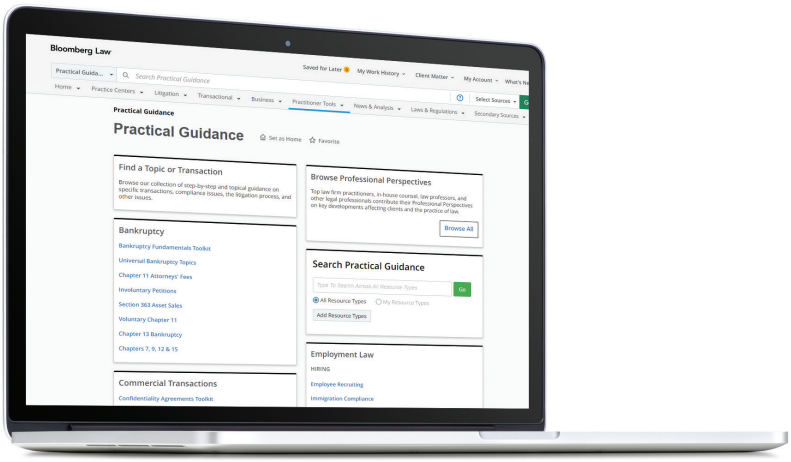
Bloomberg Law

The Essential General Counsel Toolkit

Guidance and tools for your in-house legal department

Table of Contents



Introduction

To help your legal department tackle emerging challenges and work more efficiently, we've compiled a toolkit of Bloomberg Law's expert-drafted Practical Guidance, featuring thorough overviews, how-to guidance, checklists, and annotated sample forms and agreements. The collection of resources in this toolkit offers just a glimpse of what is available to subscribers.

Not a subscriber? **Learn how** Bloomberg Law's Practical Guidance can help you tackle new or unfamiliar legal issues and reduce reliance on outside counsel.

Topical coverage includes:

- Bankruptcy
- Commercial Transactions
- Corporate Practice
- Corporate Transactions
- Executive Compensation & Benefits
- Labor & Employment
- Legal Profession
- Litigation
- Health Care
- Intellectual Property
- Privacy & Data Security
- Tech & Telecom

ENVIRONMENTAL, SOCIAL, AND GOVERNANCE

Overview – ESG & Corporate Strategy Integration

Environmental, social, and governance (ESG) concerns have moved from being desirable corporate citizenship matters to top priorities for both companies and investors. Many companies face challenges, however, in integrating ESG matters into their business models.

The integration of ESG matters into a company's business model can lead to significant bottom-line benefits. A positive ESG environment can lead to:

- positive organic growth;
- reduced costs;
- facilities risk mitigation;
- reputational enhancements;
- increased worker retention and productivity;
- supply chain improvements;
- reduced regulatory scrutiny;
- stakeholder approval; and
- enhanced access to capital, including conventional sources and new capital resources, such as green bonds.

Several factors are responsible for the lack of integration of ESG into company's business models. These include:

- institutional inertia;
- concern over the impact of ESG actions on short-term financial results;
- a lack of ESG expertise throughout all levels of the business;
- compliance costs; and
- the failure of the board or management to identify the impact of ESG factors on company operations and performance and relation to value creation.

Integrating ESG into the Company DNA: Start at the Top

It is important to obtain board buy-in with regard to ESG integration. The board must be fully informed and of ESG initiatives and engage in active oversight. ESG integration is a key component of a company's risk management and mitigation. While the board of directors is not engaged in routine risk management, risk oversight may fall within a board's fiduciary responsibilities under state law.

The extent of board oversight responsibility varies according to each company's applicable state corporate law. Under Delaware law, directors do enjoy significant protection under the business judgment rule. In the ***Caremark*** decision, the Chancery Court stated that "only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exits—will establish the lack of good faith that is a necessary condition to liability." Despite the protections afforded by Caremark, however, boards of Delaware corporations should not abdicate oversight of ESG risks, and trust their exposure to a future court's definition of a "sustained or systemic failure."

SEC rules do not specifically provide for board risk oversight. However, under **Regulation S-K Item 407(h)**, public companies must "disclose the extent of the board's role in the risk oversight of the registrant, such as how the board administers its oversight function, and the effect that this has on the board's leadership structure." For more information on the integration of ESG or sustainability committees, see **Overview—ESG & Sustainability Governance Structure**.

The "tone at the top" is essential to effective integration of ESG concerns into a company's business model. In addition to the board, individuals such as the general counsel, public relations director, corporate secretary, human resources director, investor relations officer, risk management director, and sustainability officer should all be involved. Investors, employees, and other stakeholders will expect this commitment.

ESG is a complex system covering issues ranging from climate change to supply chain management. No company can address all possible ESG issues that it could face at one time. For meaningful performance improvement, each

company should identify its most significant ESG risks and prioritize its efforts toward mitigating those risks.

Company-Wide Implementation

Companies should develop and widely distribute written ESG practices, procedures and policies throughout the company, and to stakeholders such as vendors and contractors. The company should make training and educational resources available as needed for the benefit of all employees. See **Comparison Table—ESG Communications Strategies**; **Overview—ESG Management System Elements & Benefits**.

While it is not necessary to have one person responsible for all ESG initiatives, or to create a new position to serve this function, it is important for the company to have a point of ownership to coordinate ESG activities. See **Overview—ESG Management System Elements & Benefits**. A single point of ownership prevents ESG concerns from becoming siloed within various departments and offices. The general counsel is a logical choice for ESG ownership, but companies have also employed the corporate secretary, the investor relations officer and others in this role. See **Overview—Role of the General Counsel**.

Measures of Success

Companies will want to measure the success of their ESG initiatives. It is important to establish a benchmark, likely through a third-party provider of ESG data and ratings, and monitor the company's progress over time. Employee surveys are useful tools for measuring worker awareness and implementation of the initiatives. Investor relations may also wish to engage with its large institutional investors to measure their satisfaction with the company's ESG initiatives.

ENVIRONMENTAL, SOCIAL, AND GOVERNANCE

Form – Sustainability Policy (Annotated)

It is the responsibility of XYZ Company (the company) to operate its business in a way that will contribute to the development of a sustainable future. XYZ understands the impact of our business activities on the environment and society, and will act to fulfill its corporate social responsibilities and make contributions to our communities and to society.

Practice Tip: Sustainability should be a major corporate objective. Sustainability is an important component of corporate social responsibility (CSR) and good corporate citizenship. Companies should view sustainability as more than CSR and treat sound environmental policy as a key part of the business model and a vital component of future profitability.

The company will:

- comply with, and exceed where practicable, all applicable environmental, social and corporate governance laws, rules and regulations;
- fully implement and comply with our internal environmental requirements where specific environmental legislation does not exist or is not sufficient;
- integrate sustainability considerations into all our business decisions;
- inform all employees, clients, contractors and vendors of our sustainability policy;
- make environmental compliance a priority and emphasize pollution prevention and efficient use of resources in planning and operating our facilities;
- optimize its innovations, business strategy and operations by setting both financial and nonfinancial targets and maintaining constructive relationships with all stakeholders; and
- review and annually report on the company's sustainability performance.

The company will strive to:

- create open, accessible and innovative work environments;
- reduce operational costs and environmental impacts through conservation and waste reduction;
- drive profits in a socially and environmentally responsible way;
- engage company personnel in developing a culture of sustainability through employee education and training;
- engage with our customers to foster environmentally responsible usage of our products;
- see that our business partners are committed to sustainable development, and partner with our suppliers to operate sustainably and reduce waste;
- be active in its communities, and be regularly engaged in community initiatives focused on environmental stewardship and energy efficiency;
- constructively work with elected bodies, government agencies, trade associations, environmental organizations, and others to develop practical and effective environmental laws and regulations;
- support research on the environmental effects of our raw materials, products, processes, discharges, emissions, and wastes; and
- regularly assess environmental impacts in the design of new and modified products

The company commits to minimizing its impact on our environment through:

- being an environmentally responsible neighbor in our community;
- conserving natural resources by reusing and recycling;
- using processes that do not adversely affect the environment in our operations;
- ensuring the responsible use of energy throughout the organization;
- conducting rigorous audits, evaluations, and self-assessments of the implementation of this policy;

- working toward making all company services and products energy-efficient and environmentally friendly; and
- correcting incidents or conditions that endanger health, safety, or the environment, promptly reporting any such incidents to the relevant authorities, and informing affected parties as appropriate.

Practice Tip: The key to a successful sustainability policy is widespread implementation and communication. Companies should take steps to insure that all employees, contractors, vendors and other interested parties are aware of and understand the policy. Companies should provide for education and training in sustainability best practices, and provide well-publicized communication lines for any questions or issues arising under the policy.

"The high level view of patent law provided by Bloomberg Law gives a good refresher on some topics that do not come up routinely in practice and I can refresh my understanding of topics. For contract drafting, the research and details that Bloomberg Law provides is invaluable in saving time and money in repeated drafting and editing."

Don Smith, Associate IP Counsel
Zebra Technologies

Bloomberg Law's Practical Guidance provides task-based, how-to coverage, including overviews, checklists, sample forms and agreements, timelines, drafting and negotiating guides, and more.

Because of our one platform, one price promise, our Practical Guidance is richly integrated with other Bloomberg Law assets – including state Chart Builders, our Precedent Database, news, dockets, Smart Code®, and Points of Law. And we continue to expand and enhance our offerings at no additional cost to subscribers.

*Not a Bloomberg Law subscriber? **Request a demo**.*

LABOR & EMPLOYMENT

Sample Policy – Paid Sick Leave (Annotated)

Editor's Note: Federal law does not require employers to provide paid sick leave, but many state and local laws do require employers to provide it. This model policy provides language employers can use to create paid sick leave policies, highlights key differences in state and local paid sick leave laws, and provides information on enhanced leave related to the Covid-19 pandemic. As with any policy, employers should check federal, state, and local requirements before creating or implementing a paid sick leave policy.

Paid Sick Leave Policy

[Employer] provides paid sick leave to employees to use for medical-related reasons and complies with all federal, state, and local leave laws. This policy addresses how employees earn and can use paid sick leave for medical-related reasons.

Comment: Most state and local earned paid leave laws require employers to notify employees of their right to earn and use paid sick leave. Some laws allow employers to satisfy this requirement by implementing and distributing a written policy, while others require employers to post notices informing employees of their sick leave rights. See **State Chart Builder: Earned Paid Leave (Policy, Notification, and Poster Requirements)**; **State Labor & Employment Law Posters**; **Local Paid Leave Provisions Chart**.

EMPLOYEE ELIGIBILITY

All employees are eligible for paid sick leave to use for medical-related reasons.

Comment: State and local laws that require employers to provide paid sick leave may specify which employees must be entitled to time off. Some states allow employers to use eligibility requirements, such as providing leave only to employees who work a minimum number of hours, are employed in certain jobs, or have been with the company a specified amount of time. In every case, employers are permitted to create policies that provide leave to more employees than required by law. See **State Chart Builder: Earned Paid Leave (Coverage)**; **Local Paid Leave Provisions Chart**.

REASONS FOR SICK LEAVE

Employees can use sick leave for medical reasons such as illness or injury, medical treatment, visits to health-care providers, or to care for certain family members' health needs.

Employees can use paid sick leave to care for the health needs of the following family members: spouse, biological child, adopted child, stepchild, legal ward, or child for whom an employee has day-to-day responsibilities to care for or financially support (for example, a grandparent who provides daily care for a grandchild). Employees also can take paid sick leave for their biological, adoptive, step, or foster father or mother, or for any person who had day-to-day responsibilities or provided financial support for them as children.

Comment: State and local laws may specify how employees can use paid sick leave and may require employers to provide paid sick leave for nonmedical reasons, such as to escape domestic violence or participate in court proceedings. Laws can also vary regarding who is considered a family member for purposes of paid sick leave. Regardless of any specifications in a particular law, employers are permitted to provide leave that is more expansive than the legal requirement. **State Chart Builder: Earned Paid Leave (Reasons for Leave)**; **Local Paid Leave Provisions Chart**.

Leave Related to Covid-19

Employees are permitted to use paid sick leave to arrange for a Covid-19 vaccine, to receive a Covid-19 vaccine, and to recover from side effects related to the vaccination.

Employees who need leave for any of the reasons listed by the U.S. Department of Labor as related to the Covid-19 pandemic should contact [Name of Contact] or their immediate supervisor.

Comment: Eligible employers that choose to provide emergency paid sick leave pursuant to the Families First Coronavirus Response Act (**Pub. L. No. 116-127**) as amended by the American Rescue Plan Act of 2021 (**Pub. L. No. 117-2**) must review and comply with all

obligations. In addition to the expanded reasons for leave, employers that provide FFCRA leave must also comply with coverage, notice, and pay requirements. For more information on FFCRA leave, see **Covid-19 Emergency Leave**.

In addition to federal law, several states have enacted enhanced paid sick leave requirements in response to Covid-19. Employers should review their paid sick leave policies to ensure they comply with enhanced requirements. See **Search: State Legislative Activity**.

AMOUNT OF SICK LEAVE

Full-time employees earn sick leave at the rate of one day every month. Part-time employees earn sick leave on a prorated basis.

Employees can carry over up to 60 days of sick leave into the following calendar year.

Comment: Most state and local paid sick leave laws set a minimum amount of paid sick leave that an employer must provide. The minimum may be expressed as a set amount of leave that must be awarded to employees when they become eligible, a specific accrual rate that allows employees to earn leave based on the hours they work. Laws that specify an accrual rate generally allow employers to cap paid sick leave at a set number of hours and may allow employers to "front load" leave by providing it to employees at the start of their employment. See **State Chart Builder: Earned Paid Leave (Leave Amount)**; **Local Paid Leave Provisions Chart**.

For employers subject to overlapping state and local leave requirements, the amount of leave provided must satisfy each law.

Employees who are covered by [Employer]'s short-term disability benefits program ordinarily are eligible for short-term disability benefits after five consecutive workdays of paid sick leave. For more information about these benefits, contact [Name of Contact for short-term disability benefits].

Comment: Short-term disability benefits are income replacement benefits funded through private insurance or a state- or city-run program. Unlike earned paid leave, short-term disability benefits are not accrued by employees and do not become available unless an employee experiences a qualifying event. Employees who qualify for benefits generally receive a portion of their salary for the duration of their eligibility. See **State Chart Builder: Temporary Disability Insurance**.

Employees who exhaust their paid sick leave and short-term disability leave may be entitled to additional unpaid leave under the federal Family and Medical Leave Act. Employees who qualify can use unpaid leave for a number of reasons, including the birth, adoption, or placement of a child; because of their own or certain family members' serious health conditions; or to care for a servicemember who becomes seriously ill or injured while serving in the U.S. Armed Forces. For more information on unpaid family and medical leave, see [Employer]'s **Family and Medical Leave Policy**.

Comment: Leave provided under a paid sick leave policy can, but is not required to, run concurrently with the leave required by the federal Family and Medical Leave Act. See **29 U.S.C. § 2612(d)(2)**.

REQUESTING SICK LEAVE

Employees who know in advance of the need for sick leave, such as for a planned doctor or dentist visit, must provide notice to their supervisors ten days prior to the date of leave, or as soon as is practicable.

If employees can't provide advance notice of their need for leave because of a medical emergency or sudden illness or injury, they must notify their supervisors before the beginning of their work schedules or shifts, or as soon as practicable if they are already at the workplace.

Comment: Some state and local laws limit the amount of notice employees can be required to give in advance of planned paid sick leave, so employers should be cautious about such notice requirements in their policy. See **State Chart Builder: Earned Paid Leave (Notification Requirements)**; **Local Paid Leave Provisions Chart**.

MEDICAL CERTIFICATION

Employees who are absent on sick leave for more than three days in a row must provide

written documentation from their health-care provider of their inability to work due to health-related reasons within one business day of returning to work.

Comment: Some state and local laws specify when an employer can require medical certification and what documents can be used to satisfy certification requirements. See **State Chart Builder: Earned Paid Leave (Certification Requirements)**; **Local Paid Leave Provisions Chart**. Generally, employers should avoid medical certification requirements that overly burdensome on employees, such as requiring documentation for short illnesses that do not require medical care.

PAY AND BENEFITS DURING SICK LEAVE

Employee sick leave is considered paid leave. Employees earn their regular rate of pay for leave provided under this policy.

VIOLATIONS OF EMPLOYER'S PAID SICK LEAVE POLICY

Employees who violate this policy can be subject to discipline, up to and including termination, according to [Employer]'s discipline policy.

LABOR & EMPLOYMENT

Checklist – Developing Reasonable Accommodations for Religious Observances & Practices Policies (Annotated)

Editor's Note: Under Title VII of the Civil Rights Act of 1964, employers are prohibited from discriminating against employees and applicants based on religion. See 42 U.S.C. § 2000e-2. Employers also must abide by state and local nondiscrimination laws that can be more expansive in religious protections than federal law. See State Chart Builder: Religious Discrimination. In addition, employers must make reasonable accommodations for employees' religious beliefs, observances, and practices unless the accommodations create undue hardship.

Employers can review the following materials to help them develop and maintain policies on reasonable accommodations for religious beliefs, observances, and practices:

- Reasonable Accommodations for Religious Observances and Practices Policy;
- Religious Accommodation Request and Action Form; and
- Religious Accommodation Evaluation Form.

Policy Pointers

Items employers should consider in developing a reasonable accommodations for religious observances and practices policy include:

General purpose and coordination.

Comment: Policies should include an affirmative statement of employers' commitment to reasonable accommodation of applicants' or employees' religious beliefs, observances, and practices. Policies to accommodate applicants' and employees' religious beliefs, observances, and practices should be coordinated with other company policies such as policies on hiring, promotion, recruiting, job-sharing, and leave. All these policies should be reviewed to ensure that they comply with Title VII and other federal, state, and local nondiscrimination laws.

Sincere beliefs.

Comment: When considering employees' requests for religious accommodation, employers should assess whether employees' work conflict arises from a sincere religious belief. See POL. EEOC guidance states that since the definition of religion is broad, and the employer may be unfamiliar with beliefs, observances, and practices, the employer should ordinarily assume an employee's request is based on a sincerely held religious belief. Traditional and unconventional religious beliefs are protected under Title VII if they are sincerely held.

Accommodating time-off requests.

Comment: Employers often accommodate employees' requests for time off to observe religious holidays or other religious occasions by allowing employees to swap shifts with other employees or take paid or unpaid leave. See POL. Some employers have established a system of floating holidays under which employees are given a number of days of paid leave they can apply toward the holidays of their choice.

Employee transfers.

Comment: If employees have a religious-based conflict with a job, employers might be able to accommodate employees by transferring them to a lateral position that doesn't pose the same problem. See POL.

Holiday policy.

Comment: Holiday policies can help employers avoid inadvertent religious discrimination. Such policies should address how employers treat secular and religious holidays. Employer policies regarding holidays should specify paid and unpaid holidays, eligibility requirements for holiday pay, pay rates, availability of floating holidays, and observance of weekend holidays.

Dress and grooming codes.

Comment: Employers generally must accommodate employees' dress and appearance practices that are based on religion. See **POL**.

Training.

Comment: Employers should implement training for all managers and supervisors on federal, state, and local EEO laws concerning reasonable accommodations for religious observances and practices; they also should train all employees on complying with employers' policies about reasonable accommodations for religious observances and practices. Employers should conduct such training at the time of hire to alert new employees, including managers and supervisors, about reasonable accommodations for religious observances and practices. To ensure compliance with requests for reasonable accommodations for religious observances and practices, employers should conduct annual training on EEO laws concerning reasonable accommodations for religious observances and practices for managers and supervisors, as well as annual training for all employees on employers' policies about reasonable accommodations for religious observances and practices.

Bloomberg Law's Practical Guidance provides task-based, how-to coverage, including overviews, checklists, sample forms and agreements, timelines, drafting and negotiating guides, and more.

Because of our one platform, one price promise, our Practical Guidance is richly integrated with other Bloomberg Law assets – including state Chart Builders, our Precedent Database, news, dockets, Smart Code®, and Points of Law. And we continue to expand and enhance our offerings at no additional cost to subscribers.

*Not a Bloomberg Law subscriber? **Request a demo**.*

"Bloomberg Law is where we look for a general understanding and to answer questions.

Practical Guidance on Bloomberg Law has given me just the type of information I need when I need a quick overview and understanding of a topic. I begin with what is available on Bloomberg Law before I go to a law firm to get advice. It is my go-to resource!"

Deon Retemeyer
Associate General Counsel, NEC

PRIVACY & DATA SECURITY:

Checklist – Key Data Security Questions When Reviewing Vendor Contracts (Annotated)

Contributed by **Melissa Krasnow**, Partner, VLP Law Group LLP, where she advises clients in the education, financial services, health and life sciences, manufacturing and technology areas on domestic and cross-border privacy, data security, big data, artificial intelligence and governance matters, technology transactions and mergers and acquisitions.

If a company has conducted a preliminary assessment of vendors, or if the company has not conducted such preliminary assessment of vendors or does not have such preliminary assessment process, the following checklist raises key questions as a company reviews the terms of a proposed vendor contract.

1. Personal Information

How is personal information defined?

Comment: How personal information is defined can determine whether the contract is favorable to a given party. A broad definition generally favors the company, while a narrow definition favors the vendor, especially in light of security incidents and security practices.

- Does the definition refer to a specific law/regulation, e.g., GDPR, CCPA, CPRA, etc.?

  Comment: Consider whether a specific law/regulation is applicable to the contract or whether a definition from a law/regulation would be appropriate even in the absence of the law's/regulation's applicability.

  Note: The CCPA's provisions remain in effect and are enforceable until the same CPRA provisions become enforceable. The CPRA generally becomes operative on January 1, 2023. CPRA enforcement of the provisions added or amended by the CPRA begins on July 1, 2023.

- Does the definition refer to special categories of personal information, such as sensitive personal information? If so, how are they defined?
- Does the definition refer to a specific contract or document?

  Comment: Determine whether a specifically referenced contract or document is applicable and/or appropriate.

- Are examples of personal information and/or personal information identifiers specified?

  Comment: Determine whether examples of personal information and personal information identifiers are representative of the information at issue in the contract.

Is there a separate definition for confidential information?

- How is confidential information defined?
- Is personal information included in the definition of confidential information?
- Is personal information to be treated as confidential information?

  Comment: If personal information is included in the definition of confidential information or if personal information is to be treated as confidential information, then the provisions for confidential information also need to be taken into account regarding personal information.

Are there types of information defined separately from personal information and confidential information?

2. Applicable Law

Are specific laws/regulations incorporated into the contract?

- If not, should they be?
- If so, in which context?

  Comment: Consider the extent to which a specific law/regulation (e.g., GDPR, CCPA, CPRA, etc.) applies to the contract. Determine what clauses regarding compliance with "all applicable laws and regulations" mean in a particular contract. Review other contracts referenced in clauses incorporating other contracts, including to determine which laws/regulations are cited therein.

Is specific guidance, or are specific industry practices, standards, or frameworks incorporated into the contract?

- If not, should they be?
- If so, how are they included and defined?
- Are they required or recommended as a "best practice"?

  Comment: Certain guidance, industry practices, standards, or frameworks can apply to a company in addition to laws/regulations. Determine their applicability, whether they should be referenced, and which party must abide by them.

Does the contract address potential changes to laws/regulations/guidance, etc.?

Comment: Consider including a clause indicating how the parties should respond to changes in laws/regulations/guidance, etc. affecting their respective obligations. If a forthcoming change is known (such as certain obligations under the CPRA), consider provisions with appropriate effective dates.

3. Security Incident

How is security incident defined?

- Are unauthorized and/or unlawful uses and/or disclosures addressed? If so, how?

  Comment: Unauthorized and/or unlawful uses and/or disclosures can be defined separately from security incident. All definitions should be analyzed together in order to ensure clarity regarding a party's obligations regarding an event or events.

- Is a suspected security incident included in addition to an actual security incident?

  Comment: Suspected security incident language is generally favorable to the company. Sometimes a suspected security incident becomes an actual security incident. The vendor may not agree to suspected security incident language because it may increase the number of security incidents covered by the contract.

- Does the definition incorporate language from or refer to the CCPA?

  Comment: If the CCPA is or could be applicable, CCPA language should be included, i.e., "unauthorized access and exfiltration, theft, or disclosure of nonencrypted and nonredacted personal information as a result of the [vendor's] violation of [its] duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" (Cal. Civ. Code §1798.150). Such language would be generally favorable to the company, and any other CCPA contract requirements should be complied with.

  Note that when the CPRA's provisions become operational on January 1, 2023, language should reflect the updated text, i.e., "unauthorized access and exfiltration, theft, or disclosure of nonencrypted and nonredacted personal information (*including email address together with a password or security question and answer that would permit access to the account*) as a result of the [vendor's] violation of [its] duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" (Cal. Civ. Code § 1798.150, italicized text added by the CPRA). Such language would be generally favorable to the company, and any other CPRA contract requirements could be addressed.

- Are there specific exceptions to the definition of a security incident?

  Comment: Specific exceptions are generally favorable to the vendor. In lieu of exceptions, consider whether reference to a particular law/regulation would be more favorable to the company.

Does the contract address how, when, and to whom a security incident must be reported?

- Who is required to report the security incident?
- Is there a specific contact and contact information for providing and receiving such reporting?
- Is anyone else permitted to provide or receive the report of the security incident?
- Which specific information must be reported?

  Comment: Consider whether a specific list of information would more beneficial than a generic obligation to produce "all relevant information."

- How must it be reported?

  Comment: For example, in writing, via email, etc.

- Must it be reported within a specific time frame?
- Are updates required, and if so, with any particular frequency?

  Comment: Since facts and circumstances can change, an obligation to provide updated information is key. Frequency depends on what the parties negotiate.

- Which actions must be taken to prevent, contain, and mitigate security incident?

Comment: The party that receives the report of the security incident should be provided with information about such actions.

Is a prompt or immediate investigation required?

Is cooperation regarding the security incident required:

- between parties?
- with law enforcement and/or regulators?
- with incident response personnel (internal and external)?
- with insurers and insurance brokers?
- Must a root cause analysis of the security incident be provided?

  Comment: A root cause analysis means a principle-based, systems approach for the identification of underlying causes associated with a particular set of risks (National Institute of Standards and Technology **SP 800-30, Rev. 1**, and **SP 800-39**), in this case, regarding a security incident. Whether a root cause analysis is required to be provided and other details, such as who performs such root cause analysis (for example, a third party), when and how, etc., depends on what the parties negotiate.

Are there restrictions regarding disclosure of or publicity regarding a security incident?

Comment: A party may wish to restrict disclosure of or publicity regarding a security incident to align messaging and minimize the potential for discrepancies.

Does the contract specify which party is to have control of the investigation and management (including notification) of the security incident?

Comment: Both parties may seek to retain control for brand and reputation purposes. Determine notification obligations to affected individuals, regulators, and others under law.

Does the contract specify which party is responsible for costs relating to the security incident (e.g., legal, forensics, credit monitoring, printing and postage, other remediation, etc.)?

Comment: Costs vary depending on the nature and magnitude of the security incident. Certain laws/regulations address obligations relating to credit monitoring (for example, California and Massachusetts breach notification laws).

- Does the contract require mitigation measures and/or actions to prevent recurrence?

  Comment: The party that receives the report of the security incident should be provided with information about such mitigation and actions.

- Does the contract require notification and/or documentation regarding mitigation measures and/or actions to prevent recurrence? If so, to whom and in what format?

4. Security Practices

Does the contract require specific physical, administrative, and technical safeguards?

- If so, what are these safeguards?
- Are the safeguards for personal information only?
- Do they cover confidential information?
- Do they cover other specified or defined information?
- Does the contract require implementation and maintenance of a written information security program (WISP) with specific safeguards?

  Comment: Certain laws/regulations require WISPs; requirements vary. Determine which laws/regulations apply and determine appropriate requirements. If a WISP is not required by law/regulation, consider contract requirements based on specific guidance, industry practices, standards, or frameworks.

Does the contract include security requirements specific to the vendor?

Does the contract require policies and procedures to detect and protect against actual or suspected security incidents?

Does the vendor have separate policies and procedures addressing security?

- If so, what do they cover?

Does the vendor have separate business continuity policies and procedures?

- If so, what do they address?

Does the contract require due diligence and include other measures regarding the vendor's employees and/or subcontractors (such as background checks, training, policy and contract requirements, etc.)?

Does the contract specify access control measures?

Does the contract address and define encryption measures?

> **Comment:** Encryption measures can be defined by law/regulation. See, for example, the California and Massachusetts breach notification laws.

Does the contract specify restrictions on the use and/or disclosure of personal information, confidential information, and/or other specific or defined information?

Does the contract include specifications regarding personal information, confidential information and/or other specified or defined information relating to:

- secure transmission?
- secure storage?
- secure disposal?

Does the contract address monitoring, testing, and updating of safeguards, program, policies and procedures?

Does the contract permit or require assessments or audits of the security program?

- What are the assessments or audits?
- How are they invoked and performed?
- How frequently?
- Who performs them?
- Who pays for them?

Does the contract specify that deficiencies found in the security program must be corrected?

- If so, how must correction of such deficiencies be communicated and to whom?

PRIVACY & DATA SECURITY:

Overview - Drafting Privacy Policies

Adapted from Privacy & Data Security Practice Portfolio Series 545, ***Drafting Privacy Policies for Websites, Apps and Other Digital Services***, by ***Julia Jacobson***.

Consumers provide companies with a great deal of personal information, including sensitive information about their finances, their health and other data that can open them up to identity theft and fraud. However, they often do not fully understand how the company will use that information or share it with others, or that they have certain rights regarding the information.

Privacy policies are an important tool for businesses—from financial institutions and healthcare providers to any company that has a website—to help their consumers understand how they will collect, use, store, share and transfer personal information. These policies also allow companies to garner good will and trust from consumers by emphasizing the companies' respect for consumer privacy and transparency about their practices. Thus, even when notifying consumers about privacy practices is not required by law, it is a good idea for a company that provides digital services to offer one.

Drafting a privacy policy that is sufficiently clear, accurate and transparent for consumers to make informed choices about sharing information is no easy task. Privacy policies are often difficult for users to understand—they can be tediously long and full of legal jargon. They can also fail to fully describe the privacy practices the company actually follows, rather than aspires to follow, or may make promises that are impossible to keep, since there is always some risk of data breach even at the most responsible companies. Making inaccurate statements and promises in a privacy policy can expose a company to lawsuits, enforcement actions and damages to reputation.

The complex patchwork of both state and federal legal and regulatory requirements that may apply to a privacy policy also complicates the drafting process. For instance, websites that are directed toward children must comply with the requirements of the Children's Online Privacy Protection Act (**15 U.S.C. §§6501–6506**).

"Bloomberg Law's Practical Guidance saves my department time and money by providing a significant repository of sample forms, agreements, and checklists to help me get started on solving problems."

CLO
Financial Services Firm

Health-care providers, health plans and health-care clearinghouses must comply with the requirements for protected health information in the Health Insurance Portability and Accountability Act (**Pub. L. No. 104–191, 110 Stat. 1936** (1996)) and its Privacy Rule (**45 C.F.R. Part 160**, Part 164, Subparts A and E). In addition to posting a general privacy policy for users of their websites and mobile apps, businesses that are significantly engaged in financial activities must post a notice of privacy practices for financial information in accordance with Federal Trade Commission (FTC) requirements. And many state laws and regulations, such as those regulating how businesses address data breaches, will influence what provisions are included in a privacy policy.

Privacy Policies for Digital Service Providers

Any business that provides a website, mobile application or other Internet-connected service (collectively, digital services), should post a privacy policy in a clear, conspicuous place on the service. Since the policy will often be the only explanation of the service's privacy practices that users encounter, the drafter should make sure it is accessible to the average user, uses plain, approachable language, and accurately represents the information practices in a way that allows the user to make an informed choice about using the service.

Begin drafting this type of policy by conducting a pre-drafting review of the digital service, as described in the **Privacy Policy Drafting Checklist**

for Digital Service Providers. This will involve utilizing the service as a user would, interviewing various personnel at the digital service provider, and reviewing laws and regulations. This review should focus on both factual inquiries, such as what type of information is collected, how it is collected, what it is used for, and how the digital service provider stores and safeguards it, as well as legal inquiries, such as whether the digital service provider collects sensitive information subject to additional regulation, what state laws are applicable, and whether relevant trade organizations have self-regulatory schemes.

Next, determine the structure of the policy. Consider using multiple layers—a brief highlights section and a more complete policy, as well as a set of frequently asked questions or a Glossary of terms that may not be familiar to the general public. Once the structure is planned, drafting can begin. Review the **Sample Privacy Policy for Businesses That Maintain Digital Services** to get a sense of what should be included and how it should be worded, and make sure the policy includes the essential provisions described in the **Privacy Policy Drafting Checklist**.

In addition to drafting a public-facing privacy policy for display on the digital service, it's also good practice for a digital service provider to create an internal **Sample Information Security and Data Privacy Policy** that applies to employees, contractors, associates and third parties who access information collected by the provider. This document should set out much more detailed policies and procedures for how information is physically secured, how electronic information is secured from unauthorized access and how the provider ensures that these policies are followed. This policy should be for internal use only and should not be released to the general public so as to prevent potential hackers from accessing information.

Privacy Policies for Financial Institutions

As part of the Gramm-Leach-Bliley Act (**Pub. L. No. 106-102**, **113 Stat. 1338** (1999)) and its Privacy Rules (**16 C.F.R. Part 313**), the FTC requires financial institutions to provide special privacy notices to customers. "Financial institution" is defined to include all businesses "significantly engaged" in financial activities. The term applies to a broad range of businesses, some of which are obviously financial institutions (e.g., banks, lenders, mortgage brokers, credit reporting agencies and ATM operators) and some of which would not normally describe themselves as financial institutions (e.g., accountants and other tax preparation services, retailers offering their own credit cards, automobile dealerships that offer leasing, and appraisers). The FTC requires all financial institutions' privacy notices to describe their information collection and sharing practices and advise customers of their right to opt out of certain practices. This notice must be provided to new customers, generally at the time they become customers, and to existing customers on an annual basis.

To make it easier for customers to comprehend a financial institution's privacy practices and to compare different institutions' practices, the FTC, in conjunction with several other agencies, released a succinct, two-page **Model Privacy Notice Form**. While institutions are not required to use the Model Form and may instead craft their own, those that use it consistent with its instructions are deemed to satisfy the FTC's legal and regulatory disclosure requirements. To be deemed compliant, the financial institution also must present the Model Form in a way that is clear, conspicuous, and intact and must use the same page orientation (portrait), format, and order of elements of the Model Form. Institutions may not change the content of the form or add any information, except as specifically permitted in the instructions, and may customize the form only where the Model Form expressly allows.

The FTC released two versions of the Model Form: **one that includes opt-out provisions** and **one that does not**. Financial institutions are required to use the opt-out version only if they share or use information that triggers an opt-out (that is, if they share information with affiliates about consumers' creditworthiness or with affiliates or non-affiliates for use for marketing to consumers).

Privacy Policies for Covered Entities under HIPAA

Under the HIPAA Privacy Rule, "covered entities" are required to comply with certain requirements governing use and disclosure of the individually

identifiable health information they maintain (known as "protected health information" or PHI). "Covered entities" include health-care providers, health plans and health-care clearinghouses (i.e., businesses that process health data or transaction information, such as billing services).

Under the Privacy Rule, covered entities are required to develop and distribute a Notice of Privacy Practices. As discussed in greater detail in **Guiding Principles for Drafting Notices of Privacy Practices**, this notice should explain, in a clear and accessible manner, individuals' rights with respect to their PHI and the privacy practices of **health plans** and **health-care providers**, including uses and disclosures. The Department of Health and Human Services (HHS) developed Model Notices of Privacy Practices for both health plans and healthcare providers to improve patient experience and understanding.

Covered entities should also develop more robust descriptions of information practices in documents like the **Sample HIPAA Privacy Policies and Procedures**. This document should go into greater depth than the Notice, providing instructions to patients for who want to exercise certain rights regarding PHI and setting out internal protocol for handling PHI, responding to requests and complaints and ensuring compliance with the Privacy Rule.

In addition to ensuring that its own information practices comply with HIPAA, a covered entity must ensure that its business associates (i.e., those who perform functions and provide services on behalf of the entity) appropriately safeguard PHI they receive, create or maintain on the entity's behalf. HHS issued **Sample Business Associate Agreement Provisions** that covered entities can use in contracts to ensure that their business associates are obligated to meet HIPAA requirements for using and protecting PHI.

Privacy Policies for Employers

In general, employers may monitor employee usage of employer electronic communications systems and devices, but if they do so, they should inform employees of these practices. One of the most effective ways to do this is to incorporate electronic communications policies, like those set out in the **Model Notice of Electronic Communications Practices for Employers**, into employee guidelines. These policies should cover whether the employer monitors employee usage of the employer's electronic communications systems and devices, when the employer and third parties will access employee corporate e-mail accounts and other computer files, and what monitoring the employer will do when employees use their own electronic devices or personal accounts.

TRANSACTIONAL:

Sample Clause – Pro-Buyer Supplier Business and Supply Continuity Covenant (Annotated)

Editor's Note: In this supply agreement provision, the supplier covenants to undertake various measures to ensure the continuity of its supply to the purchaser.

Sample Language:

X. Business and Supply Continuity

(a) Supplier recognizes and acknowledges its obligation hereunder to provide a reliable, responsive, and uninterrupted supply of [product to be supplied] to Buyer for the purpose of [insert name of business (e.g., "the operation of its soft drinks business unit"), or end product to be manufactured (e.g., "manufacturing jet engines")]. Supplier shall maintain relationships with various alternative sub-suppliers that may be relied on by Supplier in the event of any disruption to Supplier's existing sources of supply and/or in any event Supplier is unable to furnish [product to be supplied] as required hereunder.

(b) Supplier shall develop and maintain a contingency plan for supplying [product to be supplied] hereunder for events that would otherwise interrupt a reliable supply chain. This plan shall be tested, updated and maintained throughout the term of this Agreement. Supplier shall review this plan on an [Annual or other periodic] basis with representatives from the Buyer.

(c) To further protect against business and/or supply disruptions, Supplier shall, when reasonably available and commercially feasible, obtain and maintain business interruption insurance covering any loss due supply chain interruptions. Such insurance shall be maintained on terms and conditions that are consistent with [industry best practices] and acceptable to the Buyer.

Comment: The purpose of this provision is to require the supplier to make a three-fold commitment to ensure the continuity of its supply to the purchaser under the supply agreement. The supplier is agreeing to (1) maintain relationships with alternative or "Plan B" suppliers, (2) create and maintain a supply contingency plan (access law firm research on supply contingency plans **here**.), and (3) obtain business interruption insurance. This supplier covenant may be included in the "commercial terms," "terms and conditions," "purchase terms," "terms of purchase," or other similar section containing covenants and terms of a supply agreement or purchase agreement. This provision would work in tandem with and complement other provisions in the agreement addressing changes to the supply, notice requirements, buyer approval of supplier modifications to the supply, delays, etc. This provision may be tailored to meet special concerns of the buyer, and to reflect specifics of the supply relationship at hand, for example addressing domestic and international dual sourcing arrangements, and/or logistics concerns.

While this provision is styled as a commercial term or supplier covenant, it may, additionally or alternatively, be written as a representation and warranty stating that each of the three safeguards included above are in place at the time of the execution of the agreement. The advantage of including these safeguards as supplier covenants is that they remain as active requirements the seller must comply with through the life of the contract whereas representations and warranties reflect the status or compliance of the supplier at the point in time when the representations are made. It could be advantageous to a buyer to have both covenants and representations and warranties regarding these supply chain safeguards included.

Example Clause Searches: Access our Transactional Precedent Database for **contingency plan provisions**, **sub-supplier provisions**, and **business interruption insurance** provisions in publicly filed supply agreements.

Value/Risk Analysis: Supply chain vulnerabilities compel parties to incorporate safeguards into critical supply agreements. This type of provision is of especially high value in key supply contracts that are critical to the business continuity of the buyer. The risk of not including such safeguards is that a buyer is left to depend on the supplier's own judgment and plans to protect against supply chain interruptions without having a formal contractual say in what those safeguards should be.

Affected Clauses:

- **Definitions.** Terms such as "sub-supplier," "contingency plan," "business interruption insurance," and the like may be needed to be added to the definitions section of the agreement to which this provision is added.
- **Notice requirements.** Notice requirements may be triggered by this provision.

- **Representation and warranties.** This provision is styled as a commercial term or supplier covenant. Additionally, or alternatively, parties could include supplier representations and warranties stating that each of the three safeguards included above are in place at the time of the execution of the agreement.
- **Insurance.** This provision may need to be harmonized with or referenced by other insurance related provisions in a supply agreement to which it is being added.
- **Termination.** The parties may elect to make failure to comply with this provision a breach that triggers termination rights.

TRANSACTIONAL:

Sample Clause – Mutual Indemnification for Data Breach (Annotated)

Editor's Note: This mutual indemnification for data breach clause provides for specific indemnity in the event that a **data breach** (which may be referred to as a security breach, data incident, information security incident, or similar term) has actual or potentially adverse effects on the confidentiality, integrity, or availability of data entrusted to a contracting party as part of a transaction. It may be inserted into contracts that involve the bilateral sharing or exchange of data between parties in a similar bargaining position, including for commercial contracts such as services, sales, consulting, and strategic partnership agreements. This clause may also supplement, or be incorporated in part into, a **broad general indemnification clause**.

"Bloomberg Law's Practice Guidance resources provide us with built in categories that have been curated by Bloomberg lawyers who have put significant thought into which specific areas of every single process needs guidance, saving us the time and expense of having to seek help from outside counsel."

AVP, Legal Operations
Financial Services Firm

Sample Language:

SECTION [X]. Indemnification for Data Breach

Each Party ("Indemnifying Party") agrees to defend, indemnify, and hold harmless the other Party, its subsidiaries and its and their respective successors, assigns, directors, officers, employees, agents, and affiliates (each, an "Indemnified Party" and collectively, the "Indemnified Parties") from and against all claims, demands, actions, suits, damages, liabilities, losses, settlements, judgments, fines, penalties, costs, and expenses [incurred as a result of a third-party claim], including but not limited to reasonable attorneys' fees and reasonable costs of computer forensics work required for security incident investigations[, notifications to affected individuals and other entities as required by law, credit monitoring or identity theft services provided to affected individuals for a period not to exceed the greater of twelve (12) months or the time required by law, a call center to respond to inquiries of affected individuals for a period not to exceed the greater of thirty (30) days or the time required by law,] and any other security incident remediation efforts that are commercially reasonable under the circumstances (collectively, "Claims and Costs"), directly or indirectly arising out of or related to an [actual or suspected] occurrence of unauthorized access, acquisition, disclosure, or use of an Indemnified Party's Confidential Data [or Personally Identifiable Information] while in the possession of or under the control of the Indemnifying Party, its contractors, or agents in connection with this Agreement [and as a result of the acts or omissions of the Indemnifying Party, its contractors, or agents] (each such occurrence, a "Data Breach")[, to the extent that such Claims and Costs did not result from the acts or omissions of an Indemnified Party].

Comment: An indemnification provision that addresses data breaches allows parties to allocate responsibility for the types of claims and costs typically associated with a party's data becoming compromised by an information security incident, regardless of the relative fault or ordinary negligence of the parties. Bracketed language in this sample clause would limit responsibility to data breaches that result from an indemnifying party's own acts or omissions, as opposed to, for example, a company that falls victim to a hack despite implementing reasonable data security measures and meeting all of its contractual obligations relating to data protection. Indemnification can be further limited to a data incident that results from a breach of specific provisions of the agreement, such as representations concerning data security requirements or compliance with certain applicable privacy laws. Parties may also negotiate exceptions for liabilities stemming from the acts or omissions of the party impacted by the data breach, as the bracketed exception at the end of this sample clause shows.

Bracketed language in this sample clause also allows the option to limit the types of costs that an

indemnifying party would be responsible for to those that result from a third-party claim, rather than costs that a party may incur while investigating the nature and scope of a data breach or hiring outside counsel in anticipation of possible litigation. Similarly, other bracketed language in this sample provides the option of expressly stating that even a suspected, yet-to-be-confirmed data breach may trigger indemnification responsibilities, such as covering the costs of hiring a computer forensics team to determine if confidential data was in fact exposed.

The types of claims, costs, and other liabilities that may stem from a data breach depend on whether personally identifiable information ("PII"), or data that can be used to identify a specific individual, was stolen or exposed. When PII is involved in a data breach, the types of potential third-party claims can expand from aggrieved proprietary data owners to state and federal regulatory agencies and even affected individuals with a private claim of action. The unauthorized disclosure of PII can also increase the range of potential breach remediation costs from a standard security incident investigation to mandatory reporting and notifications and even the offering of credit monitoring services and call center support for affected individuals. Bracketed language in this sample clause allows the option to include such costs.

For additional practice guidance on data breach management and terminology, refer to the **Overview of Data Breach Management**, **Sample Policy for Incident Response Plan**, **Federal & State Breach Notification Requirements**, and **Defined Contract Terms Relating to Data Privacy & Security**. For additional practical guidance on indemnification in general, refer to **Clause Description – Indemnification Provision** and **Sample Clause – Indemnification Provision**.

Example Clause Search: Access our Transactional Precedent Database for **Indemnification for Data Breach Clauses** in publicly filed agreements.

Value/Risk Analysis: An indemnification for data breach clause can protect parties from the unique risks and significant expenses associated with the investigation, remediation, and legal defense of an information security incident and can help fill in the cost coverage gaps that may be left by traditional remedies for breach of contract. If the contracting parties are unable to agree upon the matter of indemnification for data breach, either in a stand-alone provision or as part of a general indemnification clause, each party providing sensitive or highly-valuable data should ensure that there is some form of protection from the sizable costs involved in a breach, such as through the limitation of liability clause's categories of compensable losses.

Affected Clauses: Clauses potentially impacted by the inclusion of an indemnification for data breach provision, and which may impact the provision itself, include but are not limited to:

- **Privacy and Data Security Requirements.** Specific data-related requirements in the agreement may be referred to in a data breach indemnification clause to trigger indemnity or provide for an exception to indemnification when the injured party has failed to follow such requirements.
- **Information Security Incident Response Procedures.** An agreement may contain required procedures that govern both internal and external steps to take in response to a data breach, such as when to notify authorities and how the parties must cooperate in the investigation and remediation of a breach. Such procedures may impact indemnification triggers and exceptions.
- **General Indemnification**. A stand-alone indemnification for data breach clause should take precedence over an agreement's general indemnification clause with regard to the triggers, exceptions, and covered claims and costs that are uniquely applicable to an information security incident. Parties should carefully review all indemnification language in a contract and ensure that the order of precedence in the event of a conflict between terms has been properly addressed.
- **Limitations of Liability.** Because the costs associated with the investigation, remediation, and legal defense of a data breach can be extremely high, parties will often cap the maximum amount of out-of-pocket expenses that they may owe as an indemnifier. Limitations of liability provisions also often provide exceptions to prohibitions on consequential damages and compensable losses related to a breach of confidentiality or data security obligations and for indemnification generally.
- **Insurance.** **Cyber insurance coverage**, as well as some traditional insurance policies that cover certain **cyber-related losses**, may provide relief for expenses incurred from investigation, remediation, and asset losses stemming from a data breach. A party providing sensitive data may require the recipient of such data to carry specific policies. The parties may also negotiate caps on maximum indemnifiable amounts that align with the applicable limits of their respective policies.
- **Force Majeure.** A **force majeure clause** could impact fault-based indemnity for data breach if a party relies on a force majeure event as an excuse to suspend its performance of data-related obligations. If a data breach occurs as a result of such suspension, the injured party could be left without a method of recovering expenses. Parties sharing data should ensure that their force majeure clause expressly exempts privacy and data security requirements, any business continuity or disaster recovery provisions that address data restoration and recovery, and obligations related to compliance with privacy laws from being subject to a force majeure suspension of performance.

- **Applicable Law.** Agreements may specify which laws are applicable to the transaction and allocate responsibility for compliance in accordance with each party's respective industry expertise, especially in the area of **privacy and data security** where there are many industry-specific areas of compliance that may apply based on categories of data involved, proposed uses, and jurisdictions. **State privacy and data security laws** can vary significantly by data type and industry sector.
- **Definitions.** In particular, the definitions of terms such as "Confidential Information", "Personally Identifiable Information", "Data Breach", and "Third-Party Claims" will be material to drafting a clear and effective indemnification for data breach clause that properly addresses the nature of the transaction, types of data, and information systems involved. Definitions may also include terms related to **privacy and data security laws and regulations** that are applicable to the transaction.

LEGAL OPERATIONS:

Checklist – Project Management for Legal Operations: Step by Step

Editor's Note: This document is part of a Practical Guidance series focused on **Project Management for Legal Operations**. For additional coverage of legal operations and related topics, see our **Legal Operations** practice page.

Below are steps that can be used to guide legal operations projects. For more information, see **Overview – Project Management for Legal Operations**.

Step 1: Determine Project Needs

- ❏ Identify relevant stakeholders.
- ❏ Determine general timelines, budget, project objectives, and project scope with stakeholders.
- ❏ Memorialize this information as an initial set of requirements.

For more information, see **Overview – Planning for Legal Operations Projects**.

Step 2: Build the Project Team and Roles

- ❏ Determine what roles are needed on the project (i.e. project manager, analyst).
- ❏ Select team members with knowledge and experience relevant to the project and roles.
- ❏ Assign team members roles based on their skills.

For more information, see **Overview – Building a Team for Legal Operations Projects**.

Step 3: Gather Formal Project Requirements

- ❏ Assign requirements gathering to the appropriate team member(s).
- ❏ Meet with stakeholders to outline the requirements for the project.
- ❏ Set up a meeting with stakeholders to discuss any conflicting requirements.
- ❏ Finalize requirements and review with stakeholders to ensure understanding.
- ❏ Document all requirements in a repository.
- ❏ Develop and formalize success criteria through which the project will be evaluated.

For more information, see **Checklist – Developing Requirements for Legal Operations Projects**.

Step 4: Develop Project Charter and Plan

When drafting the project charter, work with stakeholders to:

- ❏ Identify and document all stakeholders.
- ❏ Formalize and document the goals, scope, and budget of the project.
- ❏ Draft the charter with all relevant information, timelines, and stakeholders.
- ❏ Review the charter with stakeholders and finalize.

When drafting the project plan, work with stakeholders to:

- ❏ Document objectives, scope, timelines, schedule, and deliverables/outcomes.
- ❏ Document each role and stakeholder in the project.
- ❏ Identify and document project risks and dependencies.
- ❏ Review the plan with stakeholders and finalize.

For more information, see **Overview – Project Management Documentation for Legal Operations**, **Worksheet – Project Plan**, and **Worksheet – Project Charter**.

Step 5: Develop the Communication and Change Management Plans

- ❏ Determine objectives for the plans.
- ❏ Determine the audience for each communication or activity.

- ❏ Determine the information that will be communicated to each audience.
- ❏ Set up a communication or activity cadence.
- ❏ Select the medium of communication, if applicable.
- ❏ Create an official timeline of when communications and/or activities should be executed.

For more information, see **Overview – Change Management and Communications**, **Worksheet – Project Communication Plan**, and **Worksheet – Project Change Management Plan**.

Step 6: Develop the Product or Process

- ❏ Determine the design elements that the project team will handle.
- ❏ Review requirements and develop specifications for the design.
- ❏ Review the product or process with stakeholders and finalize.

Step 7: Develop the Training Plan

- ❏ Determine the changes that the project will represent for the organization.
- ❏ Determine the best training methods and materials to use.
- ❏ Design training courses and materials.
- ❏ Create schedule and timeline of training activities.
- ❏ Review the training plan with stakeholders and finalize.

For more information, see **Overview – Training Techniques for Legal Operations Projects**.

Step 8: Execute the Project

- ❏ Execute the communication plan.
- ❏ Execute the change management plan.
- ❏ Execute training activities.
- ❏ Eaunch the product or process.
- ❏ Meet with the organization to provide more information and training as needed.

For more information, see **Overview – Executing a Legal Operations Project** and **Checklist – Executing a Legal Operations Project (Step-by-Step)**.

Step 9: Monitor the Project

- ❏ Meet with users and get their feedback on the project.
- ❏ Measure success of the process or product using success metrics.
- ❏ Make changes to the project to account for any deficiencies.

For more information, see **Overview – Monitoring a Legal Operations Project** and **Checklist – Monitoring a Legal Operations Project (Step-by-Step)**.

Step 10: Close Out the Project

- ❏ Create a project report containing lessons learned and presenting findings to stakeholders.
- ❏ Perform due diligence activities.
- ❏ Ensure that all requirements were met.
- ❏ Transition responsibilities to permanent roles in the organization.

For more information, see **Overview – Closing Out a Legal Operations Project** and **Checklist – Closing Out a Legal Operations Project (Step-by-Step)**.

LEGAL OPERATIONS:

Checklist – Developing Requirements for Legal Ops

Editor's Note: This document is part of a Practical Guidance series focused on **Project Management for Legal Operations**. For additional coverage of legal operations and related topics, see our **Legal Operations** practice page.

Step 1: Plan

- ❑ Assign the appropriate team member(s) to gather requirements
- ❑ Determine with which stakeholders the team members need to consult
- ❑ Determine the appropriate kind of meetings to host with stakeholders (one-on-one, group, etc.)
- ❑ Develop questions to ask stakeholders to elicit requirements
- ❑ Determine if any tools, such as surveys, will be used to gather requirements
- ❑ Develop/Prepare any tools being used to gather requirements, if applicable
- ❑ Set up meetings with stakeholders to gather requirements

For more information, see **Overview – Planning for Legal Operations Projects**.

Step 2: Gather an Initial Set of Requirements

Meet with stakeholders to outline the project requirements

- ❑ Launch any tools being used to gather project requirements, if applicable
- ❑ Document identified requirements
- ❑ Evaluate documented requirements and identify any contradictions/conflicts

Step 3: Finalize the Requirements

- ❑ Meet with stakeholders to discuss conflicting requirements, if applicable
- ❑ Resolve conflicting requirements, if applicable
- ❑ Revise requirements documentation, if applicable
- ❑ Review revised documentation with stakeholders to ensure accuracy and understanding of the requirements, if applicable
- ❑ Reflect any further changes from the stakeholder review in requirements document, if applicable
- ❑ Review finalized requirements and any changes with stakeholders
- ❑ Save finalized requirements

LEGAL OPERATIONS:

Checklist – Responding to Mistakes

Editor's Note: This document is part of a series focused on lawyer development. For more information, see the **Lawyer Development Toolkit** and **In Focus: Lawyer Development**.

This checklist is intended to provide some general guidance if you realize you may have made a mistake on a legal matter.

A few items to keep in mind:

- Not all mistakes are equal. Some may have a simple fix and some may be more complicated.
- Legal ethics is a specialized area full of nuance so consider seeking expert guidance, especially for more serious issues.
- Be mindful of the existence of attorney-client privilege when disclosing the error to internal counsel.
- Exercise care when disclosing potential errors to the client to avoid negating insurance coverage.

For resources on a lawyer's ethical obligations, including ethics opinions, state ethics rules (click on any state in the map), secondary sources, and more, see **ABA/BLAW Lawyers' Manual on Professional Responsibility**.

❏ **Don't ignore it.** Ignoring a potential issue or hoping no one notices has been proven to be a poor strategy. And fraudulently concealing an error is not something you want to be accused of doing.

❏ **Don't jump to conclusions.** It is tempting to start playing out worst case scenarios. Try to stay calm and measured so you can thoughtfully consider your options and next steps.

❏ **Be proactive.** Once you realize a mistake has been made, conduct your own investigation about the cause of the mistake, the scope of the mistake, whether it can it be rectified, and what the potential ramifications are for the client. Before discussing it with someone, get all the information together to be able to answer the most predictable questions and have a suggested plan of action ready. Being proactive about responding will show you are taking the mistake seriously and don't expect others to clean up your mistakes.

"The high level view of patent law provided by Bloomberg Law gives a good refresher on some topics that do not come up routinely in practice and I can refresh my understanding of topics. For contract drafting, the research and details that Bloomberg Law provides is invaluable in saving time and money in repeated drafting and editing."

Don Smith, Associate IP Counsel
Zebra Technologies

PRACTICE TIP: Depending on the size of the mistake, this internal investigation could take as little as 15 minutes or as long as several hours. However, you don't want to wait several days before taking affirmative steps to rectify the mistake or disclosing it to a supervising attorney to ask for guidance.

❏ **Seek practical guidance, especially for smaller mistakes.** Determine with whom to discuss the mistake, as well as the timing. The timing likely will depend on the gravity and urgency of the matter. It is prudent to disclose the mistake and seek guidance as soon as you have wrapped your arms around the problem.

❏ **Seek ethics guidance, especially for more serious mistakes.** Many firms have an ethics committee that fields questions about ethical issues. Bar associations also have ethics hotlines where you can seek confidential guidance on the rules of professional responsibility. Both are great resources, along with mentors and colleagues. BUT,

before seeking guidance from internal resources, you should confirm the scope of any attorney-client privilege with such internal counsel. Some communications with internal ethics counsel may be privileged and thus not subject to disclosure to the client, and some may not. This issue must be raised at the outset before disclosing the facts concerning the potential error.

- ❏ **Your response is important.** How mistakes are handled is often even more significant than the mistake itself. Be honest and own your mistakes. Attempting to deflect blame or delay reporting the issue ultimately is unlikely to work in your favor.
- ❏ **Carefully consider whether an error was made before disclosing externally.** Although lawyers owe certain ethical duties of communication to clients,before disclosing any potential error, consider: (1) whether an error was in fact made and (2) whether the error is likely to harm or prejudice the client. Some errors, even if deemed harmless, could cause the client to consider terminating the representation. Such errors would likely need to be disclosed to a client. Obviously not all errors are created equal. Some may be minor and fixable, while others are substantial and are damaging to the client. If you are unsure whether the error should or must be disclosed to a client, it is wise to consult with an ethics lawyer. For more on a lawyer's obligations to disclose potential errors to clients, see, e.g., **Ethics Opinions Search**.

PRACTICE TIP: Some mistakes won't rise to the level of needing to tell the client. For example, if you forget to add a case citation or fact to an opening brief on an issue, but are able to include it in the reply brief without objection so there is no harm, no foul, that may not need to be disclosed to the client. Use your judgment and discuss your mistake internally before revealing it externally.

- ❏ **Carefully choose your words with the client.** Disclosing a mistake to a client is an issue that should be vetted with legal ethics experts. While it is often advisable, even when not ethically required, to be up front about an error being made and discuss potential recourse for the client (e.g. seeking independent counsel; right to terminate the representation), discussing ***liability*** could vitiate any insurance coverage. Thus, great care must be taken when communicating with the client.
- ❏ **Consider whether the representation can continue.** Once a conflict arises to a certain level between a lawyer and a client, the representation cannot continue. If the mistake is significant, raise the issue with ethics counsel who will be able to conduct the appropriate conflicts analysis.

About Bloomberg Law

Bloomberg Law combines the latest in legal technology with workflow tools, comprehensive primary and secondary sources, trusted news, expert analysis, and business intelligence. Our deep expertise and commitment to innovation provide a competitive edge to help improve attorney productivity and efficiency. Bloomberg Law is the only legal research provider to include continuous enhancements to its platform at no cost to existing subscribers. For more information, visit **Bloomberg Law**.

MKT-468683 0422rc