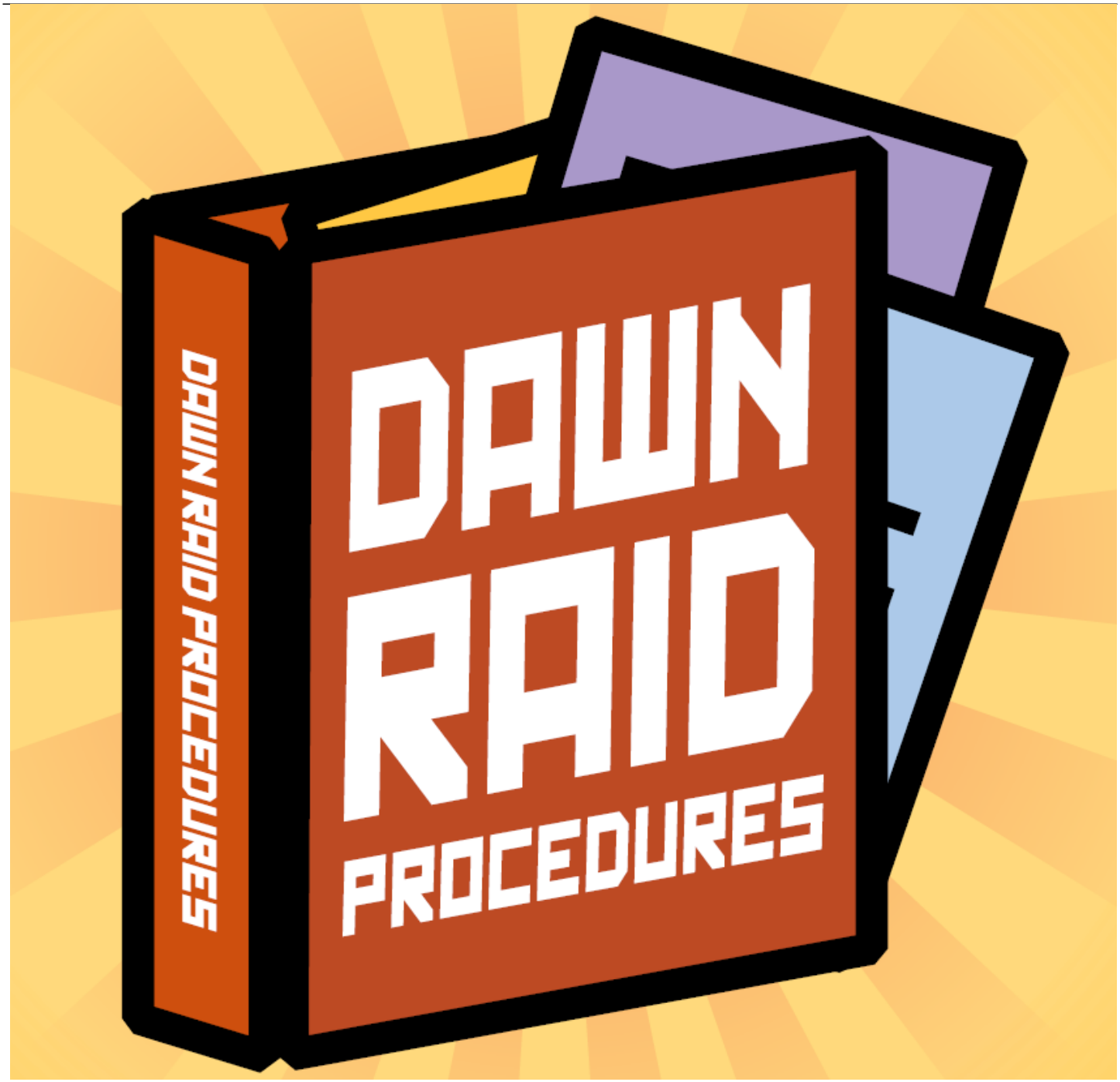
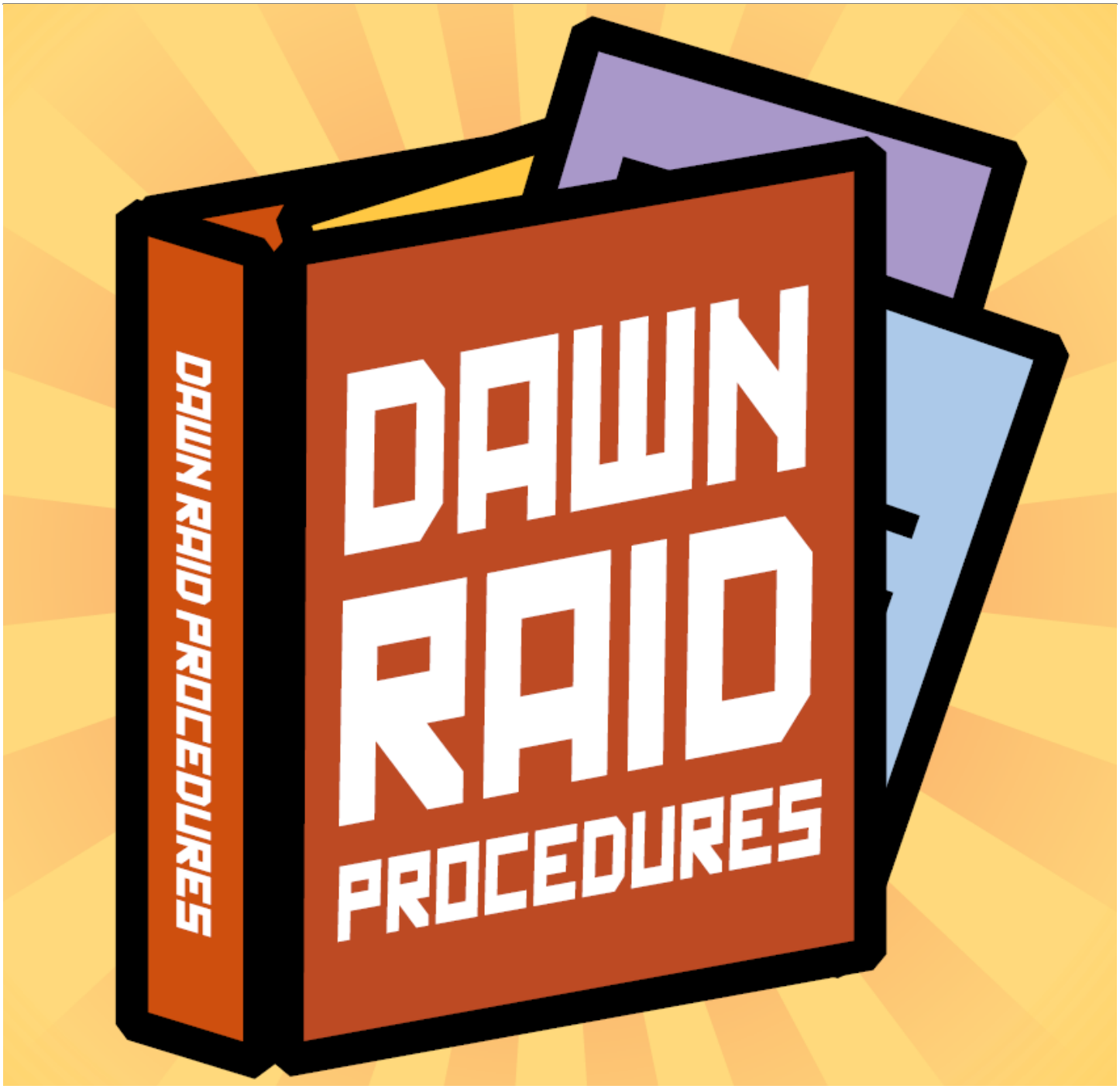
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

# Preparing for Government Investigations: What to Do and What Not to Do

**Compliance and Ethics**


DAWN RAID PROCEDURES
DAWN
RAID
PROCEDURES




## CHEAT SHEET

- ***Dawn raid policy.*** Every company should have a dawn raid policy and procedure that is regularly reviewed and practiced during semi-annual drills.
- ***Ethics trainings.*** Corporate conduct and ethics trainings must be routine, targeted to positions (from directors to third parties) and geography, and be frequently updated.
- ***Internal investigation.*** If a company discovers misconduct on its own, it should undertake an internal investigation and consider the decision to self-report to the relevant agencies.
- ***Involve outside counsel.*** Consult with outside counsel before signing anything during the execution of a warrant and before releasing any public statements about the search.

Law enforcement agents are briskly walking out of the elevator lobby and toward the reception area of your office. Your organization's employees are standing around gaping. No, it's not a nightmare — it's a dawn raid, and you've just been handed a search warrant. Record scratch, freeze frame … you're probably wondering how we got here.

> It's never too early to plan and train for a government raid.

## What's the problem?

Misconduct will happen. In the fictional scenario described, misconduct has happened. One employee's actions, a scheme by a group of employees, or a systemic problem left unidentified and unchecked could easily result in misfortune. Whether a violation of the Foreign Corrupt Practices Act, negligent or nefarious use of personally identifying information of your organization's customers, or inappropriate contact with competitors or insider trading, government investigations can happen to any company.

And it's not just the US government that will investigate misconduct, of course, and it's not just one government that will take enforcement action. In just one of the numerous examples of concerted enforcement actions and cooperation, approximately 80 people have been charged in connection with the bribes Odebrecht paid to high-level officials in a dozen countries to secure billions of dollars' worth of projects around the world. The company pleaded guilty in the United States and was required to cooperate with the respective countries' ongoing investigations of individuals and to retain an independent compliance monitor for three years. The United States, Brazil, and Switzerland were able to achieve the largest global fine ever imposed in a corruption case — more than a dozen countries cooperated for this result by exchanging relevant information as required by the OECD Convention.

Another example of coordinated activity between US and non-US law enforcement is the Telia case, which involved assistance from authorities in more than a dozen jurisdictions that did not participate in the settlements: Austria, Belgium, Bermuda, the British Virgin Islands, the Cayman Islands, Cyprus, France, Hong Kong, Ireland, the Isle of Man, Latvia, Luxembourg, Norway, Switzerland, and the United Kingdom.

As in-house counsel, you've kept yourself informed, with guidance from every government agency you can get alerts from and continual compliance-related training. You are aware of the damage your company could experience — and all of the potential vulnerabilities that the government is going to probe during its imminent investigation. You are also almost certainly aware that there are overlaps — as well as gaps — in your company's existing compliance apparatus, and you're running through a checklist in your head.

That list, although compiled over years of practicing law and taking responsibility for the complex and high-value workings of your organization, won't be enough. Responding to misconduct will always require a team, a commitment to determining the extent of exposure, and comprehensive remediation. It will also require an established response plan and all corporate parties adhering to it. It's never too early to plan and train for a government raid.

## What’s the preparation?

Investigations are normal. But most don’t end with a search warrant and pending criminal charges. Conduct can be reported to the hotline or up through management chain, or maybe it was discovered in a routine audit or by an automated monitoring system red flag. At any rate, an investigation file was opened. Any investigation will consist of a string of decisions — and will be marked by serious pitfalls lurking all along that path.

Let’s say that the misconduct at the center of our scenario had been identified well in advance of the arrival of law enforcement. The first question is whether the conduct has stopped. Once there is a positive response to that question, a cross-functional internal investigation team should review the employee conduct, the robustness of the company’s written compliance policies and procedures, and the factors to be considered when weighing the decision to self-report to the relevant government agency or agencies.

Once the investigation has determined that laws, regulations, and/or internal company policies have been violated, upper-level management should create a discipline plan in line with the employee handbook and previous instances of employee misconduct that doesn’t run afoul of protections against employee retaliation.

In concert with the disciplinary action, remediation planning will be underway, not only to prove to the government agents (who aren’t yet on the scene, of course) that the company is taking the compliance failure seriously but also as a matter of good leadership. The bottom line is that compliance failures cause reputational damage and cost money.

During any internal investigation, focus on why and how something happened — the root-cause analysis. A compliance program will look ineffective if the same type of failure continues to occur, and looking ineffective to a government enforcer or to a plaintiff can turn out just the same as being ineffective.

Every director, executive, manager, employee, contractor, agent, supplier, and third party must know the company’s approach to corporate conduct and ethics. Training must be regular, targeted to position and geography, and frequently revised. But no amount of training or executives’ statements committing to the highest legal, regulatory, and internal standards will prevent 100 percent of misconduct. Even if our scenario’s fictional company had a world-class compliance program, the likelihood of a government investigation would never have been zero.

Which means that the in-house legal department — along with counterparts from human resources, risk management, finance, and/or information technology teams — must be prepared for the search warrant. One in-house lawyer with a mental checklist is not sufficient, and do not assume that only your headquarters might be the target of a raid.

## When the government is at the door, what do you do?

Back to the present. You’re staring down at the warrant. In this situation, you’re not completely unprepared for the visit from a team of badge-wielding, vest-wearing law enforcement officers, but the experience is definitely not your favorite way to spend a Tuesday morning.

**Every company needs to have a dawn raid policy and procedure — maintained in a binder at**

**the reception desk — that has been regularly reviewed and practiced during semiannual drills.** The first item in that binder will be the contact information for the designated responder — although you, as a lawyer, are aware of what can and cannot be said or done during a raid, do not forget to train all of your front-facing employees, in all levels, on how to act and whom to call when government agents arrive. In our fictional scenario, you are that responder. Contact your defense counsel as soon as the enforcement agents arrive. Once you've recorded the agents' names, read the search warrant, and directed all employees to not destroy, delete, or hide documents of any kind or any other potential evidence, you need to make decisions about whether and how to keep operations running without interfering with the search. Track the extent of the search to confirm that it adheres to the bounds of the warrant. While you, as designated responder, may decide to delegate some of these tasks to other personnel, especially if the search is over a wide area or on separate floors of a building, be sure they and all other employees do not consent to a search that exceeds the scope of the warrant. Cooperation with law enforcement does not mean granting the search access to areas not defined in the warrant or addressed by an affidavit of probable cause. And no employee should volunteer anything to law enforcement about locations where additional evidence might be stored if they are not listed on the warrant.

Because you are a top-notch in-house counsel in this hypothetical, there are procedures in place for the storage and labeling of privileged material. You are careful to identify them to law enforcement as well as noting all contact the government has with those privileged materials.

## What do you do when the government has left?

You've already read the warrant and observed the search. Law enforcement officers have taken documents and imaged hard drives. Your employees are still standing around gaping, and some of them may even have been pulled aside for interviews with agents.

The business of the company is its business, and in order to get back to it, you must lead a comprehensive accounting of what happened and what was said during the raid. Add detail to the government's inventory of what was taken, especially if employees have noted specific items or documents that have been removed from their personal workspaces.

Fact-finding following law enforcement's departure will need to be started quickly, planned carefully, and completed diligently. Our fictional company will have to issue a document preservation notice immediately and suspend normal document retention policies during the course of the government investigation. The investigation could be completed in weeks or last for years, and it will be part of the continuing internal investigation that will occur in parallel.

No matter when you were first notified of potential misconduct and began investigating the circumstances, all the fact-finding, collection of evidence, and communication with prosecutors will end up as preparation for potential lawsuits. The legal purpose of any internal investigation is necessary to establish at the outset for the protection of privilege, though note that any audits having been completed as routine matters of business will likely be determined to not be privileged.

Of the many legal and governance reasons to undertake a full internal investigation of the misconduct, there is also a very practical reason: the potential for cooperation credit from prosecutors. A clear showing to prosecutors of a comprehensive, robust, and verifiably in-use compliance program will go a long way, as will a showing of remediation of the misconduct.

In a situation like the one described here, outside counsel would have been contacted as directed in

the response binder and likely would have been present for at least some of the execution of the warrant.

**Lessons learned**

A recent horror story involved the CCO of a Fortune 150 company whose home was the object of a raid at 6 am. Slight detail — he had joined the company merely three days before the raid took place.

Have a policy and a procedure about government raids written in plain language. Real plain language. The last thing you want is to have the company's employees trying to decode what you wrote in any of these documents during a stressful moment like a dawn raid.

If the company you work for has at least one branch in addition to headquarters, train the front desk/reception team in all the facilities and create a quick reference guide for them in the language that they speak (if the branches are in other countries). Refresh the guide and the training as necessary. Try to run mock situations to assess the efficiency of your training.

Establish only one or two people per facility to be the points of contact with government authorities in the event of a raid. You want the raid to finish as quickly as possible, so having multiple people involved is simply not efficient.

Be as specific as you can in your policy and procedure. Language like "we will cooperate with law enforcement" may give the employees the idea that law enforcement can enter and roam the facilities unaccompanied and at their will, which should not be the case. Reviewing the scope of the search warrant and being careful not to expand its scope are things you need to teach your employees.

You will want trained "eyes" accompanying the government enforcement agents around to avoid them taking more things than necessary. Unless you designate several attorneys to follow them around, which may not be feasible, your training of the employees designated to deal with law enforcement should include scenarios to help employees identify what should and what should not be taken, and more importantly, how the employees should communicate with law enforcement about what should not be taken.

Ideally, you need to have a draft of your best litigation hold notice available and ready to be sent to relevant employees at all times. These logistics are hard to figure out once the dawn raid is already taking place, so have email lists ready and update them as necessary.

Be mindful of what is happening in the market that your employer is part of. If you see dawn raids taking place at your competitors, there is a slightly increased chance you may be next.

Last, but not least: Do not panic. The entire company will be counting on you to lead the way in situations like this. Would you feel safe as a passenger on a plane if you saw the pilot crying inconsolably? That's how the employees would feel if you have a meltdown during a raid.

## Who needs to know?

Maybe the fictional company in our scenario is the world's largest widgetmaker or maybe its CEO is married to the biggest pop star in history, but most companies can assume the onset of a government investigation would fly under the radar, right? Not a chance. If everything goes in your favor while dealing with the immediate response to the search warrant, and nothing ends up online before you can get outside counsel to the offices and your crisis communications firm on the line, your company will still have to acknowledge an investigation at some point.

At the most basic, the board will have to know. Then comes the decision about whether, when, and how to tell the public. Just as you should not have signed anything for the government during the execution of the warrant without consulting with outside counsel, be sure to get thorough advice from outside counsel prior to releasing any public statement about the search. There could be legal consequences to public statements, but there are also the collateral consequences of reputational and brand damage and the potential loss of customers. Protecting reputational risk is a complicated endeavor with potentially astronomical costs for failure.

**Whether it's a civil suit, government enforcement activity, an internal investigation, or an instance of potential misconduct, don't think that you can manage it alone.** Get advice on how to communicate with the public.

## How do you learn from what you see in the news happening to competitors and industry peers?

Digging into others' bad examples might not be the most empathetic response to headlines of a law enforcement raid, but it can be very effective. When you see what another organization has done wrong, you can add to the strategic risk and compliance plan that already exists at your company. It might be a company in your industry or in your geographical area, or it might be one whose general counsel, chief compliance officer, or CEO is someone you know. Once you've reviewed all the information available to you, determine whether you need to take concrete action to protect your company.

And don't forget that the last step of this investigation doesn't involve closing a book, it means taking out a fresh sheet of paper to fill with lessons learned for the next time there is misconduct — and there will always be a next time.

Fernanda Beraldi

Senior Director, Ethics and Compliance

Cummins Inc. in Indianapolis

Beraldi has 15 years of legal experience and started at Cummins in 2015 after having worked for more than six years for Embraer SA. She is dual-licensed in Brazil and Indiana and graduated from Mackenzie University in Sao Paulo, Brazil, and she completed a Master of Laws program in Corporate and Commercial Law at Robert H. McKinney School of Law in Indianapolis (cum laude).

Amanda Allen

Team Lead — Regulatory and Compliance

Bloomberg Law

She develops legal reference content and practical tools across a variety of corporate and transactional topics, including corporate compliance and investigations, corporate legal department management, antitrust, and alternative entities. Prior to joining Bloomberg Law, Allen spent eight years at Congressional Quarterly/CQ Roll Call. Allen received her undergraduate degree from the University of Chicago and her JD from the William S. Richardson School of Law at the University of Hawai‘i at Manoa.