SureCloud.

technology leaders club

Optimizing IT Compliance

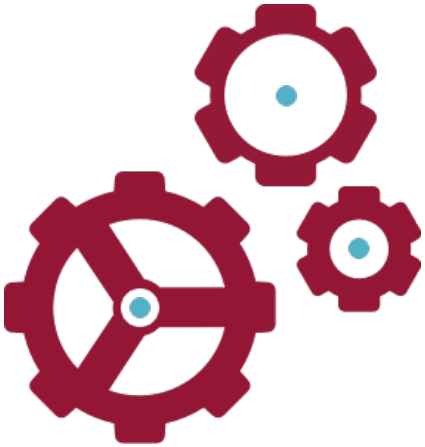
Real-world lessons in embedding and scaling an optimized IT compliance program

SureCloud – ebook 2021

Introduction

Satisfying the thousands of information security, IT and data privacy requirements that make up today's complex regulatory landscape is an ongoing challenge. Sustaining IT compliance programs can be complicated, expensive and time-consuming. As the volume of regulations increases and existing requirements change, it becomes harder to map controls to requirements at scale. Effort can be duplicated across departments and silos. Defining responsibility and enforcing accountability is challenging. And you need to be confident that the outcome delivers what the wider organization expects

We brought together a number of senior compliance and security professionals to share their thoughts, ideas and experiences about these challenges at a series of roundtables. This ebook captures the main points of our conversations.



Our contributors?

The professionals joining us at the roundtables hosted and moderated by Rela8 Group's Technology Leaders Club included:

VP Information Security at a major U.S. financial services company with $1.9 trillion in assets

Senior Director of Security for a technology-driven biopharmaceutical solutions company

Chief Architect of an insurance company with 1.9 million members

Senior IT Security Manager at a $90 billion revenue retail giant

IT Compliance Director for a transformative IT software and services company

Director of Information Security with an AI-driven customer care solutions business

Lead Risk Manager for the world's largest building society

VP Business & Technology for a multinational universal bank with a revenue of £21.7 billion

CISO of a global leader in engineering and industrial software

Head of Security & Compliance for a trend-leading, creative retailer

CISO at a prestige automotive manufacturer

Group Cyber Security Compliance Manager for a broadcast telecoms company with over 12.7 million customers

Cyber Risk & Compliance Manager for a leisure business that hosts 4+ million people a year

CISO at an international energy company

Head of Cyber Security for a £1.5 billion turnover building materials supplier

Senior Information Security Architect at one of the world's largest consumer co-operatives

Senior Manager of Information Security with a transcontinental pharmaceuticals business

IT Security Manager for a global, multi-channel fashion retailer

Director of Cyber Security for a multinational utilities company

Senior Director of Technology Solutions for a Fortune 500 corporation with over $170 billion in total assets

InfoSec Risk Manager for a financial services giant and FTSE 100 constituent

The seven main challenges and real-world lessons for embedding and scaling an effective optimized IT compliance program

Challenge 1 How do you create a single set of controls that you can break into different views?

Challenge 2 How do you measure your compliance maturity?

Challenge 3 How do you measure the effectiveness of controls?

Challenge 4 What happens when things change?

Challenge 5 How do you align corporate risk with compliance?

Challenge 6 How do you involve the whole organization?

Challenge 7 How do you manage third-party compliance?

Challenge 8 How can compliance be leveraged to support your organization?

How do you create a single set of controls that you can break into different views?

Challenge 1:

How do you create a single set of controls that you can break into different views?

Managing and measuring compliance against different standards and regulations across different business departments needs to be optimized to avoid duplicated effort. Controls are often administered by finance or compliance teams, but it is better if they are automated into IT systems.

Real World Solution: Standardize and adapt

Standardize your controls and adapt rather than rewrite them for different areas. Take a pragmatic approach to codify and Standardize as you still need to present meaningful views.

The key is to adapt rather than rewrite and match the view of the control to the level of person looking at it. Build high level controls for senior leadership teams and gain their buy-in to make sure they are part of the process.

Include the Standardized controls in an integrated Governance Risk and Compliance platformthat is not used for anything else. This then becomes the single source of truth.

Uphold the policies in the systems that end-users are familiar with. Use hooks and automation to bring the policies into line with the automated GRC platform. By connecting it to tools that people are using, they don't have a reason not to be compliant.

Be realistic. Do not clamp everything down so much that you cannot do anything. Maximize and optimize your efforts to do what is meaningful and achievable with your resources.

Remember that regulation and standards don't necessarily make you secure. Frameworks have to be relevant and map to your business.

How do you measure your compliance maturity?

Challenge 2:

How do you measure your compliance maturity?

Compliance maturity levels vary considerably by organization, industry, and geography. All levels were represented at our roundtables; from the person who was invited to create the information security department policies from scratch on their first day, to the organization implementing a controls framework commissioned from one of the 'big four'.

Understanding where your organization is on a maturity scale underpins a lot of the decisions you will take to optimise your compliance program.

Real world solution: Use a controls framework and aim for continuous improvement

Without measurement it is hard if not impossible to show improvement. A controls framework gives you a means to measure your organization against key criteria and show where you need to focus to improve your position. The framework should be tailored to your business and be more than an audit-driven 'tick box' exercise. Whatever happens, it must not be to the exclusion of security. From a pragmatic perspective, security is every bit as important as meeting regulatory requirements.

External reviews are helpful to show a scorecard of your compliance/cyber security maturity and provide recommendations for improvement.

Wherever you are on the compliance maturity scale, improvement should be continuous. It involves frequently assessing the controls framework for its continued relevance as things change and businesses restructure. This means looking at control effectiveness and your control descriptions to make sure they still apply.

Many look to Standardized frameworks that apply to their industry or discipline. The most commonly referenced are NIST's Cybersecurity Framework and ISO-27000. There are many other different frameworks that address the challenges of different industries. Organizations should adopt a framework as a baseline and evolve it over time. Do not expect everything to be done in one year.

The Secure Controls Framework [Secure Controls Framework | Cybersecurity & Privacy Controls] is a helpful resource that lists 850 controls, rationalized and baselined across over 150 global regulations, frameworks and standards.

Click here for SureCloud's definitive guide to IT COMPLIANCE MANAGEMENT MATURITY

How do you measure the effectiveness of controls?

Challenge 3:

How do you record and report the effectiveness of controls?

Delivering tangible reports on GRC matters is an ongoing challenge. Often the effectiveness of a control is subject to interpretation and can lack objectivity. Providing accurate, timely and impactful updates to senior management is often difficult and time-consuming and can be counterproductive if there is either too much or not enough detail.

Real world solution: Use metrics that make sense

This is one of those areas where a pragmatic approach is essential. There is no point measuring things that are not appropriate. Rather than sticking rigidly to a framework, use metrics that are appropriate for your organization and your position on a maturity curve.

The metrics you use have to be appropriate for the audience you are reporting to. Use different metrics for different levels of management according to what they need to see. Senior management need less detail than control owners, for example. Choose metrics that are meaningful and show an accurate position.

Aim to get real-time metrics, if possible. Take feeds from different controls to continuously monitor compliance.

Establish what insight board members want and what metrics are meaningful to them by asking them. This can help open a discussion about risk at the high level that can trickle down to the rest of the organization.

Build the need for metrics into the controls and control descriptions. For some, this means ensuring that every control implemented has a way of being scored effectively and rated.

Challenge 4:

What happens when things change?

If there is one constant in business, it is change. Businesses change, structures change, processes change – even standards change. One of the biggest challenges is making the control owner aware of the change and what the implications are, and what action they need to take.

Real world solution: Revisit control frameworks and controls

Where responsibility for meeting standards lies in different teams, annual compliance audits can be the first time GRC or security is even aware of a change. The first thing to do is to identify what changes have happened, and that requires good channels of communication between teams.

Build workflows to help manage updates and changes to the controls directly. Include regular communication and updates within the workflows.

Revisit controls to address organizational change. For example, a cloud migration project will involve revising access controls. Many organizations have had to update their controls and framework to allow for remote working during the pandemic and introduced Identity Access Management (IAM) controls that specifically relate to the cloud.

When you are aware that there are changes in standards, revisit the controls and build on the principles you have established, but bear in mind the proportionality of where to apply them. Assess what is really at risk and where the changes apply.

Push the workflows and control changes out to the control owners so they are aware of the change. It is important to follow up to make sure that they have understood the change and have accepted it and understand what they need to do in terms of retesting or updating the language.

Challenge 5:

How do you align corporate risk and compliance?

Compliance and risk management are closely aligned. Compliance with established rules and regulations helps protect organizations from a variety of unique risks, while risk management helps protect organizations from risks that could lead to non-compliance. This can itself pose a risk to an organization.

Real world solution: Elevate the conversation

There can be a mismatch between risk directors looking at enterprise risk management (ERM) and cybersecurity – whether that sits in risk or in IT – who use risk registers to report technical controls. Multiple lines on the technical risk register may be reflected in just one or two lines on the corporate risk register.

Create an end-to-end map across the business capability, IT capability, process and software and put it into a tool that gives a 360o view of the GRC framework. This allows you to indicate the risk associated at each area and level of the business.

Taking a holistic approach means driving the business owners to understand that that they are the risk and control owners, and holding them to account.

Risk tends to be driven upwards to the board from technical security and legal teams rather than down from the board. The ideal would be a connection where risk flows up and down, but few organizations claim to be in that position. That said, it is an improving situation, particularly where security and compliance teams are having the right conversations and elevating them to the board.

For most, it is a case of having a statement that is understandable to the board. This should be along the lines of 'this is where we currently are, this is where we want (or need) to be, and this is how we get there'. Or, more realistically, 'if we do this activity with investment over future years, this is where we will be' in order to secure investment.

Set an expectation for continuous investment. Compliance is not a one-off but needs to constantly adapt as the business evolves.

Security maturity assessments, either in-house or via the right partner, can get the board more involved in the conversations around risk. External assessments often help focus executives' minds on what compliance or non-compliance means for them, rather than hearing it from security.

Challenge 6:

How do you involve the whole organization?

One of the biggest challenges is getting people to understand and contribute to GRC. To be effective, compliance, risk management and security must be grounded in the organization's purpose. They are not an end in themselves but protect the whole organization's operations and reason for existing. They should not operate in silos, but sadly many do. How do you raise the profile of compliance?

Real world solution: Change the perspective

A compliance program can be a complex web of requirements and changes. An optimized compliance program has to protect the whole organization. The responsibility for that is outside of the remit of a single individual or team. It involves every function, every department and every level within the organization.

The challenge is getting buy-in and removing the idea that compliance is handled by some remote force that imposes rules and checks, and prevents business from happening.

For some, this involves changing the way the business sees controls and control management. Business can see compliance as a 'stopper' that prevents it from implementing changes.

In fact, compliance is a way to ensure business happens in a secure way and in compliance with regulations.

Cultural change may start at the top, but it needs regular ongoing discussions throughout the business.

When change happens, there can be some frustration if there is too much emphasis on testing those changes, especially when resources are constrained. A hybrid approach involving audit and testing is helpful.

Encourage sorting out known issues outside of a testing plan. This gives the business room to sort out problems that may risk non-compliance, rather than pointing at the problem and saying 'fix this'. Speaking a non-technical language helps control owners understand why meeting requirements will help their business, and frame compliance as an enabler rather than as an enforcer.

How risk management is delivered into your organization is central to its success. Gain buy-in from the top that compliance means 'doing business securely' not preventing change or development.

How do you manage third-party compliance?

Challenge 7:

How do you manage third-party compliance?

No organization or enterprise operates in isolation. Third-party vendors are used to supply services for a number of reasons; to reduce cost and increase efficiency, to provide specialist skills, and to release internal resources.

Every organization is challenged with monitoring and managing the risk of multiple third-parties that they share confidential information with.

As the digital ecosystem grows, the increase in parties that access your systems and data means additional vulnerability and heightened risk to privacy and security.

Real world solution: Include third-parties in your compliance program

Organizations should take a holistic view and extend their compliance program to third-party vendors to ensure the whole ecosystem is compliant with regulations.

Third-Party Risk Management (TPRM) starts in earnest at the procurement and on-boarding stage but should be sustained through regular questionnaires with evidence collected to verify answers.

Keep the questionnaires up to date and remove questions and requirements that are not relevant. Research shows that the focus of someone answering due diligence assessments drops by over 40% after the first 100 questions and exponentially increases.

Organizations can take a lighter touch through a 'security as partnership' approach that allows an element of self-service.

The third-party completes pre-screening questions built into the questionnaire or tool and allows the business to make its own decisions of where to involve security.

Put accountability for third-party control in the hands of the business and/or relationship owners.

Click here for The SureCloud Platform.

How can compliance be leveraged to support your organization?

Challenge 8:

How can compliance be leveraged to support your organization?

It's not enough these days to just be compliant. Compliance can offer value to businesses, and clear communication of this is vital when it comes to getting buy-in from the key stakeholders. Currently, compliance is largely seen as a cost center – so the challenge now is bringing the IT security and compliance teams out of the shadows and demonstrating the value they offer the business as enablers, not roadblocks.

Real world solution: Reframe the risk

Compliance takes time, effort, and money – this makes it a tough sell from a business perspective outside of doing the bare minimum required by law and regulations. When promoting investment in compliance for your business, frame the discussion around risk appetite.

Compliance laws exist for a reason and falling afoul of them will cost businesses dearly.

Data breaches and cyber attacks are no longer a case of if, but when. Being caught out could cost businesses millions in fines and untold amounts in reputational damages. By approaching the discussion like this you make a clear case for ROI – do they spend on compliance, or do they lose a lot more in a data breach? It is important to identify the risks in monetary terms, this shifts the decision to being less about technology, and more about the business.

Once the stakeholders are made aware of what they have to lose and you have their investment, then you can start to discuss what they stand to gain by investing in compliance. By ensuring that compliance is built into processes and products from their inception, you save a lot of pain in re-engineering down the line, and you make your operations more receptive to new compliance regulations.

With compliance baked-in and receiving the necessary investment, platforms and tools can be utilized to promote automation, regular checks and tests, and several other good practices that would otherwise be too time-consuming to realistically manage. This allows companies to be agile and offers scalability that would otherwise be impossible, making growth and staying on top of new regulatory requirements possible.

Now not only is compliance saving money, but it's also promoting growth and supporting your organization.

In conclusion

There are as many different views and ways of implementing an effective, optimized compliance program as there are companies. It does depend on your level of maturity, the industry you are in, the attitude towards risk and many other factors. It can seem daunting if you are just setting out. Even if your program is well established, implementing changes and getting buy-in can seem just as daunting.

The key is to start small and build out. Do not try to do everything at once. And you don't have to try to do everything unaided. There are tools, services and expertise available to help.

SureCloud offers a range of GRC applications and Cyber & Risk Advisory services designed to transform the way risk management is delivered into your organization – covering strategic planning, process automation, and other business outcome focused services.

Thank you

We would like to thank everyone who participated in our roundtables. The frank and open discussions helped to shine a light on the challenges happening in the real world, and some of the solutions they have adopted to address them.

For more information about SureCloud's solutions, please contact us at sales@surecloud.com

For more information about the Technology Leaders Club round tables, please visit technologyleadersclub.com