Praise for
INVESTMENTS UNLIMITED

"This book does an amazing job of explaining how good DevOps practices can help ensure that your software is safe, secure, and auditable. I learned a lot from it, which I can't say often after reading DevOps books over the last ten years. This is a must read for any CISO or executive looking to improve the security and compliance practices in their organization."

—Ross Clanton, Chief Architect and Managing Director, American Airlines

"*Investments Unlimited* builds upon years of DevSecOps literature while firmly anchoring the principles into regulated entities like financial services. The technology fable will keep you engaged with relatable stories, conversations, and practical knowledge for you to implement at your own firm and inside your team."

—Dr. Branden R. Williams, VP IAM Strategy, Ping Identity

"Finally we have a book that can be leveraged by everyone in your organization involved in meeting security, audit, and compliance requirements. You'll be able to apply this practical guidance immediately, and I really appreciate the inclusion of all of the functions and roles required to be successful. It's a great reminder that we are all in this together!"

—Courtney Kissler, CTO, Zulily

"Today, software developers are just as much security engineers, whether they know it or not. In a unique and compelling way, *Investments Unlimited* illustrates how to safely automate security testing, audit, and compliance to help organizations move faster and safer. It's a fast and fun story that sheds light on a much needed subject: the importance of bringing security, audit, and compliance out of the shadows and into the everyday life of a developer. Security, audit, and compliance are everyone's job every day. *Investments Unlimited* joyfully brings to light that these essential functions are enabled by DevOps."

—Jim Manico, Founder and Secure Coding Educator, Manicode Security

"This book helps overcome the fear and frustration many technology organizations have with audit and compliance. The story of Investments Unlimited builds shared understanding across functions and roles in an engaging way and shows us the practical steps to make more speed, stability, and compliance a reality in our own organizations."

—**Jeff Gallimore**, CTIO, Excella

"There are countless books documenting the techniques and tooling of DevOps. But rather than a technical how-to, Investments Unlimited abstracts much of the nitty-gritty to tell the story of what a DevSecOps transformation might look like for the people and teams of an enterprise organization."

—**Maya Senen**, Sr. SRE

"This book should be required reading for every software product manager and engineer. Learn how to apply security, compliance, audit, and automated testing capabilities in your organization by reading a fictional story that does a great job relating the challenges faced daily."

—**Thomas Underhill**, JD, Director of Trust Engineering Programs, VMware

A Novel about DevOps, Security, Audit Compliance, and Thriving in the Digital Age

INVESTMENTS UNLIMITED

By

Helen Beal
Bill Bensing
Jason Cox
Michael Edenzon
Tapabrata Pal
Caleb Queern
John Rzeszotarski
Andres Vega
John Willis

IT Revolution
Portland, Oregon

25 NW 23rd Pl, Suite 6314
Portland, OR 97210

First Edition
Printed in the United States of America

27 26 25 24 23 22 1 2 3 4 5 6 7 8 9 10

Cover and book design by Devon Smith

Library of Congress Control Number: 2022935846

ISBN: 9781950508532
eBook ISBN: 9781950508549
Web PDF ISBN: 9781950508563

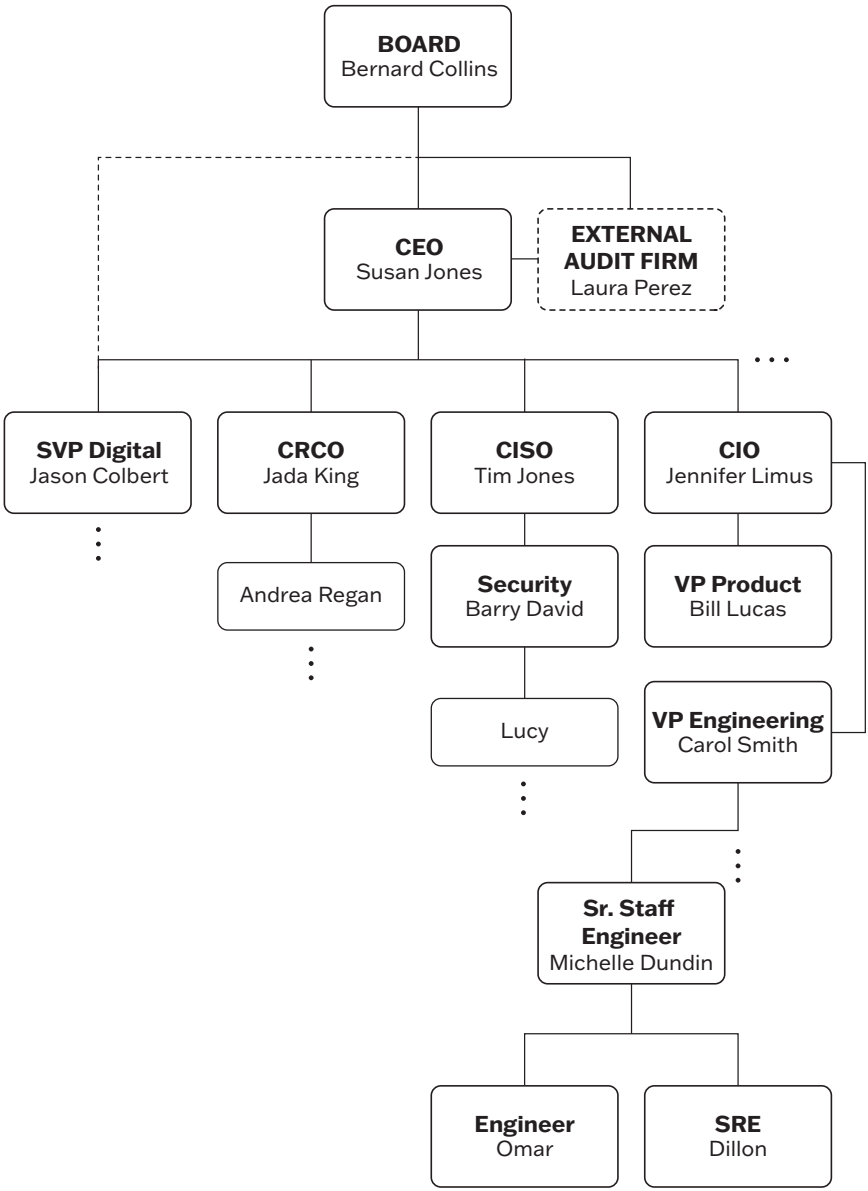
This is a work of fiction. Names, characters, and businesses are the products of the authors' imaginations. Any resemblance to actual persons, living or dead, or actual businesses is purely coincidental. However, certain real long-standing institutions, agencies, and public offices are mentioned. The events in this book are fictional but inspired by many real-life events.

For information about special discounts for bulk purchases or for information on booking authors for an event, please visit our website at www.ITRevolution.com.

INVESTMENTS UNLIMITED

To all those change agents in every organization
who dare to challenge the status quo,
build bridges instead of walls,
and propel us into the unlimited future.

CONTENTS


BOARD
Bernard Collins
CEO
Susan Jones
EXTERNAL AUDIT FIRM
Laura Perez
SVP Digital
Jason Colbert
CRCO
Jada King
CISO
Tim Jones
CIO
Jennifer Limus
Andrea Regan
Security
Barry David
VP Product
Bill Lucas
Lucy
VP Engineering
Carol Smith
Sr. Staff Engineer
Michelle Dundin
Engineer
Omar
SRE
Dillon

INVESTMENTS UNLIMITED DIRECTORY

Bernard Collins, Chairman of the Board
Susan Jones, CEO

Jason Colbert, SVP Digital Transformation
Jada King, Chief Risk and Compliance Officer (CRCO)
Tim Jones, Chief Information Security Officer (CISO)
Jennifer Limus, SVP of Engineering and Chief Information Officer (CIO)
Bill Lucas, VP of Product
Carol Smith, VP of Engineering, Digital Banking

Michelle Dundin, Senior Staff Engineer
Barry David, Security
Andrea Regan, Audit & Risk
Omar, Staff Engineer
Dillon, Staff Site Reliability Engineer
Lucy, Security

Laura Perez, External Audit Firm

PREFACE

Governance. People have multiple reactions to that word. To some, it brings about anxiety, frustration, fear, and anger. To others, it means control, the maintenance of peace, order, and safety. Whatever reaction you may have to that word, you'll likely find that you are somehow responsible for either maintaining or complying with governance to some degree.

IT governance in the enterprise is hard. Regardless of the reaction you have to the concept itself, there is a great deal of difficulty in doing governance well. Like any process, governance seeks to provide controls to safeguard the treasures that a company holds of value, which include people, data, brands, and products. Sadly, the execution of governance in practice often creates massive friction, frustration, and failure for the teams attempting to deliver value for their organizations.

This book tells the story of Investments Unlimited, Inc. (IUI), a fictional company in the financial sector. But the same tale can be told about any industry or enterprise that deals with governance.

The goal of this book is to help enterprises radically rethink governance and how software is built inside the enterprise. By introducing concepts, tools, and ideas to reimagine governance, we seek to catalyze a more humane way to enable high-velocity software delivery that inspires trust and is inherently more secure.

As you travel through this narrative, we hope you pick up modern ways to view, deploy, use, and survive governance in a fun way that helps deliver organizational objectives. Ultimately, what you take away will make it easier for you to deliver business value better, faster, safer, and happier.

—The Authors

PRELUDE

"Dad? Bad news."

The rain against the government office window on the gray New England afternoon had gotten so strong that Greg Dorshaw had to ask his teenage daughter to repeat herself. His old flip phone was getting harder to hear.

"Dad, they called off the game because of the weather. You don't need to come. Drive safely on your way home."

Dorshaw never missed his daughter's softball games. This week, the wet Boston weather had given the Supervisory Officer an excuse to stay late in the office and dig into a curious email he had received from his team earlier that day.

Eager for some quiet time to focus, he turned off the fluorescent lights in his Federal Reserve Board office, poked at what remained of his takeout Pad Thai, and focused on the email. With his face lit only by the light of the monitor, he read:

> **Subject Line: IUI preliminary examination results**
>
> Greg, looks like history is repeating itself. Seems like another fintech firm is going to require a formal action.
>
> The team is quite concerned . . .

CHAPTER 1

Monday, March 28th

Susan Jones had been the CEO of Investments Unlimited, Inc. (IUI), for five years. She was quick on her feet and always appeared to ask the right questions and make the right decisions. The board trusted her. But right now—although you couldn't tell from her demeanor—she was panicking.

"How did you find out?" Susan said into the phone, nearly gasping. It was family pizza night, but she had stepped away from the kitchen to take the urgent call. Behind her the noise of her family, Rich and Lucas making Rich's famous pizza, seemed to disappear. All she could hear was the beat of her own heart and Jason, her SVP of Digital Transformation, on the phone.

"I met with Bernard this evening at our regular two-finger Scotch session. He let me know that the MRIA[1] will be issued to IUI." Jason paused. "You know, it may feel like regulators are out to get us, but they're really there to help us and help protect our customers."

"You could have fooled me," Susan replied, half under her breath. She didn't think Jason heard her as he kept talking.

"It's not uncommon for an MRIA to be informally notified through back channels so there's no surprise when it's issued. Bernard has a good relationship with the director of the regulatory agency approving the MRIA. That director reached out to Bernard as a show of good faith," Jason said.

Susan took a deep breath. She was familiar with an MRIA, a Matter Requiring Immediate Attention, but only in concept. Actually being issued one was alarming. Federal regulators only issue an MRIA when something is seriously wrong at a bank. They aren't handed out like candy. Susan had heard horror stories from other institutions, but she'd never had one issued at a bank she worked at—let alone the bank she ran.

"Do you know what the MRIA is about?" Susan asked.

---

1. For more details on MRAs (Matters Requiring Attention) and MRIAs (Matters Requiring Immediate Attention), please refer to Appendix 1.

"Yes, and it's frankly embarrassing. There are over fifteen MRAs that have been issued to IUI over the past year. We've asked for several extensions on those, but there doesn't seem to be a clear plan to close them. That's why this MRIA is being issued. Our team hasn't provided any evidence of progress, and the agency now thinks we have a huge problem."

"I see," Susan said. But really, she didn't understand at all. *How did my team let this happen?* she wondered. *How did* I *let this happen?* Her CAO (Chief Audit Officer) had repeatedly assured her that everything was in order with these MRAs. Clearly that wasn't true.

"As you know, it's a big issue," Jason said. "Just remember, you're CEO because Bernard thinks the world of you and knows you're extremely capable. I reminded him that he couldn't have retired without you. He agreed."

"Thanks for the kind words, Jason. We'll have to get the whole team together first thing in the morning to tackle how we found ourselves in such a mess. There's nothing more we can do tonight."

"Sounds good," responded Jason. "I'm sorry to interrupt your evening, but I knew you would want to know. I'll talk to you tomorrow. Have a good night."

"Yes, thanks, Jason. I'm glad you called. Good night." Susan ended the call and sat down at the dining room table. It was a long table that fit over fifteen people, and it was always made up as if there was a dinner party starting at any moment. The orderly array of dishes in front of her seemed to mock her as she processed the implications of the call with Jason. Her mind was racing for answers and solutions.

She sat there, waiting for the numbness to wear off, waiting for her thoughts to slow down to a crawl.

"Love, are you okay?" Rich asked softly as he walked out of the kitchen.

"Yes, I'm fine. Give me a minute, and I'll come in to help with the pizza," Susan replied. She could smell the old Sicilian tomato sauce recipe that Rich was cooking up. It was a favorite of his, handed down from his great-grandmother to his mother to him. She took a deep breath. The delicious aroma was like therapy. Maybe she was starting to feel better—or maybe she was just hungry. Either way, she walked into the kitchen.

As Susan looked around, all she could see was a mess. White flour covered the countertops and floors. It looked like a fresh coat of Aspen snow had covered their kitchen.

"Well, this is certainly a 'matter requiring immediate attention' if I've ever seen one," Susan said, walking over to her six-year-old son, Lucas, happily drawing smiley faces in the flour on the countertop.

"No need to meet Jason this evening?" Rich asked, bringing Susan an apron.

"Nope, the phone call did enough damage for one night," Susan responded, tying the apron on.

"Ohhhhh, did Mommy get in trouuuble?" Lucas asked as he wiped his flour-covered hands all over Susan's once-clean apron.

"Oh, Lucas," Rich reprimanded gently. "Mommy didn't get in trouble. There's just a problem at her work. But she'll fix it. That's why she's the boss," Rich said with a smile toward his wife. He placed a big round of pizza dough on the counter in front of them. Flour flew up into the air, and Lucas laughed.

"What kind of problem?" Lucas asked as Susan spread sauce over the dough. "Did you talk while your boss was talking? Or break a rule? 'Cause Xian broke a rule at recess today, and he had to sit for the rest of recess and not play at all."

"No, I didn't break a rule," Susan said. "There's just some housecleaning at work that hasn't been getting done like it should. And now we have a whole lot of cleaning to do in a short amount of time."

"Is it like when Grandma comes for a visit and you get all crazy?" Lucas asked, dramatically flinging his arms around.

Rich stifled a laugh and turned to grab the toppings.

"No, no. It's more like when I ask you to clean your room. That's like an MRA—what we call a Matter Requiring Attention," Susan said, adopting her most serious movie-trailer voice.

"I hate when you tell me to clean my room."

"Yes, well, what's happened is we've been asked to clean our room lots of times, but apparently no one has done it, or at least not very well, so now we have to deal with a MR-*I*-A, a Matter Requiring *Immediate* Attention."

Lucas's eyes widened.

"Think of it like you're on your last warning and you're about to get a time out," Rich added. "Or get sent to the principal's office."

"Wow. Mommy really *did* get in trouble," Lucas said. Then he reached for a huge handful of mozzarella and dropped it in the center of the pizza.

Susan suddenly realized she needed to inform her leadership team and set aside time tomorrow for assessing the situation.

"Rich, give me about five minutes before we top the pizzas. I need to do one last thing."

Susan hurried back into the dining room and fired off a quick message to her senior staff using the inter-office chat system.

"Sorry to break into your evening, everyone, but this news can't wait. Jason and I were informed of an MRIA coming our way. Please do what you can to clear your schedules between 10 and 2 tomorrow. We have a lot of work to do."

She pressed send and walked back into the kitchen.

Susan settled into her side of the bed as Rich pulled up the latest episode of the comfort TV show they were watching these days.

"So, you've got quite a firestorm to settle at the office, huh?" Rich asked.

"Yes. An MRIA is no joke," Susan explained.

"If I recall correctly, isn't the next step some type of formal action by the regulators?" asked Rich.

"Yes, it is. Something like that would have a devastating impact on IUI and everyone who works there. No doubt it could end Bernard's time as chairman, finish my career, and tarnish me for the rest of my working life. If it gets to that point, there are many companies looking to purchase our assets in a fire sale." Susan frowned as she said all of this.

"You'll figure it out. They didn't make you CEO for nothing." Rich clicked the button on the remote and started the show.

Susan's mind wandered. She reflected back on how IUI had started fifteen years ago as a small company in a crowded industry clamoring for business. Like those nearby research centers, they sought to discover new ways to deliver investment and banking value to the world. She remembered the lean years where they struggled to get by.

In just the past twelve years, this small but big-hearted company had managed to not only survive but also thrive with its winning strategy of focusing on socially responsible investing. This differentiator resonated in the market and soon began to pay off. Three years later, the one hundred–person firm had expanded to a thousand employees and just topped $400 million in revenue and total assets of $20 billion. Things were looking pretty good.

They had also recently begun a digital transformation utilizing the business-accelerating principles of Agile and DevOps. Jason had been hired to help with this. He was given the charter to take intuitive digital products to the next level. He had a bold vision. He wanted to completely redesign the user experience, making complex financial transactions and products approachable, easy, safe, and reliable. He was doing all of this while helping their teams adopt more modern and Agile ways of working. The first releases of these intuitive tools or digital products proved to be way better than expected. Feedback from customers was astounding and conversion rates for new accounts were growing faster than ever. It felt like the next voyage of IUI was just about to set sail!

But now things were looking a little more like a sinking ship.

Susan wasn't sure how she had found herself in such an uncomfortable position. She had assembled a great team to lead IUI into the future. Her CIO, Jennifer Limus, was brilliant. As a developer turned leader, Jennifer always seemed to have her finger on the pulse of technological innovation.

How did this get so out of hand? Susan thought to herself.

Susan wondered if she would be able to sleep. Her mind was spinning, searching for answers. Eventually she was able to drift off, dreaming of ships sinking under her kitchen faucets, dinner plates bobbing in the water, and regulators shouting from the countertops.

Tuesday, March 29th

Susan arrived in the company board room ahead of everyone else. Her admin accompanied her to set up the virtual teleconference, place the printed MRIA documents on the table, and adjust the lighting. Susan took her seat and looked out the window. Clouds were gathering. *An apt metaphor*, she thought to herself.

Jennifer, the CIO; Tim, the CISO; Bill, VP of Product; and Jada, the Chief Risk and Compliance Officer (CRCO),[2] arrived a few minutes later and took their seats around the table. It was clear that everyone was anxious and tensions were high.

"Well, you all know why we're here today," Susan began. "I need answers, and fast. But first, I'd like to announce to everyone that effective today, Jada will act as Chief Risk and Compliance Officer, heading both Audit as well as Risk."

Murmurings began to fly around the room. Susan quickly held her hand up, a clear sign for everyone to quiet down. "I want to make this clear. No one has been fired. Fredrick has been looking to retire, and he has taken this as an opportunity to finally spend more time at that cabin of his and teach his grandkids to fish. I wish him the very best. I'll be looking to fill the void he left, but it will take a while. I have every confidence in Jada's abilities until then."

Even with Susan's attempts to quell the fear in the room, it was clear that everyone was tense. She understood. It had been a hard discussion with Fredrick early this morning. Despite her best attempts to assure Fredrick that she didn't pass blame to him, he had made it clear that he didn't feel he was up to the task anymore and that he had full confidence in Jada taking over.

"Okay, everyone. Now that that is out of the way, let's get down to business. I've heard what Fredrick had to say, but now I want to hear from all of you. How did we get to the point where the OCC has hit us with an MRIA?"

Immediately, Jada spoke up. Jada had been with IUI as long as Susan, and she was always quick to offer her opinions. Her passion had made her a great CRO, and

---

2 One of the themes that continues to evolve is the interaction and relationship between the chief audit executive (CAE) and the chief risk officer (CRO). The roles of these positions are highly interrelated and interdependent. In fact, in many organizations they are merged into a single role, such as CRCO.

hopefully a great CRCO. But that same strength also made her come across as rigid and abrasive at times.

"I've been warning everyone about this for the past year," Jada answered, looking around the room. She added, "Yet consistently I was told that product release deadlines were a higher priority."

"Come on, Jada. You know we had no choice," Bill said. As VP of Product, Bill was obsessed with shipping features and products that would delight clients and drive revenue. He was always pushing to get things done and could always be counted on to defend his team. He had been with IUI longer than anyone else in the room and knew their customer well. He was sometimes slower to accept new mindsets and ways of working, but his intentions were right. "Without these new features and updates, the apps would be deemed unusable, and our customers would vote us off the island. It's like the Risk team doesn't even know we're running a competitive business here."

"Of course we know that, Bill. We're trying to help protect IUI and its competitiveness," Jada responded. "We can't be competitive if our applications and customer data aren't secure. I've been cautioning you guys that we've let our delivery teams do whatever they want in the name of DevOps and digital transformation. We have no control. For heaven's sake, we are a bank!"

Susan leaned back in her chair. She wasn't pleased by the blame that was being tossed around the room.

"Jada's right," Tim began in his typical firm yet calm voice, obviously trying to rein in a discussion that was quickly taking a bad turn. "We're all looking out for IUI."

Tim had a commanding and official presence about him that fit his role as CISO. When he entered the room, people paid attention. His résumé included a long list of leading financial cyber groups, as well as some large IT audit firms. "To be fair," he continued, "we have all of these MRAs listed in the product backlog. Why hasn't the Dev team been delivering on them?"

Bill rolled his eyes. "Honestly, it seems to take forever to just get features out. I don't know what our Dev teams do all day. They clearly can't keep up."

"Keep up?!" Jennifer looked perplexed. She was probably one of the youngest executive leaders at a company the size of IUI, but her knowledge and skill far outweighed many of her peers at other institutions. "I think everyone understands that we attack whatever is in our multiple backlogs with the engineers we have available. But each product's backlog is growing on a daily basis with new features and demands." Jennifer looked over at Bill and continued, "The problem is we never get enough time to address technical debt, much less the frequent 'urgent new feature' fire drills that the Product team keeps hitting us with."

"So hire more people!" Bill shot back.

"You think it's that easy? It's not. The demand for quality engineers is extremely competitive, and then we still have to onboard those we do hire. We have many open spots right now, and the new engineers we just hired are still coming up to speed. I don't think any of us saw the tsunami of new feature work that would be hitting us." Jennifer took a deep breath, obviously trying, then looked over at Susan for support.

Susan sat at the head of the table, quietly watching and listening as her team bickered like teenagers. She had expected some finger-pointing, but this was worse than she imagined. Most of all, she was just confused. She had been receiving enthusiastic reports from all of her VPs about the great progress they had made with DevOps over the past few years. And after IUI had brought Jason in a year ago as SVP of Digital Transformation, the progress had only increased. However, now it seemed like the left hand didn't know what the right had been doing.

"Look, this isn't productive," Susan said, standing up. "I need some real answers. What is the current situation with the MRAs and what are we going to do about it? I need to show the board that we have a clear plan of action. The regulators have informed us that we have just three months to address all of their concerns and show we have a plan to move forward. Three months before IUI gets hit with a formal enforcement action from the regulators. Three months before every one of you and every person who works for you is suddenly out of job or IUI is taken over by the government.[3] Three months before everything we have built comes crashing down around us.

"Now, I don't think anyone in this room wants to have to tell their entire team that their leaders failed them." Susan paused and looked at each person around the table. She was relieved to see some of them squirm slightly under her gaze. It meant the message was hitting home.

"We get it," Jada said, breaking the silence. She took a breath. "The MRAs that led to this MRIA deal with a lot of issues related to our IT governance—the way we develop, run, and manage our software. We'll get a summary list for you."

"Thank you," Susan said, sitting back down in her chair and looking at Tim, who was sitting next to Jada.

Tim looked at Jennifer, then back to Susan. "I'll work with Jennifer to put together our action plan to get these addressed. But it isn't going to be easy. We have a lot of work going on right now . . . "

"There's always a lot of work going on," Susan interrupted. "And I don't need to be told that this will be hard. What I need are solutions. IUI's survival could be in jeopardy, with serious consequences to our thousands of employees and their families. This must be our top priority."

---

3 You can view a real cease and desist order issued against MUFG Bank here: https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-100.html.

Susan looked around the room and worked up a grim smile. "I know we can get through this. There's plenty of talent in this room and on your teams. We have just three months to fix this mess or it's game over. It's as simple as that."

Susan stood again. "Now, I have to go and meet with the board, who will likely want us to bring in an external auditor to review and sign off on our closure package with regulators. But I want regular updates on your progress. My assistant will be putting a weekly huddle on all of your calendars. I expect great things from you all. Let's figure this out. Let's make this happen."

Heads nodded. Susan grabbed her tablet and exited the room.

CHAPTER 2

Tuesday, March 29th (*continued*)

"Okay everyone, let's do this!" Tim announced. He was standing at the front of a conference room crammed with VPs and SVPs. He had been in meetings like this many times before. Everyone was here to defend their territory, to just say they were part of it, or to sit back, listen, and then complain later.

Tim looked around the room. Carol, the VP of Engineering Digital Banking, was seated right across from him, and Bill was seated across from Jada. Each of the political nemeses were now face to face without Susan refereeing.

Let the melee begin, he thought, was tamping down his feigned enthusiasm.

"Carol, let's get you up to speed," Tim began. "Jada, Bill, Jennifer, and I met with Susan earlier today regarding the MRIA we received. Has Jennifer filled you in on the conversation?"

"Yes, yes, Jennifer and I met earlier, and she gave me the rundown. If I understand it correctly, we shot ourselves in the foot by not responding adequately to these MRAs over the past twelve months. I think it was something like fifteen MRAs that either we didn't respond to or our response was sub par?" Carol shared.

"That's right," Tim responded. "Today's agenda is simple. We must compile a list of the findings. We will then review this list with Susan and our progress on addressing the actions in the weekly huddles with her and, likely, an external audit team, until we submit our response to the regulators in three months."

Bill quickly interrupted. "What do we do about the big release? Our teams have been working on Project Prisma for the last few quarters. We can't cancel that."

"Really? What do we do when we're shut down?" Jada shot back.

"Obviously we need to keep the business running while addressing the MRIA," Tim jumped in, hoping to quell yet another fight between Product and Risk.

"Let's take a step back. What kept us from addressing these issues right up front? Why haven't we responded to the MRAs sufficiently? What's the bottleneck?"

Bill furrowed his brow. "Are we talking about the MRIA or the MRAs? I'm totally confused now."

"If we had responded to the MRAs in time and adequately, we wouldn't have the MRIA." Tim sounded a little exasperated.

"Well, we did push back on several of these MRA findings," Carol spoke up. "We asked questions on the ones that don't make sense or don't apply. But we got radio silence. Zero response!" She turned to Jada. "We get no help from the Risk or Audit teams."

Jada looked puzzled.

Carol looked back at Tim. "See?! That's the problem. We not only have to manage our engineering projects but we have to shepherd all this paperwork to get stuff done here. I don't have enough people to do that. And it sure isn't in our backlogs."

"Yes, yes, I get it!" snapped Tim. "I understand the bickering, but that isn't helping right now. We are here today to identify the issues raised in MRAs that led to this MRIA and then report back to Susan." Tim felt like a broken record.

Carol sighed. "It always falls to Engineering to fix everything. I won't have all the blame game going against my developers. Engineering is about building things, building bridges across seemingly impossible problems and arriving at new destinations. I know some people here have little appreciation for the role, but there are great rewards in seeing good outcomes.

"I'm inviting Michelle, one of my senior staff engineers, to this meeting," Carol announced. "She has historically raised compliance concerns, and she'll be an asset to this conversation." Carol turned to her phone and typed a message on the interoffice chat system.

"It's terrifying that Engineering and Product have no clue how to manage risk," Jada said, warming up her artillery.

"Isn't that your job?" Bill responded with a smug smile.

"Ugh." Tim sat down. It looked as though he had given up on refereeing the meeting. The conversation went on like this for several more minutes, a constant stream of back and forth, not one of the prize-fighters addressing the single action for the meeting that Tim had laid out.

"Okay, we aren't getting anywhere," Tim said loudly, raising his arms to quell the discussion that had risen several octaves in the last five minutes alone. "So much complaining," he stated, as if he epitomized a glass house. "You all are starting to sound like my kids fighting each other when I tell them to clean their room. I'm always amazed at the big mess they create while trying to clean up the small mess. Truth is, it's simply because they spite each other rather than work together."

Michelle arrived like a whirlwind and the room went silent. Her arms were full of a laptop, tablet, paper notebook, and pen. She sat down next to Carol and hastily arranged her stuff on the table. Her long black hair was pulled back into a ponytail and her eyes were bright. She looked poised for action and clearly had something to say.

Carol introduced her to the room, most of whom had never met or worked with her directly. "Michelle is one of my best engineers, despite the fact that she's been

at IUI the shortest of anyone else in this room. But there's no doubt in my mind that she needs to be here. Since Michelle joined IUI from a smaller company, she's brought with her a youthful energy and knowledge of the latest ways of working. She doesn't shrink from expressing her opinions, even to senior leadership." Carol looked pointedly around the room. "She's a change agent. And that's exactly why Jason had recommended her for the job, and why we need her to help with this mess."

"But does she have the necessary experience . . ." Jada began.

"After she joined IUI as a junior engineer, Michelle soon took on the mantle of security liaison for the entire Engineering team," Carol interrupted. "She's worked with Tim's group conducting code reviews of applications all across IUI. And she's been responsible for answering questions that come up during PCI DSS[1] compliance reviews. She even coauthored the annual state of security report."

"Okay, okay," Jada said. "Sounds like she's a good person to help us out. Let's hear what she has to say."

"I knew this was going to happen," Michelle said firmly and succinctly. "I sent out a memo months ago warning everyone about this exact scenario, but everyone was too busy to pay attention? Well, here we are. I told you that our manual, one-size-fits-all security review with IUI's large portfolio of applications was a disaster waiting to happen. Our software development life cycle risk reduction practices are just too immature. And on top of that, we've been ignoring the findings from our own Audit team."

Bill snapped in response. "If Security and Audit would get us a unified set of requirements and work with us to comply without slowing us down so much, we'd be in a better place." Bill's frustration was evident in his voice and on his face. "We're constantly balancing competing requirements for the IUI portfolio. What we need to be doing is delivering value to our customers. You try doing that while juggling competing priorities from the business."

"Bill, not to be too much of a punk, but I do that. Me! It all rolls downhill, and guess who has two thumbs and is at the bottom? This person," Michelle said, her thumbs pointing at her face as she stood up for herself. Carol smirked.

A short, tense pause was felt in the room. "Audit doesn't have requirements," Jada broke in. "Audit's role is simple. We look at the controls, what IUI says it should do to manage risk, and compare it to what we actually do. Audit doesn't make the rules—heck, they don't even recommend controls. Audit answers the question: Is IUI doing what they say they should be doing?"

"That's not true. This time last year I remember getting a long list of 'thou shalts' from Audit. It's like you all intentionally keep the details to yourself and then slap our

1 Payment Card Industry Data Security Standard: https://www.pcisecuritystandards.org/.

hands when we don't read your minds!" Bill shot back. "If I can't get requirements from you, then where do we get them from?"

Tim quickly interrupted, "Jada, Bill . . . hold those thoughts. We're supposed to report to Susan on the MRIA. We need this exact conversation but not right now."

Michelle quickly followed up. "I suggest we break down the audit finding into stages and then try to understand what technology and process improvements need to be applied." She opened her laptop to begin reading the summary of the findings.

"Michelle, I appreciate the enthusiasm, but let's take this up a level," Tim replied. "The MRIA has summarized all the previous findings. It states here in the Executive Summary: *Inconsistent process, ineffective in ensuring security and compliance, resulting in unauthorized and vulnerable software with significant number of defects being released to production.*"

"That tells us nothing!" Michelle stated passionately. "Inconsistent process? Well, hashtag-facepalm, duh. This is only telling us what we already know." Frantically scrolling through the report on her screen, Michelle followed up with, "Where in here do they tell us specifically what we need to fix?"

"They don't and they won't," replied Jada. "That report only tells us what we already know: we aren't following our own processes, and our processes may be missing something. It's our job to respond with what we will do to address that concern. Where are the teams storing their processes these days? The Risk organization stores all its information and tracking details in our GRC system."

Just mentioning the Governance, Risk, and Compliance system caused an audible groan in the room. Jada didn't even pretend to be shocked. Her own teams even complained about the GRC system and its impossible user interface.

"Engineering teams document their processes in markdown and source control them in our Git repositories. The same area where we store code," Michelle responded.

"Security is supposed to capture info and store it in the knowledge management module of our internal service system," Tim added.

"Product tracks all of its requirements in our ticketing system," Bill said.

"Four organizations and four different places to store information. That seems like a red flag," Carol said. "Michelle, how do the engineers use each of these systems?"

"Engineering takes its marching orders from the ticketing system the Product team uses. We live our lives in that system. In general, no one in engineering knows about the GRC system. Nor do they care. I only know about it by researching compliance issues we had with a release a couple quarters ago. As for the knowledge management system, well . . ." A sudden pause filled the room, then Michelle continued. "We know about it, and most of us have access. Although we don't use it. Most of the information is incomplete, out of date, or inaccurate. If we have a secu-

rity issue or question, we back channel it. If we can't back channel it, we consider it a good old college try, then move on. Our best security advice mostly comes from internet searches."

Tim barely managed to keep a straight face as he heard Michelle's last comment.

Carol said, "If you're the most in-the-know person, and this is how you operate, this looks like something we need to consider. How can we ever do what we say we are doing if we can't figure out where to go to do the things we need to do?"

"I swear I read that same sentence in a Dr. Suess book before," Bill quipped.

"Our response to Susan is becoming a bit clearer now," Tim interjected. Everyone turned their heads toward him, all with confused expressions. "We can't tell her what's wrong when we collectively don't know specifically what the issue is. All we know is, somehow, someway, the full process is broken. Bits and pieces may work in silos, but it doesn't work as a full system, and I'm broadly speaking when I use the word 'system.'"

"Then what should our response be?" Jada asked everyone around the table.

"I have an idea," Tim said, regaining control of the conversation. "Michelle has the best grasp on how things operate. She has proven she's able to work across all of our areas." He looked at Michelle. "Michelle, how long would it take you to dig deeper, read the specific MRAs, and come up with a current state and the basis of a proposal for a future state?"

Feeling a bit under the gun, Michelle responded, "Are you asking me to figure out how to respond to the MRIA?"

"No, not at all," Tim replied. "Think of it as an outline with a sole focus on listing the specific issues. We'll collectively build a response, but first, and to your point earlier, we need specifics."

"Okay, sure. What's the timeline?" Michelle asked.

"Today is Tuesday, and the weekly huddle is every Thursday," Tim said.

"Well, we won't have the details this Thursday. I don't think that any quality research can be done with what remains of today and tomorrow."

"Yes, I agree," Tim interrupted. "Let's meet next Wednesday, same time and place. That gives you a week. Remember, we aren't looking for solutions right now; we're simply looking for an outline. The best outline would be based upon, and I'll restate what Jada said earlier, *what we say we should be doing and what we are, or are not, doing*."

All eyes were on Michelle. She sat there deep in thought. She didn't appear to be under pressure. Rather, she appeared to contemplate if the time was satisfactory for the required research. A few seconds passed as if they were ten long minutes.

"Carol, Bill, I need to offload some work to the team today. To make this happen, this needs to be my only focus. I have enough research so far that I'm confident I can have an outline by next Wednesday if I'm not also trying to do other work."

"Okay, good. Remember, while you're accountable for this, you don't have to be the only person to actually do the work. Bill, can you assist Michelle?" Tim asked.

Bill looked bewildered. His organization's backlogs were so backed up that each backlog had a backlog item to review the backlog! He had his own process issues to figure out with Marketing, Sales, and Finance. But Bill knew this was not a question but a political "volun-told" situation. He didn't have to agree. After all, he didn't report to Tim. But he knew how important this was. Bill had a keen sense that work like this may become a mainstay for him, and his organization, in the future. This was important.

Bill replied with a simple, "Yes, I can."

"Okay, so we have a plan," Tim said. "Come next Wednesday, Michelle and Bill will have a draft outline of the things we say we are doing and the reality of how we are or are not doing them. To ensure as much clarity as possible, we must keep our scope to the poorly answered MRAs addressed under the MRIA statement in the executive summary."

Tim looked around the room. Everyone nodded in agreement. A rush of optimism swept the room. It felt like things were finally starting to move.

"Tim, why don't you, Jada, and I stop by Susan's office to set expectations?" Carol said, as it was evident the meeting was coming to a close.

"Agreed," replied Tim. "This MRIA is a ticking time bomb."

Wednesday, March 30th

Michelle and Bill showed up to the office the next day at their usual time. Bill wandered over to Michelle's cube around 9:30 AM.

"Morning, Bill," Michelle said.

"Good morning to you as well. So, do you have a recommendation for where we start?"

"Yes, yes I do. I combed through all of my emails and previous research last night. I moved it all to a new folder on the shared drive called 'MRIA Madness.' More of an ode to March Madness; less about our own madness."

Bill chuckled a bit. He thought the title was witty.

"First thing I'll do today is speak again with each of the people I've talked with to generate this research. I started a document called *1 - MRIA Outline*. I added the '1' to it so it's the first document when you open the share drive."

"Good call," Bill replied.

"I'll summarize my findings in this document and link to any other relevant information. My approach is to start with Risk and Audit. I want to trace the process

starting with us stating 'this is what we do.' I've decided to give a single word to these 'things we do.' I'm calling them promises. 'This is what we do' is a promise we are making to regulators and customers and to each other."

"That's actually brilliant, Michelle," Bill replied. "Putting my Product hat on, that would be a good way to market any change management we need behind this. Controls are very sterile, but promises—well, no one wants to break a promise."

Michelle smiled, recognizing the compliment. "Sure. Thanks, Bill," she said. "After I find all these promises, I'm going to trace each one to some type of implementation. We need to see how we commit to keeping these promises we make. It's basic, but it's a start. I don't want to over complicate the discovery process. What do you think of the approach?"

"Ship it," Bill replied. "How about you and I meet up at 3:00 PM every day? I'll set aside two hours to analyze your info and help compile the outline. Does that work for you?"

"Sure, works for me!"

This first day seemed to be the longest and shortest day at the same time. Michelle spent every minute hopping around the office. No one was outside her scope of calendar invites and office drop-ins. She was pleased to find that many of the people she talked to were more than willing to help.

During it all, she realized a very important aspect of humanity. People love to talk about themselves, especially when someone is listening to them moan about a problem. Even though Michelle was still fairly junior in her career, she had a natural knack for facilitating unstructured conversation.

For one meeting, Bill joined. He was impressed with how she led the conversation with empathy. She often said things like "I know what you mean. I felt the same way," or "I can see how that was difficult for you." Bill on the other hand was visibly annoyed by some of their criticisms, demeanor, and complaints. He was able to keep his mouth shut, but his blood was boiling on the inside.

Michelle noticed. She smiled and thought to herself, *For a person who's mostly listening in, Bill sure looks like he wants to share a few choice words with people*. Michelle took a different approach, however. She found endearing ways to cut through the complaining and self-centered attitude of many people. As a result, she was able to elicit facts.

Three o'clock in the afternoon came quickly. It seemed to creep up on Michelle like a bad guy in a horror film. She arrived at Bill's office. It wasn't much, really. It was like all the other offices at IUI. It was situated on the outside wall of the floor

with windows on two walls and the standard, sterile, corporate-painted sheetrock for the other two walls. There was a tidy desk and a small conference table in the room. It looked like a great spot to work until she realized how hot the office was with the afternoon sun beating down on them through the windows.

Michelle and Bill reviewed all the interviews from that day. It was clear that they had uncovered two big pieces of information. First, they had documented the use of over twenty-four systems, spreadsheets, and documents used to capture the "things we say we are going to do." Second, their list of interviewees had grown exponentially.

"I know we've grown, but wow, you don't realize how big a small company can get until you try to talk to almost every employee," Bill said.

"I have no clue what it was like here before, when you old-timers had to walk to work, uphill, both ways, in the snow," Michelle joked. "But yes, we are big. I've now met folks who have worked here longer than I have but I can't recall ever seeing their faces before."

"Well, with all that aside," Bill continued, "I think we can start the document."

Sitting next to Bill at his office conference table, Michelle opened up her *MRIA Outline* document and typed the following:

MRIA

Finding/Concern
- Inconsistent process, ineffective in ensuring security and compliance, resulting in unauthorized and vulnerable software with significant number of defects being released to production.

Current State - Promises (aka "Controls")
- Documented software release process
- Documented software testing process
- [Continue here tomorrow]

"Well, that summarizes everything. Although that just seems like too few words for all the jibber-jabbing, complaining, and real facts we uncovered today," Bill said.

"It's late and I'm too tired to think about how to include anything else. We have copious notes. If we need to, we can always go back to them," Michelle responded.

"Touché, touché," Bill said.

Michelle saved her document and then closed her laptop. It was a couple minutes past five, and she had to get going. Her babysitter got cranky if she had to watch Michelle's twins later than six o'clock.

"I need to leave. I've had enough for the day. Let's pick this back up tomorrow," Michelle suggested.

"Agreed," Bill responded.

Michelle walked back to her cube, grabbed her belongings, and started toward the parking garage. She passed many of the people she'd spoken with earlier. Tossing each one of them a soft smile, she couldn't help but wonder to herself, *IUI has smart and driven people. How could so many things go wrong at a place like this?*

CHAPTER 3

Tuesday, April 5th

The next few days seemed to fly by. Michelle put on her best Sherlock Holmes, with Bill acting as her Dr. Watson. It seemed like there wasn't anyone she didn't speak with. Michelle would have set a meeting with the janitorial staff if she'd thought they had useful insights into how IUI kept promises to external auditors and customers.

Sometimes, it seemed like Michelle's and Bill's back-to-back meetings resembled a cheesy '90s rom-com montage of the first year of a relationship, where everyone is getting along. Everyone is agreeable, energetic, and open. Other times, it resembled one of those serious montages of time spent on computers, debating one another, and burning the midnight oil.

By Tuesday afternoon, the *MRIA Outline* document had grown substantially.

MRIA

Finding/Concern
- Inconsistent process, ineffective in ensuring security and compliance, resulting in unauthorized and vulnerable software with significant number of defects being released to production.

Current State
- Promises (aka "Controls")
  - Documented software release process - Not documented
  - Documented software testing process - Somewhat documented, teams do things differently
- MRAs
  - Insufficient Response - 4
  - Not Responded To - 11
- Main Systems for Process and Documentation
  - Risk - GRC System
  - Security - Knowledge Mgt. Module
  - Server Mgt. System - CMDB

- Product - Ticketing System
- Engineering - Git Repo
- Other Systems
  - Outside of the four main systems, there are 38 other "systems" that consist of community documents and wiki pages but mostly spreadsheets stored all over the company, sometimes on personal computers.
  - See "Appendix - Spreadsheets & Informal Systems" for detailed information and system owners.

Actionable Items
- Based upon the MRAs issued, the following items should be addressed with formal, standardized approaches:
  - Goal
    - Define a minimally acceptable release approach.
  - Objectives
    - Enforce peer reviews of code that is pushed to a production environment.
    - Identify and enforce minimum quality gates.
    - Remove all elevated access to all production environments for everyone.

"It's amazing what happens when you can focus and finish a task, even on a seemingly tight deadline," Bill said.

"I think we talked to everyone," Michelle replied.

"Yes, we did. Everyone, their mother, and their grandparents." Bill studied the document on Michelle's laptop. "This is a solid summary. It's on point for Tim and Carol's request. I think it sets the stage for next actions and solutioning. What do you think?"

"Of course I'm good with it! Condensing all of this information was painful. I feel like there's so much more to say," she replied.

"This isn't really any different than identifying features for a product. Think of all those folks as customers and what we did as requirements analysis," Bill said.

"Oh, that makes sense," said Michelle.

Wednesday, April 6th

"Holy hell!" Jada nearly screamed as she read through the printed version of the *MRIA Outline* document in front of her.

Michelle looked around the room. The expression on the team's faces as they read varied from stunned, shocked, and disappointed to what Michelle could only describe as outright disgusted.

"Forty-two systems . . ." Tim said in disbelief. "This is the type of information Susan needs. Not all of this nitty-gritty," he said, flipping through the appendix sections, "but this first page tells the truth that needs to be told. Even though it hurts looking at this."

"Tim, to make the most of this meeting, let's discuss the *Actionable Items* listed here. Information like this is key to the IUI response to the MRIA," Jada said.

"Okay, great," said Tim. "Let's start with the goal: *Define a minimally acceptable release approach*."

"We've made great strides toward this in our DevOps journey, but we still have some gaps, particularly in digital banking," said Michelle, looking at Carol. "Developers tend to use workarounds in legacy back end processes. Our documentation is either nonexistent or unclear. Developers who know the process follow it. But those who don't know the process blame problems on legacy systems and the older applications developers who were here before our DevOps journey.

"It's further complicated by the subjective nature of how we create evidence. For example, all the evidence is implicitly defined in our CMDB[1] system without any hard or objective evidence being stored anywhere. Tim's team runs reports against that CMDB system."

"Yes," said Tim. "And for the most part we believe we're in compliance. But we don't actually validate the data."

"Why not?" asked Jada. No answer was forthcoming.

"Okay, what's next, Michelle?" asked Tim.

"We lack code reviews before deployments. It seems everyone thinks everyone else is doing this correctly, but not everyone is." Michelle laughed, failing to conceal the irony. She then continued. "There are a number of ways to bypass this process."

"Like what?" asked Jada.

"Oh, I remember this one," Bill jumped in. "Wasn't there someone on one of your teams, Michelle, who built an automated script to auto-review his own work using a service account?"

"Say what?" Jada said, surprise evident in her voice. "And then what happened?"

Michelle replied, "We took his service account away. He left IUI last year. He came from a start-up and didn't actually like our way of working . . . forget it. Let's continue."

"It's actually really frightening to see that we have wide-open gaps," said Tim.

---

1 CMDB stands for configuration management database.

"One of the issues is that we don't have a formal way to request a peer review. Basically, a person committing code has to track someone down and literally ask them to stop what they're doing to help them with the review. That is, if anyone bothers to do it. It's disruptive, slow, inconsistent, and unreliable. We don't allow for proper structure or bandwidth to support a formalized process for code reviews," said Michelle.

"But, if you ask me what makes me nervous . . . we have too many old open-source and commercial libraries and packages. We've been using these libraries for so long that nobody pays any attention to them. They're likely full of vulnerabilities and in need of patches. Heck, we don't even know if we're using correctly licensed third-party software."

"That is bad," said Tim, frowning.

"But what's even worse," Michelle continued, "is that there's no consistent evidence of the security controls that Audit can easily examine. Some teams manually enter findings into their development backlog for remediation and others pass around PDF files or spreadsheets to their leaders. It's completely scattershot."

"And there's still more?" asked Jada, with a hollow laugh.

"Oh, yes," said Tim, wide-eyed, looking first at Jada and then the rest of the team. "I have heard that we lack controls, or tollgates, within the release pipelines. When Engineering teams started implementing automated pipelines, I was told that they would put some basic control gates in there. But I guess it never happened."[2]

"Unfortunately, Tim is correct," said Michelle, shaking her head. "Over time, teams have been creating workarounds and getting exceptions to bypass the tollgates. As we've grown, so has our number of pipelines. It's made it really hard to manage what happens in each one. In fact, many delivery teams have access to the CI/CD tools but have actually turned these controls off."

"What?" said Jada, looking as if she had just witnessed someone running a red light in front of her. "How did that happen?!"

"Well, it looks like it started with just a few exceptions when there was pressure to deliver at a certain time and we couldn't afford to delay the release. In time, though, it appears our system has become the 'normalization of deviance,'" Michelle said, physically making the quote marks with her hands as she said it.

"Huh? The what of what?" someone in the back of the room asked.

"Diane Vaughan wrote a book called *The Challenger Launch Decision*. The whole *Challenger* disaster happened because deviance from correct or proper behavior became normalized in the US space program. It's actually very common in corporate culture, and, well . . ." Michelle suddenly looked a little sheepish, "it's happening here."

---

2. See Appendix 2 for more on pipelines.

"Great," Jada sighed.

"And finally . . . " said Michelle, adjusting her glasses.

"Thank goodness!" said Jada, rolling her eyes.

"We have a very serious finding related to elevated access."

"Like the other findings weren't all that serious," Tim smirked. A laugh rippled around the room.

Michelle calmly carried on. "The Development and Operations teams have a way to bypass the process. Basically, there are too many incidents of 'break-glass'[3] access to systems. No one follows the guidelines. Team leads and managers grant approval left and right. I don't think that the break-glass system even works."

"But we have clear and published guidelines for this," said Tim.

"I know," said Michelle. "But people just ignore them. We don't have a way to track elevated access requests. Our system has been open to abuse. And," she added, taking a sip of her water, "it appears it has been abused."

"This is worse than I thought," Jada said. "We have to maintain segregation of duties. We'll never receive a favorable examination with the regulators without it. Do I need to remind everyone in this room about Enron?!" Jada threw up her hands and looked around. There was silence. Michelle noticed a lot of people suddenly looking down into their laps. Throwing the name Enron around a bank was a surefire way to get people really uncomfortable really fast.

"Well," Michelle piped up. "Actually, that should be achieved simply enough through the peer review system."

"No way. We can't have a developer pushing their own code into production and still achieve segregation of duties," Jada clarified. "We'll have to show that no one has both 'developer' and 'operations' roles. And the developer role cannot deploy to production. We also need to have a way to generate reports and compare the list of 'developers' against the list of 'operations' to ensure there is no overlap. We need to do that at least once every quarter."

Michelle quickly interjected. "But Jada, we don't have two roles anymore, not in the teams that have been 'DevOps-ified.' Now everyone is a developer. We're either writing code for features or writing code for infrastructure. It's all software now."

"What?" Jada stood up, looking furious. "When did that happen? Who made that decision? Why was I not consulted?"

---

3. The concept of "break glass" (which draws its name from breaking the glass to pull a fire alarm) refers to an easy and quick way for a person who does not have access privileges to perform certain functions or obtain information to gain that access when necessary. A good "break glass" process should be well-documented and understood. It should provide a secure and auditable log, as well as notify and alert the governance and leadership team of actions taken. "Break glass" events should be an exceptional process, rarely needed or followed.

Tim leaned forward and commented sarcastically, "That was our DevOps transformation. The one we've been on for the last few years. Everybody said put Dev and Ops together, and that's what we did. We made everyone a full-stack developer and put everyone in a single role: developer."

Michelle sensed that the discussion was going downhill. She stood up and firmly said, "Listen, I was in a Lean Coffee session[4] at a DevOps conference last year. The topic on my table was exactly this, segregation of duties. There were at least fifteen people at my table who were from other banks, retailers, software companies, and FinTech startups, even some folks from that famous auto parts manufacturer, Parts Unlimited. Everyone agreed unequivocally that segregation of duties is a joke. It doesn't work."

Michelle paused for a second to judge Jada's and Tim's reactions before continuing. "We assume that just because the code deployer belongs to another role, there will be no risk, or less risk. We've all seen the movie *Office Space*! Haven't we?"

There were rumbles of acknowledgment from all corners of the room.

"Well, everyone at my table felt that segregation of duties presents an increased risk that someone not familiar with the change is actually putting the change in production!" Michelle looked at Jada. "And if you talk about a 'bad actor' scenario, an ops engineer can cause equal or greater damage than a developer."

Jada quickly interjected. "So how do you ensure that no single developer has the ability to make a code change and deploy to production without anyone else's knowledge? After all, that is the actual risk that we need to mitigate—and convince the regulators that we have it mitigated."

"Exactly!" Michelle felt a lot better now. They were back on the same page, she hoped. "We have much better ways to mitigate that risk. We have all our application code in Git repositories. We use a CI/CD pipeline to build and deploy code all the way to production. Our pipeline is nothing but a set of codified build and deployment workflows, and we store them in the same Git repository, along with our infrastructure code. Now, if we take away elevated production access from every developer and *ensure* that every code change is peer reviewed before production deployment, we will have the best way to mitigate that risk that you mentioned, Jada. The key is enforcing the peer review process."

"So," Tim said, stopping Jada before she could respond. "Do we do any of that now?"

Michelle looked away and said, "No." Lowering her voice and sounding a lot less energetic, she continued. "I mean, I know that most teams have pipelines and infra-

4. Lean Coffee is a structured, agenda-less style of meeting where participants vote on the subject(s) to be discussed and when to move on to the next subject. You can learn more in the book *Making Work Visible* by Dominica DeGrandis.

structure code in their repositories. But that's about it. And as I was saying earlier, our peer review process is broken too."

Tim looked at Bill and said, "I think we all understand the extent and nature of the problem. Let's talk about roles. Bill, as Product Manager, you have ultimate accountability for digital banking."

Bill had sat through the discussion quietly, watching the room. As Michelle had gone through the findings, he'd observed Tim and Jada's reactions. The situation that IUI had found itself in was finally starting to sink in, and he was feeling fearful.

"Yes, but am I the right owner for this? These aren't features. These are security and compliance issues. Engineering problems." There were murmurs of agreement from many in the room. A voice in Bill's head wondered what his security and compliance colleagues did besides tell him what he was doing wrong. He glanced at Michelle's face. It was evident that she didn't intend to take ownership of these problems.

"But," said Tim, "one could look at compliance and security features as non-functional requirements in a product, right? If a security hole gets exploited or a compliance control is not met, that means the software has a bug or undocumented feature. And you don't like those, do you, Bill?"

"No," said Bill. "I really don't. Michelle and I actually had this conversation just the other day. She was quoting a guy . . . James . . . "

"James Wickett," said Michelle, smiling.

"That's it. You heard him talk at a DevOps Enterprise Summit session on security bugs. He said: 'A bug is a bug is a bug.'[5] That's right, isn't it, Michelle?"

"Yup," Michelle nodded.

"You know, as Product Manager, it's my job to ensure a product's features meet market needs. And we do that. We deliver a lot. Quarter after quarter we've met and exceeded expectations. But with all that output, I'm wondering what actual outcomes we drove. I'm wondering if we created a build trap.[6]"

"What's that?" asked Tim.

"It's something I've read about recently," said Bill. "It's a concept where if you only focus on delivering features and neglect experimentation and learning, than you likely aren't building the right thing; moreover, you're not learning or improving how you're building, which is our case here. We never put stories in to improve and possibly re-architect our build process for complete traceability and compliance. This is all about shifting left on security, quality, and resiliency."

---

5. Learn more in the 2017 DevOps Enterprise Summit presentation by James Wickett, "Lightning Talk: Security is in Crisis, A New Journey Begins," at https://videolibrary.doesvirtual.com/?video=524054897.

6 Learn more about the concept of a build trap in *Escaping the Build Trap: How Effective Product Management Creates Real Value* by Melissa Perri.

Bill's revelation seemed to land well in the room. Everyone looked at Bill, then at each other. They all started to realize how these MRAs could have been ignored for so long. Everyone was so busy trying to *keep up* with daily work that they had no time to *improve* daily work. That included security, quality, and resiliency.

Bill continued, "To do this the right way, we're going to have to bring in several teams from the business. And you know those teams will likely refuse to change how they work. This isn't their process. It's not going to be easy to get this new idea through those silos. But I think I know how to have this discussion with stakeholders. They will sometimes need to wait a little longer for a product. We can't maintain a 'move fast and break things' culture if it means we end up in a mess like we're finding ourselves in today. But I still wonder, if this is a security and compliance problem, shouldn't it be owned by Risk?" He looked at Jada.

"We'll be right there with you," said Jada. "But it's your product. You should own the features. And, as Tim said and you agreed, this is a feature. We're going to have to learn to collaborate better and create a pattern of working for the rest of the organization to learn from. I don't think we've ever done this together before."

Tim agreed. "Jada, we'll need to include members from my Security teams and your Risk teams to participate in this project. I'm guessing Barry and Andrea are key people we should have working on this because . . . ?"

Jada nodded. "I'll get us a meeting set up."

"Okay, it sounds like we should treat this like a market problem," Bill said, though he still felt a little uneasy about it. "We'll need their expertise to understand what I've been missing when planning a product. And I'd like Michelle to help drive an engineering solution."

"Sure," Michelle responded. She had been surprised at how well she and Bill had worked together over the last week. And after listening to everyone's pain points and problems, she was eager to begin crafting a solution.

"Okay, I think we all know what to do next!" Tim exclaimed. "I'll take what we've decided here today to Susan at the huddle tomorrow. Then we'll reconvene in a week to share what headway we've made. Let's do this like we did today and have all the material ready before Susan's weekly huddle. Michelle, I'll set up a kick-off time with you."

"Sound great," Michelle replied.

CHAPTER 4

Wednesday, April 6th *(continued)*

The room emptied fast, but Bill stayed behind. He sat in his chair, contemplating the position he'd just put himself in: right in front of the firing line. This wasn't going to be easy. The thought of managing upward, sideways, and downward made him dizzy and uncertain. He pondered the next steps.

He needed to think. He packed up his stuff and tidied the chairs as he left the room, planning to have a beer over lunch at the local pub. The thought of an afternoon stout and some Cypress Point raw oysters made him happy.

On the way down the hall, he passed Susan's office. As he walked briskly past her door, he could see someone presenting to her.

For a CEO in a highly regulated company, Susan was pretty open. She lived the company values by never shutting her door unless it was absolutely required. Many folks were polite enough not to bother her when someone else was in the office, but it was generally accepted that you could if you needed to.

Bill's attention was grabbed by a slide that was projected on the wall monitor. Susan was reviewing it with a bespectacled man, Jason Colbert, the SVP of Digital Transformation. Jason had been brought in to lead the continued DevOps transformation of IUI a year ago, and they had just started working together on a new digital product strategy.

Jason was waxing eloquently about his presentation. There wasn't any formal style to this slide, just white words in bold, simple type on a charcoal background. The words read "DevOps failed you." It grabbed him.

Bill couldn't hear clearly what Jason was saying. He walked closer to the door and waited to see if he could make out anything.

He gave it a couple more seconds, turned around, and then walked past the door again.

That slide was really intriguing to him. No one else from IT was in the room. And why was DevOps under fire? They were one of the few firms he knew of that had successfully transformed from an outdated "Plan, Build, Run" siloed way of working to a more collaborative, product-focused approach. IUI was among the first

few companies that participated in DORA metrics.[1] Why was the head of IUI's digital transformation now suggesting that DevOps had failed?

Finally he caught a snippet of the conversation.

"DevOps failed you. But it wasn't DevOps' fault. Most people forget to apply systems thinking to their DevOps transformation. In fact, Jabe Bloom has some great blogs on this you should check out. He calls it the 'Three Economies.'[2]

"You've probably heard the term 'DevSecOps'[3] thrown around these days," Jason continued. "It's not just another buzzword; it's an admission that there is more to DevOps than just Dev and Ops. An organization must go beyond developers and operations. They must consider everyone in the value stream."

Susan was looking at Jason very seriously. Bill could only imagine the stress she was under and the pressure she was getting from the board with this MRIA.

Before Bill realized he was staring, Susan looked directly at him and smiled.

"Hey, Bill, come on in."

Bill jumped at the sound of her voice.

That dizzy feeling came back to him. His palms began to sweat. He was very uncomfortable knowing he'd been caught like a child hiding on the stairs peeking between the banisters and listening in on his parents' conversation way past bedtime. He decided to style it out.

"Sorry for the office creeping," he began. "I saw the words 'DevOps failed you' and I couldn't help myself."

Susan smiled broadly. Jason turned around to face Bill, a jovial grin on his face. This wasn't what he expected. From the tone of the conversation he had overheard, it sounded like they were discussing a dire situation. But now Jason and Susan were both all smiles.

"Yes, Jason was just teaching me a thing or two about how to build better software," Susan said. "Can you imagine that. A CEO learning about building software."

"Hiya, Bill!" Jason said with enthusiasm. "What can I say? I'm a recovering academic and sometimes I get a chance to practice my old trade. Susan is kind enough to let me chew on her ear from time to time. We were just discussing the audit findings, and I was sharing some observations and insights."

Jason always had an excited yet relaxed tone. Today he wore wrinkled khaki pants and an untucked denim button-down shirt. He seemed jolly and talked as if

---

1 DevOps Research & Assessment (DORA) is responsible for the annual *State of DevOps Report*s. Their research was also the basis for the book *Accelerate* by Dr. Nicole Forsgren, Jez Humble, and Gene Kim. https://www.devops-research.com/research.html.

2. Read more on the concept of three economies in this blog from Jabe Bloom: http://blog.jabebloom.com/2020/03/04/the-three-economies-an-introduction/.

3. See Appendix 3 to learn more about DevSecOps and the DevSecOps Manifesto.

he'd just stuck his hand in the honey pot and was licking away. Definitely not what Bill thought of as a typical Boston academic.

"By the way," Jason said to Bill, "we have a couple of Sicilian cannoli left over from Bova's Bakery. Best cannoli west of the Atlantic, you know." He nodded at the pastries, and Bill grabbed one gratefully. The oysters could wait.

"I was just telling Susan how DevOps ideals are great, but they're rooted in the core chronic conflict between Development and Operations," Jason said, turning back to Susan. "'Core chronic conflict' is a fancy way of saying that people across the organization are incentivized in ways that prevent cooperation, therefore preventing the achievement of organization-wide goals. This has directly led to the mess IUI is finding itself in today with the MRIA."

"Our incentives are causing these problems? How?" Susan had lost her smile and was once again listening to Jason with a serious look on her face. It made Bill feel the weight that she obviously had on her shoulders. He took a bite of his cannoli and sat on the edge of her desk, listening closely as Jason explained.

"Developers are incentivized to go faster, delivering more features quickly."

Bill nodded while taking another bite of his cannoli.

"Operations," Jason continued, "are incentivized to reduce risk of change. If you're delivering features quickly, you're changing at a fast pace. Therefore there is a core chronic conflict between Development and Operations. Moving quickly versus the risk of change."

"Yes, I think we were just coming to a similar finding during our MRIA meeting a few minutes ago," Bill said.

Susan turned toward him, and he suddenly felt like he'd put himself on the spot. "We were looking at how Development might have inadvertently become a build trap," he continued. "Paving at least part of the path to the mess we're in now."

"That's certainly part of the problem," Jason added before turning back to Susan. "When it comes to the audit findings, I think it comes around to the fact that the Security, Risk, and Compliance folks are trained and incentivized to think of every possible way a bad actor could compromise your system. Susan, I'll send you a copy of the book Bill's referring to."

Susan nodded her appreciation.

"Josh Corman, a famous security specialist," Jason continued, "says software's not eating the world, as has been famously said; it's infecting the world.[4] Not that creating a lot of new software is a bad thing! It's just that we're constantly creating new opportunities for security compromises. Every time you add a new feature," he said, looking pointedly at Bill, "these folks assess if the change created a compromise.

---

4. You can watch the Josh Corman presentation from LISA15 here: https://www.youtube.com/watch?v=jkoFL7hGiUk&t=1s.

"It's another core chronic conflict: developers are incentivized to regularly introduce features—the build trap you spoke of—and Security, Risk, and Compliance are incentivized to minimize the likelihood or impact of all known possibilities, which can take time if not done well, creating a problem for the developers' need to move fast, and so it goes around and around . . . "

He trailed off, lost in a vivid recollection that had come to him. Finally he came back to earth. "Sometimes the actual language that the Security folks use can be blunt," Jason joked. "I blame it on their vendors. So alarmist!" he chuckled.

Bill chewed on the revelation Jason shared. On the face of it, Bill felt this was obvious. He knew this was a big issue, but as far as he was concerned, it had always been this way, and he saw no prospect of it changing. Or could it? Hadn't they already done just this sort of change with DevOps, like Jason said?

Susan looked at Jason. "So we need to think about how we DevOps-ify Security, Risk, and Compliance?"

"Exactamundo!" Jason said. "What IUI has been able to achieve with DevOps is great, but it's not enough. And this MRIA brings to light exactly what we need to shift left next. I've been watching other organizations try to handle these types of issues. Some are treating security and compliance as if it's a feature of their product."

"Hold on, did you say 'treat security and compliance as if it was a feature'?"

"Yup," Jason nodded.

Bill was surprised, but hearing the words mirrored back to him pushed his creeping panic attack away. It was replaced with cartoon scenes of bluebirds singing, bunnies hopping, and flowers blooming. He felt a smile appear on his face.

"We just said the same thing in my meeting with Tim and Jada," Bill replied. "In fact," he said, turning toward Susan, "they'll likely be filling you in on just that at the huddle tomorrow."

"I guess great minds think alike," Susan chuckled.

"I'm not sure if it's great minds or more software common sense these days," Jason stated. "Take *The DevOps Handbook*. It points out three key aspects of DevOps: flow, feedback, and continuous learning."

"Yeah, the three ways," said Bill.

"You betcha. Well, those same concepts can be applied to Security, Compliance, Risk, and any other stakeholder along a value stream. These days, I'd argue that Development versus Operations is mostly solved. Now it's all about systematically looking at all other parties that ensure the quality of software and including them in our shift-left mentality."

"'Shift-left mentality'?[5] You've said that a couple of times. Can you explain that more?" Susan asked.

---

5. See Appendix 4 for more on the concept of "shift left."

"Sure. Shifting left is a technique for bringing software testing as far forward as possible in the software requirements and design process. Imagine a diagram of the steps in the process. Testing typically happens after several other things and sits on the right-hand side of the picture. By moving it earlier in the process, we shift it left. Have you heard your developers talk about test-driven design and development?" Jason asked, turning toward Bill for confirmation.

"Oh yeah, TDD is one of Michelle's favorite soapboxes," Bill recalled.

"Good—that's an important soapbox. When you shift things left, they become a forethought in the software design and development process, not an afterthought. Think of Security, Compliance, and Risk as a form of testing," Jason explained, looking at Susan and Bill in turn. "Shift-left testing makes people think about how the software is supposed to operate, and then they codify tests. Then, once the tests are created, the engineers build the product and automatically run the tests to see if the product passes the tests. Testing this way is like creating a blueprint.

"If you watch how cars are built, before any car is produced, a blueprint for all components is designed. That blueprint is the specification for how the car operates. Testing functions that way as well, and so should Security, Compliance, and Risk."

"To be clear, you're saying we need to start baking Security, Compliance, and Risk into the upfront software designs?" Bill asked.

"That's right! Just like testing, shifting security left allows it to be codified and automatically validated as the software is built. If it's done correctly, the only human touch the software experiences, besides an end-user, is the smart people defining the tests, the smart people codifying the security and compliance policies, and the smart people writing the software. No longer do we need to have smart people performing audits by manually checking screenshots to validate things are all good.

"Actually, that reminds me of a story I heard from a colleague at another company that shall not be named," he said, placing a finger over his lips. "She found out that one of their teams had been uploading the same screenshot as testing evidence for sixteen months!"

"Oh, please tell me that's not happening here," Susan said over Jason's laughs.

Bill was profoundly affected by this insight. It all made so much sense to him, but the problem was implementation. How were they going to actually make these changes? Why had no one talked about this before?

"As a product owner, I can prioritize security and compliance as features of my product," Bill said. "If I challenge the team to shift these actions left as a means of validating the software, maybe I can help ensure we reduce audit findings. But the findings were about the software release process. I can't change how they build software, can I?"

"Bill has a point. What do you think, Jason?" Susan said.

"Their processes reflect how you incentivize them. If you prioritize not just features but also how the features are brought to market, you give the organization a reason and the power to change the way software development is done. Most leaders and managers in digital native companies get this. They get this so well that you won't hear them talk about DevOps or anything like what we're talking about. They'll just tell you that's how they've always worked."

Jason stood up for a second and did a little stretch.

"Bill, why don't you find out what Security and Compliance needs, then work with the engineers to codify these needs into your software as if it were a feature?"

"It sounds like a good plan in theory, but I still wonder why Jada's team doesn't do this?" Bill asked.

Susan responded with a serious face. "Bill, I don't know everything about software development, but I do know that IUI is not a digital native, and therefore change has to be made. You're the person with a P&L incentive to see the change. You're the person with the opportunity to shepherd the change and help lead Jada's organization through the change."

"So, where do you think you should start?" Jason asked, looking at Bill the way his college professor used to stare at the class when she presented them with an impossible challenge.

"Well, let's see . . ." Bill felt like he was standing at the edge of a cliff.

"We've been talking about treating this like a product," Jason offered. "How would you bring a product to market when you have no objective evidence the market wants it but some qualitative evidence that it's desired?"

Bill mused out loud, feeling slightly more comfortable. "I would create small, quick experiments, minimally viable products, to see what does and does not work," Bill offered. Yeah, he knew how to do that. He and his team did it all the time.

Jason smiled. "I think you've got it. But here," Jason said as he walked over to Susan's desk. Bill was a little amazed as he watched Jason riffle through her drawers, pulling out a pen and pad of paper. "I recently read a couple of documents that I think might help you and the Engineering team on your journey." He jotted down some notes.

Jason walked back over to Bill, handing him the piece of paper.

"Now, those cannoli were a good start, but I'm hungry," Jason said, turning to Susan. "Where can we get something more substantial to eat?"