportunity questions (4.11: Recent Events) based on the timing of the interview study and reflection questions based on each individual participant (4.12: Wishes).

Coding Scheme:

Code	Subcodes	Definition
Background/Work History		Description of the Participant's background and work history (Note this code is attribute related); **Heuristic: Whenever the participant is describing something not related to their current job, code Background/Work History and look for the buzz words relatable to the subcode.**
	College Educated	Received any four-year degree from a college or university.

	Non-College Educated	On-the-job training, high school diploma, industry certification, associate’s degree, or partially completed four year degrees.
	Technical Background	Participants that have previously worked as a Software or Application Developer, Engineer, Architect or Coder, where their focus is technical implementation of software or system.
	Non-Technical Background	Participants that have previously worked as a Manager, Team leader, or Director, where their focus is overall development and management of software or system. Job titles can include Product Manager, Customer Relations rep, or Data Analysis.
	Compliance Background	Participants that have worked within or supported a regulated field, like healthcare, for more than two years, where regulated compliance is emphasized or their job, examples can include Privacy Engineer, Civil Engineer, or Compliance officer, where their focus is compliance.
	Non-Compliance Background	Participants that have worked within the Software Industry but have not held jobs or had much focus on regulatory or security standard compliance as part of their job. Job descriptions within the Technical Background code may fall into this category.
	Cybersecurity Background	Participants have job background in security or risk management, or they have performed responsibilities in implementing, assessing, or enforcing technical security features for software or technical system for 2 or more year. Job Titles can include Security Engineer or Developer, Information Assurance Manager, Quality Assurance Manager, Risk Manager.
	Non-Cybersecurity Background	Participants that have worked within the Software Industry but have not held jobs or had much focus on Cybersecurity as part of their Job. Job descriptions within the Technical

		Background code may fall into this category.
	10+ years of experience	10+ years of experience working within industry and/or extensive research with the Software Industry.
	Less than 10 years of experience	Less than 10 years of experience working within industry and/or extensive research with the Software Industry.
Current Job		Description of the Participant's current Organization, Job, Roles and Responsibilities, and Customer base. Heuristic: When participant is describing their current job, what they focus on, who their customers are, Code CurrentJob
	Compliance Focused	Description that indicates the participant's job is manage or assess compliance within the product
	Cybersecurity focused	Description that indicates the participant's job is to mitigate or manage vulnerabilities within the product
	Risk Focused	Description that indicates the participant's job is to mitigate or manage risk within the product
	Functionality Focused	Description that indicates the participant's job is focused on producing a product or new feature for end-users
	Business Focused	Description that indicates the participant’s job is focused on business side (i.e., cost and timeline to produce products, customer requirements)
	Policy Focused	Description that indicates the participant’s job is focused on adherence to internal policies and procedures. This focus can overlap with the Compliance or Cybersecurity Focus subcode.
	Research Focused	Description that indicates that the participant’s job is to improve how the organization does business through research
	Large Organization	Participant’s organization More than 10,000 employees, more than $5

		Million in revenue, and abundant human &amp; physical resources.
	Small Organization	Participant’s organization Less than 1000 employees, less than $1 Million in revenue, and limited human &amp; physical or contracted resources.
	US only Customers	Participant’s Job or organization Customers are limited to only U.S.
	International customers	Participant’s Job or organization Customers are more than one country.
	Specific Industry	Participant’s Job or organization focused on a specific industry.
	General customer base	Participant’s Job or organization has a wide customer base with focuses on multiple types of industry.
	Timeline	How long the participant has worked in their current job and/or with the organization.
DevProcess		Description of the software development process in use at the participant's organization, in general, not necessarily about reg compliance; **Heuristic: When someone is describing Software development in general. Does not have to be a particular development process like Scrum or Waterfall.**
	ReqProcess	Description of how requirements are elicited; **Heuristic: When someone is describing development and highlighting requirement (to include customer feedback and problems), code DevProcess and subcode ReqProcess.**
	DesignProcess	Description of how software design is carried out **Heuristic: When someone is describing development and highlighting Design.**
	TestProcess	Description of how testing is done **Heuristic: When someone is describing development and highlighting Testing**
	ImplementProcess	Description of how software is released **Heuristic: When someone is describing development and highlighting release or assessment prior to release of a software or system.**

	MaintProcess	Description of how software is maintained and updated throughout its life **Heuristic: When someone is describing development and highlighting updates or maintaining software after production release.**
	DEVDecision	Description of why the participant and/or their organization uses a particular development process; **Heuristic: When someone references on decision-making or why they decided to do something a certain way, that is a DevDecision code**
	DefProcess	Description of a defined SDP; **Heuristic: When someone describes SDP and puts a name to their or organizations SDP, then DevProcess and DefProcess**
	NoDefProcess	Description is not a defined SDP; **Heuristic: When either someone describe their process as "ad-hoc" or they are not familiar with it to comment on what process is used, then Code NoDefProcess - the latter has a caveat that should be noted as the Development Process is unknown to the Participant**
	DevOther	Catch-all
ReqMGT		Description of how requirements are elicited and managed; **Heuristics: When someone is talking in more detailed about requirements and how they are assessed and managed, where they come from. Then code ReqMGT**
	ReqSource	Description of where the requirements come from; **Heuristic: When someone is talking about requirements with reference to understanding or source (including customer feedback or problem), code ReqMGT and subcode ReqSource**
	ReqGathering	Description of how requirements are gathered; **Heuristic: When someone is talking about requirements with reference to understanding or what is driving a requirement**; Examples- Use

		Case, customers requirement, stakeholders meeting.
	ReqPrioritzation	Description of how requirements are prioritized. **Heuristc: When there is a description that suggest Requirements Priorization is a factor, then code ReqMGT -> ReqPriotization**
	ReqChangeMGT	Description of how requirements evolve and how that change is addressed and managed; **Heuristic: When someone is describing Change, or flexibility to Change, or how requirements are track or how the evolve, code ReqChangeMGT**
	ReqOther	Catch -all; **Heuristic: ReqOther is a catch-all code that is used when something is on the topic of requirements or Req management, not covered by other subcodes in this field**
	ReqStakeholder	Description of requirements perspective and to whom that perspective belongs to
	ReqCommunication	Description of how requirements are communicated; relatable to Compliance Communication and ComplianceReq
ComplianceMGT		Description of how the participant and/or their organization assesses, tracks, and manages regulatory and security standard compliance. **Heuristic: Whenever there is a description on the topic of compliance (regulatory, privacy, or security), how it is managed, assessed, tracked, demonstrated, or about how the participant's organization compliance program is structured or operates, then code ComplianceMGT with the appropriate subcode.**
	ComplianceAssessment	Describes how compliance is assessed
	ComplianceTracking	Describes how they track compliance requirements
	ComplianceWhy	Describes why they must adhere to a compliance requirement
	ComplianceTimeline	Describes how long they must comply when a change occurs

	ComplianceWhen	Describes when Compliance is addressed within their SDP
	ComplianceReq	Describes what compliance requirements are required and who is responsible
	ComplianceOther	Catch-all; **Heuristic: ComplianceOther is a catch-all code that is used when something is on the topic of compliance management, not covered by other subcodes in this field**
	ComplianceCommunication	Describes how stakeholders communicate about compliance (Note potentially overlaps with ComplianceReq); **Heuristic: Whenever someone is one the topic of compliance and how it is communicated amongst stakeholders or between organizations**
CompliancePreceptions		Description of how the Participant perceives regulatory and security standard compliance. **Heuristic: Whenever the participant offers their opinion, thoughts, and perceptions on Compliance, use the CompliancePerceptions code.**
	ComplianceChallenges	Description by the participant on what are some challenges to compliance (examples from the text- updating legacy system to comply with current or new regulation, communication or interpretation between stakeholders, resource availability); **Heuristic: When something in the text points to compliance might be a issue or a challenge within implementation of a SDP, the CompliancePerception -> Compliance Challenges**
	ComplianceBenefits	Description by the participant of some benefits to compliance (examples from the text- security and developer awareness, trust, and confidence in develop product, sell and compete to more customers). **Heuristic: Similar to the ComplianceChallenges, except if the data or text points to compliance as a benefit to the participant.**

	ComplianceRisks	Descriptions by the participants what are risks to compliance or non-compliance (ex. 1: Proactive compliance companies risk money and false start requirements by trying to stay ahead of compliance 2: Reactive compliance companies risk delays in features and lost manhours to compliance)
	ComplianceSeparation	Descriptions by the participant that separates security and compliance within SDP;
Opinions/Perceptions		Thoughts or perceptions by the participant; **Heuristic: Whenever someone is offering an opinion or perception, (look for key phrases "I don't think" or "I think") code Opinion/Perception then subcode on what the Opinion or Perception is referencing.**
	Stakeholders	Participant's thoughts or perceptions of other stakeholders (ex.1: Developers view lawyers or legal as overly cautious or that some of their requirements to compliance is overkill. 2: Some Developers view Security assessor's expertise as only running the tool while other developers view Security assessors as highly technical and knowledgeable, but often overwhelmed and stretch thin with the amount of products they must assess); **Heuristic: When the participant is stating their opinion/perception in reference to another stakeholder group, then code opinion/perception -> stakeholder**
	SDP	Participant's thoughts or perceptions of how they develop software (i.e., Offer opinions on how their SDP is good or could be better in some areas); **Heuristic: Whenever someone is describing why they do a particular development process and list all the benefits to justify their process there Is 1) Opinion/Perception -> SDP because it is their perception**

		specifically about their SW Development Process
	Organization	Participant's thoughts or perceptions about their organization and how it is managed in relation to RC/SSC (e.g., Some view their organization as great setup wise because it offers resources and resolution process on a particular implementation issue)
	OnCompliance	Participant's thoughts or perceptions on compliance (e.g., "Compliance is necessary but not sufficient"); **Heuristic: Whenever an opinion or perception points to a specific piece on compliance then also code Opinions/Perceptions -> OnCompliance**
	SWDevIndustry	Participant's thoughts or perceptions on the Software Development Industry in relation to RC/SSC
	Other	Catch -all; **Heuristic: Whenever an opinion or perception points to a something specific (i.e., Stakeholder, SDP, Organization, compliance) use assoicated codes. If there is an outlier use Other subcode.**
Technical Debt		Describes TD as defined as the cost of prioritizing one requirement over another and addressing it after release. **Heuristics: Whenever the participant refers to Technical Debt and/or describes something close to definition, use <u>Technical Debt</u> and the appropriate subcode as described. Data could overlap with the RegMGT -> ReqPrioritization code**
	WhyTD?	Describes why TD occurs as related to RC/SSC (ex. 1: Change in regulation resulting in production systems requiring refactoring to comply and new updates to a production system get delayed. 2: Resource availability-certain things must be prioritized and tested within a certain timeframe, which means other items get tested and assessed after release 3: Document debt)

	CostTD	What are the cost or impacts to TD as related to RC/SSC (e.g., Larger Maintenance overhead, delays in feature release
	RiskTD	What are the risks to TD as related to RC/SSC (e.g., Exploitation vulnerability, code not working optimally or buggy source code, unsatisfied customers)
	AddressingTD	Describes how they manage TD
Wishes		This is in response to the "End of Interview questions list in the RC/SSC section question L. & M. and Summary Section. Describes things the participant wishes they or their organization did differently. **Heuristic: Any kind of hypothetical to improve the organizations processes or the software industry in general use this code.**
Recent Events		Describes how recent events may have affected your organization or how you conduct business as related to RC/SSC. **Heuristic: Whenever the participant references a "News worthy" topic notable from Jan 2020 to Jan 2021, use the Recent Events code and the appropriate subcode.**
	COVID	Describes how COVID may have affected them
	Presidential election	Describes how Change in Administration may have affected them
	Regulation changes	Describes how recent regulatory decision (i.e., GDPR, EU Court decisions) may have impacted your Processes
	Regulatory Infractions	Describe if any regulatory infractions (i.e., Zoom) may have impacted your business
Technical Difficulty		Pause in the transcript
Clarify Questions		Questions is restated or clarified for the Participant
Other		Catch-all code to be applied and expanded on as a new code

Beginning of the Interview Guide Script!

IRB protocol review: [Hit Record] Before we begin, I want to thank you for volunteering your time toward this study. I also just want to remind you that we are recording this session and only Dr. Massey and I will have direct access to the interview recording. Lastly, if you want to withdraw from the study, just let either one of us know. We will also send you a notification of completion and publication for your records.

Shall we begin!

Project Manager and Developer's Questionnaire

1. Participant's Background

1.1. Give a brief history of your professional background with the software system?

1.1.1. **A presentation of the rationale:**

1.1.1.1. Context regarding the participants background and experience with software systems and their development.

1.1.1.2. It helps to understand the participants qualification and whether they are new to the Software Industry or they part of the Software Industry for a number of years and the different positions they have held.

1.1.2. **Types of data or response to question:** (Reference code: Background/Work History)

1.1.2.1. Educational Background or previous research in academia

1.1.2.2. Personal History with the Software Industry

1.1.2.3. Whether they have a technical or non-technical perspective to the subject area

1.1.2.4. Years in previous job roles

1.1.2.5. Years in current job role (Reference code: Current Job -> Timeline)

1.2. If bio, start with c.

1.3. Why are you interested in regulatory and security standards?

1.3.1. **A presentation of the rationale:**

1.3.1.1. The topic of the interview study is on Regulatory and Security Standard Compliance (RC/SSC). If the participant is going to offer their thoughts and opinions on RC/SSC, then should be able to articulate an initial interest in the topic.

1.3.1.2. This question also helps to set the tone for the rest of the interview and how inclined the participant is willing to get into details about their experience and their organization's process.

1.3.2. Types of data collected:

1.3.2.1. Personal History and experience with RC/SSC (Reference code: Background/Work History)

1.3.2.2. Reasoning of why they consent to the interview (Reference code: Current Job or CompliancePerception or ComplianceMGT)

1.3.2.3. Initial perspective on RC/SSC unbiased by the interviewers (Reference code: CompliancePerception or ComplianceMGT)

1.3.2.4. Detail examples of their applications or process when it comes to RC/SSC (Reference code: ReqMGT or ComplianceMGT)

2. Participant's Organization and their role

2.1. What is your role and responsibilities in your current organization?

2.1.1. **A presentation of the rationale:**

2.1.1.1. We ask the participants to describe in their own words their current job role and what their job entails (e.g., their responsibilities). These descriptions give us a baseline understanding of the participants job within the Software Industry and/or their organization.

2.1.1.2. It also helps the researcher to understand how involved the participant is with their organization's software development process and if RC/SSC is a requirement as part of their job role.

2.1.1.3. Lastly, we do categorize the participants in four groups (i.e., SW Developer, Data/Privacy Engineer, Manager/Director, or Regulator) for comparison and analysis.

2.1.2. **Types of data or response to question:** (Reference code: Current Job)

2.1.2.1. The participants description of their job

2.1.2.2. Information regarding their organization (Name, Size, customers, location, etc.)

2.1.2.3. Years within that role and with the organization (if not already stated)

2.1.2.4. Day-to-day responsibilities

2.1.2.5. How RC/SSC is part of their job (if not already stated) (Reference code: Current Job or CompliancePerception or ComplianceMGT)

2.1.2.6. Their involvement in their organization's development process (Reference code: Current Job or DevProcess)

2.2. Follow-on: How long have you been doing this? (If not already stated.)

2.2.1. **A presentation of the rationale:**

2.2.1.1. This is a follow-on question. If certain data has not been given in answers to previous questions, we ask these follow-ons to ensure we get the data needed for analysis.

2.2.1.2. To understand how long a person as been with a particular organization can speak to how well they know their organization and their organization's processes with software development.

2.2.1.3. Based on how long they have been with the organization, either certain initial impressions about their organization's development processes and their compliance processes can be ascertained or the participant can provide more first-hand accounts or experiences about their organization's development processes and their compliance processes. Meaning a new person with less than a years' worth of on-the-job experience might not have any first-hand accounts or experience in dealing with RC/SSC and their organization's Software Development Process versus someone with 5 to 10 years' worth of experience; however, a new person can provide initial impression and thoughts of how an organization is setup to assess and advise on RC/SSC.

2.2.2. **Types of data or response to question:** (Reference code: Current Job)

2.2.2.1. Years with the organization

2.2.2.2. Further description about their job and their organization

2.3. What are your organization's mission and goals?

2.3.1. **A presentation of the rationale:**

2.3.1.1. We ask this question to understand the participants environment in which they are working in. The participants perceptions on RC/SSC are greatly influenced by the organization in which they work in, so having a baseline understanding of their organization's priorities helps the researcher understand the participants perceptions in context.

2.3.1.2. We want to get a better sense of their customer base and how their customers affect their mission and goals. For example, an organization supporting a healthcare network will have different priorities and perspectives on compliance versus an organization that finances or general customer data.

2.3.1.3. Some of these organizations either support multiple regulated domains (i.e., they have different sectors of the company that have different compliance requirements) or they support a general customer based and therefore have to priorities or make decisions on which part of the Software development market they compete in.

2.3.2. **Types of data or response to question:** (Reference code: Current Job)

2.3.2.1. Organization's name and size

2.3.2.2. Organization's sector (i.e., healthcare, finance, government, data analytics, etc.)

2.3.2.3. Organization's priorities (e.g., requirements or their niche in the Software Industry)

2.3.2.4. Organization's Products (IOW participants might describe the products they release commercially and/or develop and use internally)

2.3.2.5. Organization's customer base (customer demographic and/or who they support)

2.3.2.6. Whether the organization develops products from the ground up, do they build custom solutions using commercial off-the-shelf (COTS) products, or do they assess software or systems.

2.4. Clarifying questions: Does your organization/the organization you advise, develop, or evaluate software or systems? (If not already stated)

2.4.1. Probes: Who do you work for, i.e., who do you advise?

2.4.2. Probe: What is their expertise?

2.4.3. **A presentation of the rationale:**

2.4.3.1. This is a clarifying question because some organizations do not develop their own in-house software (i.e., they integrate or they build custom solutions using commercial off-the-shelf (COTS) products as a baseline), but they still have a development process and requirements for compliance.

2.4.3.2. We ask this question to clarify, if not described in a previous question, organization's development process and how involved the participant and the organization is within that process

2.4.3.2.1. Do they develop?

2.4.3.2.2. Are they just customers build a system or network with COTS products?

2.4.3.2.3. Are they consultant (meaning they advise customers on compliance and what must be done to demonstrate compliance)?

2.4.3.2.4. Are they a combination of the three previously described?

2.4.4. **Types of data or response to question:** (Reference code: Current Job OR DevProcess -> DefProcess or NoDefProcess)

2.4.4.1. Types of products the organization develops and uses to answer the following questions:

2.4.4.1.1. Do they develop or they customers with compliance requirements?

2.4.4.1.2. Do they consult on compliance or are they consulted?

2.4.4.1.3. Do they build systems or network using in-house developed products, COTS products, or both?

2.4.4.2. Their level of involvement in the Software Development Process (SDP)

2.4.4.3. Whether the organization develops products from the ground up, do they build custom solutions using commercial off-the-shelf (COTS) products, or do they assess software or systems.

3. Participant's experience with the SDLC

3.1. What is your experience with the software/system development process?

3.1.1. Probe: What is the software or system development process that you or your organization typically uses?

3.1.2. **A presentation of the rationale:**

3.1.2.1. We ask this question to understand the participants background with software development and what methods they current and previously used to assess or develop software.

3.1.2.2. Part of the purpose of this study is to understand adherence to compliance as part of the software development process, so we need an understanding of the participants software development process to understand how compliance is achieved as part of that process.

3.1.3. **Types of data or response to question:** (Reference code: DevProcess -> DefProcess or DEVDecision)

3.1.3.1. Confirmation that they use a Software Development Method or Process

3.1.3.2. Participants prefer and/or current Software development method (IOW, do they use Scrum, Waterfall, Agile, DevOPS, Test Driven, etc.)

3.1.3.3. Description of their Software development methodology

3.1.3.4. Explanation of why they use or prefer their particular methodology?)

3.1.3.5. Participants history with Software Development Process (IOW, what methods they have used in the past)

3.2. Follow-on: Why do you/ your organization use that process?

3.2.1. **A presentation of the rationale:**

3.2.1.1. This is a follow-on if the participant answers with a short answer with no description of their process.

3.2.1.2. Different development techniques offer different advantages and disadvantages. Part of asking why gives the participant an opportunity to describe in their own words those benefits and challenges.

3.2.1.3. How they use development advantages to their own benefits or overcome the shortfalls of their chosen software development process (SDP) challenges.

3.2.2. **Types of data or response to question:** (Reference code: DevProcess -> DEVDecision)

3.2.2.1. Benefits to them or the organization using a particular SDP.

3.2.2.2. Challenges to them or the organization using a particular SDP.

3.2.2.3. Modification they may use in practice with their SDP.

3.3. How involved are you in this process? (Meaning involved in the beginning as a key stakeholder required to provide requirements, brought in during implementation to evaluate the software for security compliance, etc.)

3.3.1. **A presentation of the rationale:**

3.3.1.1. We asked this question because not all Software Practitioners are developers or involved in every step of the SDP.

3.3.1.1.1. Some are managers or stakeholders with a need to see a particular requirement fulfilled.

3.3.1.1.2. An example is a stakeholder that is a privacy engineers would be concern with ensuring required privacy requirement, if applicable, under HIPAA, GLBA, Privacy Shield or GDPR are being met. They would need to document and analysis evidence of compliance or raise issue with appropriate organization leads if they are not being met.

3.3.2. **Types of data or response to question:** (Reference code: ReqMGT -> ReqStakeholder or ReqCommunication OR DevProcess ->DEVDecision)

3.3.2.1. Further description of the participants role and responsibilities as part of their organizations SDP.

3.3.2.2. Description of their level of involvement with their organizations SDP.

3.3.2.3. Examples of their involvement in their organizations SDP.

3.4. Follow-on: Can you give some examples?

3.4.1.**A presentation of the rationale:**

3.4.1.1. This is a follow-on questions to the previous one that is asked if examples are not given in the previous answers.

3.4.1.2. We chose to conduct an interview study to gather rich, contextual, qualitative data on the topic of Compliance as part of the SDP. Examples from participant's stories and accounts give us the context needed to analysis the participant's unique viewpoint.

3.4.2. **Types of data or response to question:** (Reference code: ReqMGT -> ReqStakeholder or ReqCommunication OR DevProcess ->DEVDecision)

3.4.2.1. Further description of the participants role and responsibilities as part of their organizations SDP using participant's example or user story.

3.4.2.2. Description of their level of involvement with their organizations SDP using participant's example or user story.

3.4.2.3. Examples of their involvement in their organizations SDP using participant's example or user story.

3.5. Have you ever deviated from your software development process?

3.5.1. **A presentation of the rationale:**

3.5.1.1. This is a setup question to the next question as to why they deviate from their Software Development Process.

3.5.1.2. We asked this question, because we as researchers know that that it is rare that everyone follows the rigors of a particular SDP every single time. The reason is that things that can and do affect the SDP change. These things include but not limited to people, budget, requirements (functional and non-functional), and timelines.

3.5.1.3. This question is also an indicator on the participants level of experience. Software practitioners that have been part of the industry for a while, know response to change and deviation is part of working within any industry.

3.5.1.4. If the participant goes beyond a yes or no response and describe why, we are also looking for trending factors as to why a team or developer might deviate from their or their organization's established SDP.

3.5.2. **Types of data or response to question:** (Reference code: DevProcess -> DEVDecision)

3.5.2.1. Yes or No response

3.5.2.2. Description (IOW reasoning) of why they deviate from an SDP. Example: Response to a change or limitation of a resource

3.6. Follow on: A presentation of the rationale: (i.e. what decision factors or influences might have warranted a break from the traditional process?)

3.6.1. Probe: If participant does not provide an example, ask if they can provide one.

3.6.2. **A presentation of the rationale:**

3.6.2.1. This is follow-on from the previous question:

3.6.2.1.1. If the participant only answers with a Yes/No response and provides no further description.

3.6.2.1.2. To get the participant to provide an example or user story if they can.

3.6.2.2. We also ask to get the user to describe how the deviation occurs. What trade offs do they make? For example, if the limitation is time, meaning one part of the development phase took longer then another, but the deadline for delivery cannot change, then do they reduce the time in another phase, such as testing or the pre-production release process, to make up for that lost time.

3.6.3. **Types of data or response to question:** (Reference code: DevProcess -> DEVDecision)

3.6.3.1. Description of factors that might cause a deviation:

3.6.3.1.1. Internal factors: Personnel changeover, limitation on budget or time, testing resource (testers or testing labs) availability.

3.6.3.1.2. External factors: Requirements change by customer or external third-party vendor.

3.6.3.1.3. Combination of both

3.6.3.2. How they execute the deviation

4. Participant's experience with Regulatory or Security Standard Compliance

4.1. **Segway: Describe why these questions are important or define Regulatory or security compliance RC/SC)**

4.1.1. Definition of RC/SC - a software organization's ability to show that they have taken steps throughout the lifecycle to apply due diligence to assess the current meaning of applicable regulations and to ensure that meaning is implemented in specific functions of the software product.

4.1.2. **A presentation of the rationale:**

4.1.2.1. This is a note to ourselves to describe the transition into the regulatory and security standard compliance questions of the interview study.

4.1.2.2. We start here after the SDLC section to get the participants into the mindset of their SDP.

4.1.2.3. We are now circling back to the topic of RC/SSC as part of the SDP.

4.1.3. **Types of data or response to question:** No response, just a conversation starter to set the tone for this section's questions.

4.2. As a PM/SW Developer in the field of _____(i.e. medical, safety, automotive, government, financial…), I'm sure there is regulations or security standards you have to comply with. Can you give me brief description of what those standards and regulations are?

4.2.1. **A presentation of the rationale:**

4.2.1.1. We ask this question to get sense of the participants awareness of their Regulatory and Security Standard requirements.

4.2.1.2. In addition, some regulations and standards have been around for a minute while others are newer. Therefore, depending on what domain they work in (i.e., Healthcare, Government, Finance, Data, Acquisition, etc.) the maturity and stabilization of a particular regulated domain could affect their awareness and response to their Regulatory and Security Standard requirements.

4.2.2. **Types of data or response to question:** (Reference code: ComplianceMGT -> ComplianceReq or ComplianceCommunication OR ReqMGT -> ReqSource or ReqGathering or ReqCommunication)

4.2.2.1. General regulations pertaining to their domain.

4.2.2.1.1. Healthcare – HIPAA/Health Information Exchange

4.2.2.1.2. Data – GDPR/Privacy Shield/CCPA/Schremms II decision

4.2.2.1.3. Finance - PCI-DSS/GLBA

4.3. Follow on: Why those standards?

4.3.1. Probe: How did you identify those Regulatory or Security Compliance Standards?

4.3.2. **A presentation of the rationale:**

4.3.2.1. This is a follow-on to the previous question.

4.3.2.2. Referring to the previous question, we asked this to get a sense of why those standards are most important and how they are identified and learned.

4.3.2.3. This question helps with the follow-on discussion on compliance communication within the Software industry.

4.3.3. **Types of data or response to question:** (Reference code: ComplianceMGT -> ComplianceReq or ComplianceCommunication OR ReqMGT -> ReqSource or ReqGathering or ReqCommunication)

4.3.3.1. Description of internal organizational policies and procedures associated with RC/SSC.

4.3.3.2. Description of organizational training and/or certification requirements.

4.3.3.3. Description of contractual obligations with customers, third party vendors, or contractors within the organization.

4.4. When does regulatory or security compliance fit in your organization software development process? Looking at what phase of the SDLC.

4.4.1. **A presentation of the rationale:**

4.4.1.1. One objective of this study is to get a sense of when and where RC/SSC is applied and assessed within the SDLC. This question is asked to support that purpose and to see if there are some trending answers amongst the participants for further analysis and future work.

4.4.2. **Types of data or response to question:** (Reference code: DevProcess OR ComplianceMGT -> ComplianceWhen)

4.4.2.1. A description of when and where RC/SSC is applied and assessed within their Software Development Process (SDP).

4.4.2.2. Further description of the participant's RC/SSC entire process as part of their SDP.

4.4.2.3. References to Software Development phases.

4.5. How do you track and manage compliance? (Examples from current or previous projects would be great)

4.5.1. Probe: Are there any tools/frameworks you use? Why?

4.5.2. Probe: Frequency? Why?

4.5.3. **A presentation of the rationale:**

4.5.3.1. This question is asked to see if tracking changes to the RC landscape is part of the participant's business or requirements process.

4.5.3.2. This question also gives a sense of how involved or aware participants are of RC/SSC changes occurring. For certain roles, like Data and Privacy Engineer or

Product Managers tracking changes within the RC landscape is expected; however, Software Developers might not be as aware.

4.5.3.3. This question is also an opportunity to see what trending tool Software practitioners are using to track and manage requirements pushed to them from other stakeholders or entities. One of the goals and future work of our research is to build a framework/tool to help track and manage compliance.

4.5.4. **Types of data or response to question:** (Reference code: ComplianceMGT -> ComplianceAssessment or ComplianceTracking or ComplianceReq OR ReqMGT -> ReqPrioritzation or ReqChangeMGT)

4.5.4.1. Requirements Tracking process

4.5.4.2. Stakeholders responsible for tracking and managing compliance.

4.5.4.3. Requirements track and management tools.

4.6. After the release of the software or system, have you had to re-evaluate Regulatory or Security Compliance Standards against the software/system?

4.6.1. Yes or No Response

4.6.1.1. If so, how often?

4.6.1.2. If no, why not?

4.6.2. **A presentation of the rationale:**

4.6.2.1. Software must be maintained, and maintenance includes addressing/integrating new changes or requirements. Also, when a RC/SSC changes, software organization must reassess and document compliance and make changes to the requirement. We asked this question to first see if re-evaluation of product or product lines are happening and how-often. But also, to get a sense of what that process looks like and impacts when and if it occurs,

4.6.3. **Types of data or response to question:** (Reference code: ReqMGT -> ReqChangeMGT OR ComplianceMGT ->ComplianceAssessment or ComplianceTracking or ComplianceReq)

4.6.3.1. Yes/No response

4.6.3.2. Yes – Follow on: Frequency (Annually, Bi-annually, monthly, whenever an update to a release)

4.6.3.3. No:

4.6.3.3.1. Evaluation of RC/SSC is part of pre-product process or release process which occurs every 4-6 months as part of the SDP.

4.6.3.3.2. No requirement for compliance

4.7. Have you ever had any issues or challenges in complying with a Regulatory or Security Standard?

4.7.1. Yes or No Response

4.7.1.1. If yes, can you provide some details

4.7.1.2. If no, probe

4.7.1.2.1. Have you ever had a regulation or security standard change, which ended up making software that you have already deployed out of compliance?

4.7.1.2.1.1. If yes,

4.7.1.2.1.2. What did you do?

4.7.1.2.2. Have you had any internal challenges or issues working with compliance teams, security teams, or legal teams when trying to meet a compliance requirement?

4.7.1.2.2.1. If yes,

4.7.1.2.2.2. What did you do?

4.7.2. **A presentation of the rationale:**

4.7.2.1. This question is a setup for the next question on technical debt.

4.7.2.2. We ask this question to understand if the participants experience any impacts or issues with RC/SSC.

4.7.3. **Types of data or response to question:** (Reference code: CompliancePerceptions -> ComplianceChallenges or Technical Debt)

4.7.3.1. Stories or examples responding to RC/SSC or a change in the compliance landscape to include, but not limited to:

4.7.3.1.1. Technical Issues

4.7.3.1.2. Internal communication or interpretation of regulation issues

4.7.3.1.3. Vetting requirements with external parties such as third-party vendors, contractors, or customers.

4.7.3.1.4. Auditors review and assessment with compliance.

4.8. Follow-on: Would you consider it a form of technical debt?

4.8.1. Rephrase or clarification to the question: Have you ever had a known issue related to compliance that might not have been addressed prior to software package release, that you had to address after release?

4.8.2. **A presentation of the rationale:**

4.8.2.1. Technical Debt is a topic we associate and is relevant to the topic of RC/SSC because when a change happens within the compliance landscape, organizations are required to respond within the sector the regulation affects.

4.8.2.2. We asked this question to explore the relationship of RC/SSC and technical debt.

4.8.2.3. Originally, Technical Debt was its own section in the interview guide, but during pilot testing the topic of Technical Debt took over the interview and took up much more time and focus then originally intended for this interview study.

4.8.2.4. Note for Future Work: If we were to expand this interview study into a survey, it might be worth exploring a separate paper on the relationship of Technical Debt and Regulatory Compliance as a separate research paper.

4.8.3. **Types of data or response to question:** (Reference code: Technical Debt)

4.8.3.1. Yes or No Response

4.8.3.1.1. If yes

4.8.3.1.1.1. The effects it might have had on developing other functional requirements.

4.8.3.1.1.2. Decisions were made to delay RC/SSC implementation in favor of a product release (i.e., be first to market) or until a better understanding of the regulation allowed us to comply better with the intent of the regulation or law.

4.8.3.1.2. No

4.8.3.1.2.1. We have no examples regarding technical debt and RC/SSC that come to mind, or we are allowed to disclose.

4.8.3.1.2.2. Technical Debt is a choice to delay action or workaround addressing a requirement and deal with after a products release. Changes within the RC landscape that are reacted to are hardly a choice

4.8.3.1.3. Maybe – Depends on the impact

4.8.3.1.3.1. What the change means?

4.8.3.1.3.2. Whether if it is a minor delay or major restructure?

4.8.3.1.3.3. If there is a history of implementation that we can use as a outline for implementation such as a industry best practice we can point to for compliance?

4.8.3.1.4. Rather not say due to confidentiality issues or its not my first-hand account.

4.9. Follow-on: Did and how did you track such changes (through configuration or knowledge management or another form of documentation tracking)

4.9.1. **A presentation of the rationale:**

4.9.1.1. This is similar to question "4.5" within this section and a follow-on to the previous question.

4.9.1.2. We asked this to get a sense how the participant and/or their organization track and manages workarounds, code smell or any minor/major changes within the code to manage or track Technical Debt and RC/SSC.

4.9.1.3. This question is also an opportunity to see what trending tool Software practitioners are using to track and manage requirements pushed to them from other stakeholders or entities. One of the goals and future work of our research is to build a framework/tool to help track and manage compliance.

4.9.2. **Types of data or response to question:** (Reference code: ComplianceMGT -> ComplianceAssessment or ComplianceTracking or ComplianceReq OR ReqMGT -> ReqPrioritzation or ReqChangeMGT)

4.9.2.1. Requirements Tracking process

4.9.2.2. Stakeholders responsible for tracking and managing compliance.

4.9.2.3. Requirements track and management tools.

4.10. Follow-on to 4.7: We have asked if you experienced and challenges of issues in complying with Regulation or Security Standards, have there been benefits with having RC/SSC as part of your organization's or your SDP process?

4.10.1. Alternative wording: Have you experiences benefits with your organization's compliance program?

4.10.2. **A presentation of the rationale:**

4.10.2.1. We flip the challenges to compliance question to give the participant a chance to highlight some of the good that has come from their organizational compliance program or RC/SSC in general.

4.10.2.2. In case the participant has been hesitant to open about their SDP or Compliance processes for fear of a negative interpretation, this question might open them up more about their SDP and Compliance processes.

4.10.2.3. When doing a interview study, it's also good to maintain a neutral tone so not to introduce some bias into the data. This question helps to balance some of the other questions asked.

4.10.3. **Types of data or response to question:** (Reference code: CompliancePerceptions -> ComplianceBenefits)

4.10.3.1. Description of the participant's organizations compliance program or culture.

4.10.3.2. If they perceive some personal benefits to RC/SSC.

4.11. **Current events questions**:

4.11.1. **A presentation of the rationale:**

4.11.1.1. These questions were asked because of the current events happening at the time of the interviews from Nov 2020 to Jan 2021. (i.e., Change of President Administration, COVID-19 Pandemic, Schremms II decision in July 2020, Zoom's Regulatory infractions, SolarWinds incident, etc.)

4.11.2. COVID-19:

4.11.2.1. Has COVID-19 had any impact to your organization business or processes regarding RC/SSC?

4.11.2.2. Has COVID-19 had any impact on your own processes regarding RC/SSC?

4.11.2.3. **A presentation of the rationale:**

4.11.2.3.1. Background: COVID-19 has impacted the Software Industry and Regulated sectors. While some business, like Zoom, have exploded, other business have imploded, like the entire restaurant industry because no one was going out to eat. Other software businesses had to pivot rapidly, like Uber, which changed focuses from ridesharing to delivery of commodities.

4.11.2.3.2. These questions were asked to see if pandemic has added to or had any impact of the Software Industry regarding RC/SSC.

4.11.2.4. **Types of data or response to question:** (Reference code: Recent Event -> COVID)

4.11.2.4.1. Description of how COVID may have affected the participant's job or their organization.

4.11.3. Change in administration: With the new administration, do you or your organization anticipate some changes regarding RC/SSC?

4.11.3.1. **A presentation of the rationale:**

4.11.3.1.1. Background: During the Clinton Administration HIPAA went into effect. During the Obama administration the HITECH Act and HIE (Health Information Exchange) went into effect. These interviews happened between Nov 2020 and Jan 2021. Perhaps more important, the focus of executive branch agencies (e.g., HHS, FTC, FAA, etc.) is dictated by the President. A change in leadership can mean a change in enforcement on the ground for our participants or their businesses. Some in the Software Community might have thoughts or opinions of what new changes a new Administration might bring to the Compliance Landscape.

4.11.3.1.2.

These questions were asked to see if there was any anticipation of changes regarding RC/SSC based on the new administration platform.

4.11.3.2. **Types of data or response to question:** (Reference code: Recent Event -> Presidential Election)

4.11.3.2.1. Description of how a change in the Presidential Administration may have affected the participant's job or their organization.

4.11.4. Are there any recent changes might have had some regulatory or security standard compliance effects on the software or the organization?

4.11.4.1. Clarification: Have any recent regulatory changes or infractions occurred that may have affected the compliance landscape you or your organization is tracking?

4.11.4.2. Clarification: Have any recent regulatory changes or infractions that may have affected your compliance process or your organization's compliance process within your software development process?

4.11.4.3. Regulation changes:

4.11.4.3.1. **A presentation of the rationale:**

4.11.4.3.1.1. Any change to the Compliance Landscape usually requires a response and may impact an organization both internally with shift in resources to respond to the new requirements to externally with organizations having to respond to customers concerns or new requirements. We ask this question to see if recent regulatory changes have had some impact or change within the participant's organization or their own processes toward SDP.

4.11.4.3.2. **Types of data or response to question:** (Reference code: Recent Events -> Regulation Changes)

4.11.4.3.2.1. Describes how recent regulatory decision (i.e., GDPR, Schremms II - EU Court decisions) may have impacted your processes.

4.11.4.4. Regulatory Infractions:

4.11.4.5. **A presentation of the rationale:**

4.11.4.5.1. Any enforceable infraction helps to further define regulation and what is required to comply to it. We ask this question to see if recent regulatory infractions have had some impact or change within the participant's organization or their own processes toward SDP.

4.11.4.6. **Types of data or response to question:** (Reference code: Recent Events -> Regulatory Infraction)

4.11.4.6.1. - Describe if any regulatory infractions (i.e., Zoom) may have impacted your business

4.12. List of questions asked near the end of the interview based on the participants' job role and/or background. NOTE: These could be asked before the next two questions or afterwards and one or two questions were asked during the interview.

4.12.1. Based on your experience having worked with or within _______ (Fillers are legacy systems, healthcare, finance, Government contracting or sector, Data industry), what would be something that you would like to see done that, as far as RC/SSC researcher is concerns, that could benefit the Software Development Industry?

4.12.2. If you had one wish for your organization or the Software Industry regarding RC/SSC, what would it be?

4.12.3. Do you have any closing words or tidbits of wisdom to share about the Software Industry and RC/SSC?

4.12.4. If you could go back and talk to a younger version, what would you say to you?

4.12.5. Do you have any thoughts or how to either improve the science or technical expertise on the regulatory side (i.e., the creation of regulation) that might change your perspective on regulatory compliance endeavors?

4.12.6. **A presentation of the rationale:**

4.12.6.1. These are closer questions in the hopes of opening the discussion on RC/SSC that were not previously covered.

4.12.6.2. These kinds of questions help to get some out of the box discussion on topic not previously covered.

4.12.7. **Types of data or response to question:** (Reference code: Wishes)

4.12.7.1. A little more perspective from the participant on the focus of the study

4.13. Is there anything about your views or experiences with applying or evaluating Regulatory or Security Compliance Standards that you would like to add?

4.13.1. **A presentation of the rationale:**

4.13.1.1. This question is an end-of-interview question to allow the participant to add any final thoughts or experience regarding RC/SSC.

4.13.2. **Types of data or response to question:** (Reference code: Any code is applicable based on content given)

4.13.2.1. A little more perspective from the participant on the focus of the study

5. Summary

5.1. Is there anything I should have asked but didn't?

5.1.1. **A presentation of the rationale:**

5.1.1.1. This question is an end-of-interview question to allow the participant to give feedback on the interview study.

5.1.2. **Types of data or response to question:** (Reference code: No corresponding code)

5.1.2.1. Feedback on the Interview Study

5.2. Can you recommend anyone else that would be a source of this topic?

5.2.1. **A presentation of the rationale:**

5.2.1.1. This question is for recruitment of additional interview candidates.

5.2.2. **Types of data or response to question:** (Reference code: No corresponding code)

5.2.2.1. Additional contacts to recruit for the interview study

Thank you for your time!

References

[1] Ponemon Institute LLC; Globalscape, "The true cost of compliance with data protection regulations," December 2017. [Online]. Available: https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study.

[2] E. Kempe and A. K. Massey, “Regulatory and Security Standard Compliance Throughout the Software Development Lifecycle,” in Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS-54), Manoa, 2021.

[3] E. Kempe and A. K. Massey, "Perspectives on Compliance Requirements in Software Engineering," in *29th IEEE International Requirements Engineering Conference (RE '21)*, Notre Dame, 2021.

[4] S. B. Merriam, and E. J. Tisdell, “Qualitative research: A guide to design and implementation,” John Wiley & Sons, 2015.

[5] E. Lim, N. Taksande and C. Seaman, "A Balancing Act: What Software Practitioners Have to Say about Technical Debt," in IEEE Software, vol. 29, no. 6, pp. 22-27, Nov.-Dec. 2012, doi: 10.1109/MS.2012.130.