Centre for Information Policy Leadership
Hunton Andrews Kurth

3 July 2019

# The Concept of "Organizational Accountability"
# Existence in US Regulatory Compliance and its Relevance for a Federal Data Privacy Law

**CIPL Paper Snapshot**

- **Organizational accountability exists in many areas of US law, including anti-corruption, corporate fraud and white-collar crime, anti-money laundering and healthcare.**
- **Organizational accountability should be included in any new federal data privacy law to ensure corporate digital responsibility among all organizations.**
- **Omitting accountability from a new federal data privacy law will be detrimental to the success of any new regime and to the American public.**

## Executive Summary

As the US considers the adoption of a comprehensive federal privacy law, numerous stakeholders, including industry representatives and privacy think tanks, such as the Centre for Information Policy Leadership (CIPL),[1] have raised the importance of incorporating the concept of "organizational accountability" into any new US privacy law. Accountability is now globally recognized as a key component of effective privacy and data protection regulation. This global acceptance, however, creates the misconception for some that this concept is somehow a foreign import and does not fit within US corporate and legal culture. Accountability is also sometimes misunderstood as a concept that is too vague or hard to define, or as something that is promoted by industry in lieu of strict and enforceable privacy rules. Nothing could be further from the truth.

The concept of organizational accountability is deeply engrained within the current US legal system across a variety of regulatory areas and can be traced back to the enactment of the Foreign Corrupt Practices Act (FCPA)[2] in the late 1970's and the Sarbanes-Oxley Act (SOX Act)[3] in the early 2000's. The purpose of this paper is to show the US origins of this concept and to demonstrate that its current application in US law lends significant support for also including organizational accountability in any new federal privacy law.

Accountability is sometimes referred to in US law as corporate responsibility, governance, stewardship or duty. Whichever term is employed, in essence, the concept of accountability simply means that organizations must take necessary steps to implement applicable legal and regulatory requirements through a comprehensive compliance program and be able to demonstrate the existence and effectiveness of such a program – both internally (to Board and senior level management) and externally on request (to regulators, individuals and business partners). In the privacy context, this means that organizations should have comprehensive internal privacy programs that implement all relevant privacy requirements in a manner that can be demonstrated to an enforcement authority on demand. Creating such a program thus becomes a value and an enforceable requirement in and of itself.[4]

## A. The Essential Elements of Accountability

For purposes of comparison to other areas of US regulatory compliance, accountability-based data privacy and governance programs typically encompass and address the following seven core elements of accountability:

1. ***Leadership and Oversight***: Establishing leadership and oversight for data protection and the responsible use of data, including governance, reporting, buy-in from all levels of management and appointing appropriate personnel to oversee the organization's accountability program and report to management and the board.

2. ***Risk Assessment***: Assessing and mitigating the risks that data collection and processing may raise to individuals, including weighing the risk of the information use against its benefits. Risk assessment also means conducting periodic reviews of the organization's overall privacy program and information uses in light of changes in business models, law, technology and other factors and adapting the program to changing levels of risk.

3. ***Policies and Procedures***: Establishing internal written policies and procedures that operationalize legal requirements, create concrete processes and controls to be followed by the organization, and reflect applicable law, regulations, industry standards as well as the organization's values and goals.

4. ***Transparency***: Providing transparency to all stakeholders internally and externally about the organization's data privacy program, procedures and protections, the rights of individuals in relation to their data and the benefits and/or potential risks of data processing. This may also include communicating with relevant data privacy authorities, business partners and third parties about the organization's privacy program.

5. ***Training and Awareness***: Providing training for employees to ensure awareness of the internal privacy program, its objectives and requirements, and implementation of its requirements in line with the employees' roles and job responsibilities. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility.

6. ***Monitoring and Verification***: Monitoring and verifying the implementation and effectiveness of the program and internal compliance with the overall privacy program, policies, procedures and controls through regular internal or external audits and redress plans**.**

7. ***Response and Enforcement***: Implementing response and enforcement procedures to address inquiries, complaints, data protection breaches and internal non-compliance, and to enforce against acts of non-compliance.

These seven elements are consistent with other areas of US corporate law and compliance. They follow the framework of Chapter Eight of the United States Sentencing Commission Federal Sentencing Guidelines Manual[5] and have been used by US regulators to determine if an organization has maintained an effective and comprehensive compliance program in various areas of regulation, as discussed in detail below.

**B. Organizational Accountability's Existence in US Regulatory Compliance Structures**

The following section highlights various areas of US law where organizational accountability plays an important role in achieving compliance and the key features of accountability within each regulatory area. A mapping of these features to the elements outlined above can be found in Appendix A of this paper. For a full discussion of each law and regulatory framework mentioned below, see Appendix B.

**Regulatory Area: Anti-Corruption**

**1. *United States Department of Justice and the Securities and Exchange Commission Resource Guide to the US Foreign Corrupt Practices Act (FCPA)***

In many ways, the FCPA of 1977 symbolized the beginnings of corporate compliance programs in the United States. In November 2012, the Criminal Division of the United States Department of Justice (DOJ) and the Enforcement Division of the United States Securities and Exchange Commission (SEC) released a resource guide to the US Foreign Corrupt Practices Act (FCPA Guide).[6] The FCPA Guide covers a wide variety of topics, including the hallmarks of effective compliance programs.[7] These hallmarks correspond to the essential elements of accountability put forward in Section A above. They include a commitment from senior management and appropriate oversight against corruption; assessing risk to develop a strong compliance program; having in place anti-corruption compliance policies and procedures; communicating such policies to staff, management and external stakeholders; training and continuing advice; periodic testing and review of the program; as well as implementing disciplinary measures, reporting mechanisms and conducting internal investigations. For an in-depth discussion of the FCPA Guide and these hallmarks, please see Appendix B.

**Regulatory Area: White-Collar Crime and Corporate Fraud**

**2. *Sarbanes-Oxley Act of 2002***

In response to major scandals of corporate malfeasance and accounting fraud in the early 2000's, including those involving Enron Corporation, WorldCom, Tyco and accounting firm Arthur Andersen, the US enacted the Sarbanes-Oxley Act of 2002[8] (SOX Act) (introduced as the Corporate and Auditing Accountability, Responsibility, and Transparency Act of 2002 in the US House of Representatives). The SOX Act was created to crack down on corporate fraud and white-collar crime and to reform American business practices. It has had a profound effect on corporate accountability and governance over the past 17 years. Specifically, the SOX Act caused a huge spike in the adoption of and investment in SOX compliance programs by organizations and in the appointment of ethics and compliance officers in corporations across the US and beyond. The SOX Act introduced requirements to strengthen internal audit committee leadership, to provide transparency around the accuracy and completeness of company financial statements and to assess internal controls, which forms the basis of SOX compliance programs. Most importantly, the SOX Act influenced the characteristics of an "effective compliance and ethics program" as detailed in Chapter Eight of the United States Sentencing Commission Federal Sentencing Guidelines Manual.[9] These guidelines have become the most generally accepted framework for an effective compliance program in the United States. For an in-depth discussion of the SOX Act and its impact on corporate accountability, see Appendix B.

**3. *United States Sentencing Commission Federal Sentencing Guidelines Manual***

The United States Sentencing Commission Federal Sentencing Guidelines Manual (Sentencing Guidelines) were first drafted in November 1987 to set out a uniform policy for sentencing individuals and organizations convicted in the US federal court system. Chapter Eight deals with the sentencing of organizations. Importantly, Chapter Eight provides sanctions that if imposed on an organization will not only provide just punishment but will appropriately deter future criminal conduct and incentivize organizations to build, implement and maintain internal mechanisms (i.e. a corporate compliance program) for preventing, detecting and reporting criminal conduct. The Sentencing Guidelines provide a structural foundation for such effective compliance and ethics programs and support the implementation of such a framework as a means of facilitating ethical conduct and compliance with all applicable laws. This framework corresponds to the essential elements of accountability as described in Section A above.

For instance, the framework requires the exercise of reasonable oversight of the program by the governing authority and assigning overall responsibility of the program to high-level personnel; assessment of the risk of criminal conduct and implementing the requirements of Chapter Eight accordingly; standards and procedures to detect and prevent criminal conduct; communication of such policies and procedures and other aspects of the program to organizational personnel; effective training programs; monitoring and auditing to detect criminal conduct and an evaluation of the effectiveness of the program; responding to criminal conduct once detected; and disciplinary action against those that fail to adhere to the program. For a detailed discussion of the Sentencing Guidelines and the elements of Chapter Eight, see Appendix B.

**4. *United States Department of Justice Criminal Division Guidance on the Evaluation of Corporate Compliance Programs***

As the previous three examples show, organizational accountability has been a feature of US corporate compliance for many years. However, it continues to be a modern focus in US regulation. As recently as April 2019, the Criminal Division of the United States Department of Justice (DOJ) released a guidance document for white-collar prosecutors on the evaluation of corporate compliance programs (DOJ Guidance).[10] The DOJ Guidance details the characteristics of a well-designed compliance program. These include a commitment by senior and middle management to compliance; risk assessments, including for third party management; appropriate policies and procedures; program communications to employees and adequate training; periodic testing and review of the program; and disciplinary measures, a confidential reporting structure and investigation and remediation processes for any underlying misconduct. A full discussion of these characteristics and the process by which prosecutors evaluate corporate compliance programs is included in Appendix B.

**Regulatory Area: Anti-Money Laundering**

**5. *Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Examination Manual***

The Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual[11] provides guidance to examiners for assessing the adequacy of a bank's BSA/AML compliance program (Examination Manual). The Examination Manual contains an

overview of BSA/AML compliance program requirements, BSA/AML risks and risk management expectations, industry sound practices and information about examination procedures. The Examination Manual provides that a BSA/AML compliance program must provide for the following minimum requirements – a system of internal controls to ensure ongoing compliance (this requirement implements several elements of accountability including leadership and oversight, risk assessment and policies and procedures); designation of an individual or individuals responsible for managing BSA compliance; training for appropriate personnel; and independent testing of BSA/AML compliance. For a more detailed discussion of the accountability elements contained in the Examination Manual, see Appendix B.

**Regulatory Area: Healthcare**

**6. *Department of Health and Human Services Office of Inspector General Compliance Program Guidance for Hospitals***

For more than the past two decades, the Office of Inspector General (OIG) at the Department of Health and Human Services (HHS) has produced a set of compliance program guidance documents aimed at different segments of the healthcare industry (e.g. hospitals, nursing homes, third party billing services and medical equipment suppliers). Taking the 2005 compliance program guidance for hospitals[12] as an example, the OIG puts forward seven elements that comprehensive hospital compliance programs should include. These elements are based on the United States Sentencing Commission Federal Sentencing Guidelines Manual outlined above. They include designating a chief compliance officer and other appropriate bodies responsible for operating and monitoring the program; developing and distributing written standards of conduct, policies and procedures; including considerations of regulatory exposure for hospital functions and departments in policies and procedures; developing and implementing education and training programs; using audits and other techniques to monitor compliance; and the development of a system to respond to allegations of improper illegal activities and the enforcement of appropriate disciplinary action against employees who have violated internal compliance policies, applicable statues, regulations or federal health care program requirements. For a more detailed discussion of the OIG Compliance Program Guidance for Hospitals, see Appendix B.

**C. Relevance of Above US Accountability Frameworks to a US Federal Privacy Law**

- **Describes accountability's common architecture in US law**: As discussed above, the concept of organizational accountability is deeply engrained in the US legal system. Accountability's key features are also typically consistent across different regulatory areas and are in line with the essential elements of accountability put forward in Section A above. In formulating a new federal privacy law, lawmakers should take note of these key characteristics and incorporate them into any privacy accountability requirement. This will ensure consistency with other US laws and better adoption of privacy accountability in corporations across the US. It will also ensure consistency with global approaches to accountability. Finally, the key features of corporate accountability in US law are in line with the accountability "indicators" put forward in a 2018 sweep on "privacy accountability" by the Global Privacy Enforcement Network (GPEN).[13] This sweep illustrates that there is convergence between the globally accepted elements of accountability in data protection and the elements of accountability found in other areas of US law.

- **Demonstrates accountability is a transferrable concept**: The inclusion of accountability across different regulatory areas demonstrates that accountability is a transferrable concept and not unique to any one legal area or industry. It can be enforced by different regulators with expertise in their specific areas. Accountability in the data privacy context has been adopted in several international privacy laws to date and is a key consideration in the investigations and enforcement actions of data privacy regulators globally, including the US Federal Trade Commission.

- **Solution to modern day data incidents**: The SOX Act is a strong example of how a regulatory response to corporate scandals, namely mandating organizational accountability, resulted in the creation of corporate ethics and compliance (accountability) programs within American businesses, the promotion of responsible accounting practices, prevention and deterrence of corporate misconduct and, ultimately, a fundamental change in corporate behavior. Similarly, a federal data privacy law mandating organizational accountability could provide the same benefits by addressing the issues evidenced by recent data incidents, instilling a culture of corporate digital responsibility within organizations through the promotion of accountable data management practices and working to prevent and deter future misuses of data. A recent CIPL study found that following the incorporation of organizational accountability as a legal requirement in the GDPR, there has been an increased uptake of privacy management programs by organizations in Europe and abroad.[14]

- **Allows lawmakers to draw on accountability's experience in other areas of law**: One of the key lessons to be learned is from the experience of the FCPA. Although the legislation was enacted in 1977, it was not until three decades later that the FCPA Guide was released, providing critical guidance to organizations building compliance programs. In order to ensure the success of any new US privacy framework, an accountability requirement should not only be mandated in a federal privacy law but relevant regulatory guidance should complement and further clarify accountability in data protection, in line with the essential elements of accountability described in Section A above and with other areas of US law that incorporate accountability, as described in this paper. An accountability requirement in a federal US privacy law may even go as far as mandating that such guidance be produced by the appropriate regulator. Indeed, the FTC has traditionally spelled out many of accountability's key features through its consent decrees. Practically every consent decree resulting from an FTC privacy case over the past 30 years has included a requirement that the company involved establish a privacy program reflecting the seven elements of accountability outlined in Section A above. Bringing this all together in a comprehensive guidance document would be beneficial to companies seeking to comply and to individuals who will ultimately benefit from the increased legal certainty. Learning from the international data landscape, many global data privacy regulators, including the Privacy Commissioners of Canada, Hong Kong, Singapore and Australia, as well as the former EU Article 29 Working Party, have issued regulatory guidance on privacy programs and their requirements.[15] These could serve as further points of comparison for any US guidance on the topic.

- **Provides a host of benefits to individuals, regulators and organizations**: The frameworks discussed above have been influential in changing corporate behavior in the United States. These changes bring about many benefits for individuals, regulators and organizations alike. Individuals enjoy greater transparency and protections from corporate malfeasance and misconduct as accountability lifts the veil on corporate irresponsibility and negligence. Regulators are able to assess compliance in a uniform and structured way and to take appropriate and proportional action. Accountable organizations avoid legal liability, boost trust with individuals and regulators and build strong

reputations that ultimately enhance their businesses. These are just some examples of the many benefits of accountability. For a full discussion of the benefits of accountability in data protection to different stakeholders, please see CIPL's white paper on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society".[16] Furthermore, there are additional benefits to structuring an accountability requirement in a federal privacy law in the way described above and already implemented in other areas of US law. One of the most compelling benefits is that companies, their executive leadership, corporate boards and audit committees are used to and already familiar with the accountability architecture as outlined in this paper.

**Conclusion**

It is clear from the above examples that organizational accountability is deeply rooted within the US legal system – from laws tackling anti-corruption, corporate fraud and white-collar crime to anti-money laundering legislation and healthcare. Importantly, these are not the only examples of US law where organizational accountability is present. For example, it forms an integral part of export controls and regulations, as well as, competition law. Including this transferrable concept into any new US federal privacy law will be critical to ensure the corporate digital responsibility of all organizations subject to the law and ensure that Americans receive appropriate protection in the modern digital economy. Omitting accountability from such a law will be detrimental to the success of any new privacy regime in the United States and even more so to the American public.

If you would like more information about the frameworks and laws discussed in Section B above, please see Appendix B below.

If you would like to discuss this paper in more detail or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

## References

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 77 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Public Law 95-213: Foreign Corrupt Practices Act of 1977. (91 Stat. 1494; 1977), available at https://www.govinfo.gov/content/pkg/STATUTE-91/pdf/STATUTE-91-Pg1494.pdf.

[3] Public Law 107-204: Sarbanes-Oxley Act of 2002. (116 Stat. 745; 30 July 2002), available at https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf.

[4] For a detailed discussion of organizational accountability in the context of privacy and data protection, please see CIPL white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society," 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; and "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

[5] United States Sentencing Commission Federal Sentencing Guidelines Manual 2018, Chapter Eight: Sentencing of Organizations, 2018, available at https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf.

[6] United States Department of Justice and Securities and Exchange Commission Resource Guide to the US Foreign Corrupt Practices Act, November 2012, available at https://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf.

[7] *Id.* at Chapter 5 - Guiding Principles of Enforcement, Corporate Compliance Program.

[8] *Supra* note 3.

[9] *Supra* note 5.

[10] Evaluation of Corporate Compliance Programs, US Department of Justice Criminal Division, April 2019, available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

[11] Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, available at https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

[12] Compliance Program Guidance for Hospitals, Office of Inspector General, Department of Health and Human Services, 2005, available at https://oig.hhs.gov/authorities/docs/cpghosp.pdf.

[13] GPEN Sweep 2018 'Privacy Accountability', Office of the Privacy Commissioner, New Zealand and Information Commissioner's Office, UK, October 2018, available at https://ico.org.uk/media/about-the-ico/documents/2614435/gpen-sweep-2018-international-report.pdf. While the Federal Trade Commission is a member of GPEN, it was not able to participate in this particular sweep because it involved a "survey" style approach that was not in line with relevant rules on how the FTC may request information from companies.

[14] See CIPL white paper on "GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges", 31 May 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_report_on_gdpr_one_year_in_-_practitioners_take_stock_of_the_benefits_and_challenges.pdf at page 2.

[15] See (a) Office of the Privacy Commissioner for Personal Data, Hong Kong, Privacy Management Programme: A Best Practice Guide, August 2018 (revised edition), available at

https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf; (b) the Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia, Getting Accountability Right with a Privacy Management Program, 2012, available at https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf; (c) Personal Data Protection Commission of Singapore, Guide to developing a data protection management programme, 2017, available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-developing-a-dpmp---011117.pdf; (d) Office of the Australian Information Commissioner, Privacy management framework: enabling compliance and encouraging good practice, available at https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework; and (e) WP29 Opinion 3/2010 on the principle of accountability, adopted 13 July 2010, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

[16] *Supra* note 4.

# APPENDIX A

## Elements of Accountability Mapped to US Compliance Program Guidance

| CIPL Accountability Element | FCPA Guide | US Sentencing Guidelines | DOJ Guidance on Compliance Programs | FFIEC BSA/AML Examination Manual | OIG Compliance Program Guidance for Hospitals |
|---|---|---|---|---|---|
| ***Leadership & Oversight*** | Commitment from senior management and a clearly articulated policy against corruption<br><br>Oversight, autonomy and resources | Organizations' governing authority shall exercise reasonable oversight with respect to the implementation and effectiveness of the program<br><br>High-level personnel shall be assigned overall responsibility for the compliance and ethics program | Commitment by senior and middle management<br><br>Autonomy and resources | Designation of an individual or individuals responsible for managing BSA compliance<br><br>A system of internal controls to ensure ongoing compliance – it is up to the board of directors and management to create a culture of compliance and ensure staff adhere to BSA/AML policies | Designation of a chief compliance officer and other appropriate bodies charged with the responsibility of operating and monitoring the compliance program |
| ***Risk Assessment*** | Risk assessment<br><br>Third party due diligence and payments | Organizations shall assess the risk of criminal conduct and take appropriate steps to design, implement or modify each requirement set forth in Chapter Eight to reduce the risk of criminal conduct identified through the assessment | Risk assessment<br><br>Third party management | A system of internal controls to ensure ongoing compliance – internal controls should identify banking operations more vulnerable to abuse by money launderers and criminals, provide for periodic updates to the bank's risk profile and provide for a BSA/AML compliance program tailored to manage risks. | Hospital policies and procedures should take into consideration regulatory exposure for each hospital function/department |
| ***Policies and Procedures*** | Code of conduct and compliance policies and procedures | Organizations shall establish standards and procedures to prevent and detect criminal conduct | Policies and procedures | A system of internal controls to ensure ongoing compliance – a review of the bank's written policies, procedures and processes is the first step in determining the overall adequacy of the BSA/AML compliance program | Development and distribution of written standards of conduct and policies and procedures |

| | | | | | |
|---|---|---|---|---|---|
| ***Transparency*** | Communications of policies (subsumed under training and continuing advice) | Organizations shall take steps to periodically communicate policies and procedures and other aspects of the compliance program to all personnel | Ensuring the compliance program is communicated to and understood by employees (Subsumed under training and communications) | Identify reportable transactions and accurately file all required reports | Standards should be distributed to, and comprehensible by, all employees (e.g. translated into other languages and written at appropriate reading levels) |
| ***Training and Awareness*** | Training and continuing advice | Communicating policies and procedures shall be carried out by conducting effective training programs | Training and communications | Training for appropriate personnel | Development and implementation of education and training programs |
| ***Monitoring and Verification*** | Continuous improvement – periodic testing and review | Organizations shall take steps to ensure the compliance and ethics program is followed and evaluate the effectiveness of the program | Continuous improvement, periodic testing and review | Independent testing of BSA/AML compliance – audit should be conducted by the internal audit department, outside auditors, consultants or other qualified independent third parties. | Use of audits and/or other evaluation techniques to monitor compliance |
| ***Response and Enforcement*** | Incentives and disciplinary measures<br><br>Confidential reporting and internal investigation<br><br>M&A: Pre-acquisition due diligence and post-acquisition integration | Organizations' compliance and ethics programs shall be promoted and enforced consistently throughout the organization through appropriate incentives and disciplinary measures | Confidential reporting structure and investigation process<br><br>M&A due diligence<br><br>Incentives and disciplinary measures<br><br>Investigation of misconduct<br><br>Analysis and remediation of any underlying misconduct | Independent testing of BSA/AML compliance – the board or designated committee and audit staff should track deficiencies and document corrective actions. | Maintenance of a process to receive complaints<br><br>Development of a system to respond to allegations of improper illegal activities and the enforcement of appropriate disciplinary action against employees |

*Table 1 – Elements of Accountability Mapped to US Compliance Program Guidance*

# APPENDIX B

## Organizational Accountability's Existence in US Regulatory Compliance

This Appendix provides a full discussion of the regulatory frameworks and laws discussed in Section B of the paper. The key features of each framework are organized under the essential elements of accountability in Section A of this paper.

**Regulatory Area**: **Anti-Corruption**

**1. *United States Department of Justice and the Securities and Exchange Commission Resource Guide to the US Foreign Corrupt Practices Act (FCPA)***

In many ways, the FCPA of 1977[i] symbolized the beginnings of corporate compliance programs in the United States. In November 2012, the Criminal Division of the United States Department of Justice (DOJ) and the Enforcement Division of the United States Securities and Exchange Commission (SEC) released a resource guide to the US Foreign Corrupt Practices Act (FCPA Guide).[ii] The FCPA Guide covers a wide variety of topics, including the hallmarks of effective compliance programs.[iii] According to the guidance, "an effective compliance program is a critical component of an organization's internal controls and vital to detecting and preventing FCPA violations".[iv] In investigating FCPA violations, the DOJ and SEC will consider the adequacy of an organization's compliance program in deciding what action to take and in assessing penalties and the need to order the appointment of a corporate monitor or self-reporting.

The FCPA Guide highlights the importance of putting in place an accountable compliance program by noting that "[i]n appropriate circumstances, DOJ and SEC may decline to pursue charges against a company based on the company's effective compliance program, or may otherwise seek to reward a company for its program, even when that program did not prevent the particular underlying FCPA violation that gave rise to the investigation".[v] Similarly, in the data protection sphere, having an accountable privacy management program in place can serve as a mitigating factor in enforcement actions by data privacy regulators. Furthermore, CIPL has previously written about the importance of rewarding or incentivizing accountability in data protection.[vi]

The FCPA Guide puts forward ten hallmarks of effective compliance programs, which correspond to the essential elements of accountability put forward in Section A of this paper. Importantly, the FCPA Guide clarifies that these factors are designed to provide insight into aspects of compliance programs that the DOJ and SEC assess when investigating FCPA violations but qualifies that companies may consider a variety of factors when making their own determination of what is appropriate for their specific business needs. This emphasizes the flexible and scalable nature of accountability-based compliance programs.

**Hallmarks of Effective Compliance Programs**

***Leadership and Oversight***:

- **Commitment from Senior Management and a Clearly Articulated Policy Against Corruption**: The FCPA Guide notes that within organizations, compliance begins with the board of directors and senior executives setting the tone for the rest of the company. In other words, compliance must start at the top as managers and employees take their cues from corporate leadership. In assessing commitment from senior management, the DOJ and SEC will evaluate whether top management has articulated company standards, communicated them and disseminated them throughout the organization and scrupulously adhered to them.

- **Oversight, Autonomy and Resources**: The DOJ and SEC, in evaluating the effectiveness of a compliance program, will examine whether the organization has assigned responsibility for the oversight and implementation of the program to senior executives within the organization. The autonomy of such executives and level of resources provided to them to ensure the effective implementation of the compliance program are important factors in this examination.

***Risk Assessment*:**

- **Risk Assessment**: The FCPA Guide notes that "assessment of risk is fundamental to developing a strong compliance program".[vii] Furthermore, organizations that implement comprehensive, risk-based compliance programs will be given credit by the DOJ and SEC in assessing the effectiveness of the compliance program. This will be the case even where a program does not prevent a low risk violation because the organization committed greater attention and resources to tackling higher risk areas. According to the FCPA Guide, whether and to what degree a company analyzes and addresses the particular risks it faces are key factors in determining whether a program incorporates a risk-based approach to regulatory compliance.

- **Third Party Due Diligence and Payments**: The DOJ and SEC will also examine risk-based due diligence with respect to third parties in assessing the compliance program. Ongoing monitoring of third party relationships, including updating due diligence periodically are important considerations in this regard.

***Policies and Procedures*:**

- **Code of Conduct and Compliance Policies and Procedures**: According to the FCPA Guide, a company's code of conduct lays the foundation upon which an effective compliance program is built. In addition to looking at company codes of conduct, the DOJ and SEC will consider, when assessing the effectiveness of an organization's compliance program, whether a company has policies and procedures in place outlining responsibilities for compliance and detailing proper internal controls, auditing practices and documentation policies and whether appropriate disciplinary procedures have been established.

***Transparency***:

- **Training and Continuing Advice**: Subsumed under the hallmark of training and continuing advice, the FCPA Guide notes that "compliance policies cannot work unless effectively communicated throughout the company".[viii] Communicating such policies requires providing appropriate transparency around company practices to staff and management and external stakeholders, such as business partners.

***Training and Awareness***:

- **Training and Continuing Advice**: According to the FCPA Guide, the DOJ and SEC will examine whether an organization has taken measures to ensure that relevant policies and procedures have been communicated to all directors, officers, relevant employees, agents and business partners, including through periodic training and certification. Additionally, the FCPA Guide advises that

organizations should provide guidance on complying with the program generally and on an *ad hoc* basis.

***Monitoring and Verification***:

- **Continuous Improvement – Periodic Testing and Review**: As the FCPA Guide rightly notes "a good compliance program should constantly evolve".[ix] The DOJ and SEC will examine, in assessing the effectiveness of a compliance program, whether an organization regularly reviews and improves its compliance program and prevents it from becoming stale. In particular, companies should undertake proactive evaluations of the program before a problem occurs, through for example, testing internal controls, identifying best practices and detecting new risk areas.

***Response and Enforcement***:

- **Incentives and Disciplinary Measures**: The FCPA Guide emphasizes that in addition to evaluating a compliance program's design and implementation, evaluating whether it is appropriately enforced is critical to assessing the program's effectiveness. Accordingly, the FCPA Guide notes that a compliance program should apply from the board room to the supply room and that no one should be beyond its reach. In assessing effective enforcement of the program, the DOJ and SEC will consider whether appropriate disciplinary procedures are in place, whether they are applied reliably and promptly and whether they are commensurate with the violation at hand.

- **Confidential Reporting and Internal Investigation**: According to the FCPA guide, an effective compliance program includes a mechanism to report suspected or actual misconduct or violations of company policies on a confidential basis and without fear of retaliation by the organization or employer. Organizations should update internal controls and the program based on reported violations and the outcomes of any resulting investigations.

- **Mergers and Acquisitions – Pre-Acquisition Due Diligence and Post-Acquisition Integration**: The FCPA Guide notes that organizations that conduct effective FCPA due diligence on acquisition targets demonstrate to the DOJ and SEC the organization's commitment to compliance and this is taken into account when evaluating any potential enforcement action.

**Regulatory Area**: **White-Collar Crime and Corporate Fraud**

## 2. *Sarbanes-Oxley Act of 2002*

In response to major scandals of corporate malfeasance and accounting fraud in the early 2000's, including those involving Enron Corporation, WorldCom, Tyco and accounting firm Arthur Andersen, the US enacted the Sarbanes-Oxley Act of 2002[x] (SOX Act) (introduced as the Corporate and Auditing Accountability, Responsibility, and Transparency Act of 2002 in the US House of Representatives).

The SOX Act was created to crack down on corporate fraud and white-collar crime and to reform American business practices. It has had a profound effect on corporate accountability and governance over the past 17 years. Specifically, the SOX Act caused a huge spike in the adoption of and investment in SOX

compliance programs by organizations through mandating specific requirements that correspond to the essential elements of accountability described in Section A of this paper. For example:

- ***Leadership and Oversight***: The Act requires enhanced leadership and oversight of compliance obligations by strengthening the role and independence of a company's audit committee. The Act provides more leverage for members of the audit committee to oversee top management accounting decisions and makes the committee responsible for the appointment, compensation, retention and oversight of the company's independent accounting firm. The audit committee is also required to establish procedures for handling complaints regarding accounting, internal accounting controls or auditing matters.

- ***Transparency***: The Act also introduces new transparency obligations through requiring top company management to make certain written certifications regarding the accuracy and completeness of the company's financial statements, strengthens disclosure requirements by ensuring appropriate reporting of all material off-balance sheet liabilities, obligations, and transactions and mandates real time disclosures concerning material changes in an organization's financial condition or operations.

- ***Monitoring and Verification***: The Act ensures appropriate monitoring and verification of compliance by requiring management assessment of internal controls. Annual financial reports are required to include an "Internal Control Report" that states the responsibility of management for establishing and maintaining an adequate internal control structure and contains an assessment of the effectiveness of that control structure. External audits further verify compliance.

Most importantly, the SOX Act influenced the characteristics of an "effective compliance and ethics program" as detailed in Chapter Eight of the United States Sentencing Commission Federal Sentencing Guidelines Manual (Sentencing Guidelines).[xi] The requirements of such a program as set out under Section 8B2.1. of the Sentencing Guidelines[xii] respond to Section 805(a)(5) of the SOX Act, directing the United States Sentencing Commission to "review and amend, as appropriate, the Federal Sentencing Guidelines and related policy statements to ensure that […] the guidelines that apply to organizations in […] chapter 8, are sufficient to deter and punish organizational misconduct". The Sentencing Guidelines have become the most generally accepted framework for an effective compliance program in the United States and incorporate by reference the rest of the elements of organizational accountability described in Section A of this paper into the SOX Act.

### 3. ***United States Sentencing Commission Federal Sentencing Guidelines Manual***

The Sentencing Guidelines were first drafted in November 1987 to set out a uniform policy for sentencing individuals and organizations convicted in the US federal court system. Chapter Eight deals with the sentencing of organizations. Chapter Eight provides sanctions that if imposed on an organization will not only provide just punishment but will appropriately deter future criminal conduct and incentivize organizations to build, implement and maintain internal mechanisms (i.e. a corporate compliance program) for preventing, detecting and reporting criminal conduct. The existence of an effective compliance and ethics program serves as a mitigating factor in the ultimate punishment of an organization under the Sentencing Guidelines.

The Sentencing Guidelines provide a structural foundation for such effective compliance and ethics programs and support the implementation of such a framework as a means of facilitating ethical conduct and compliance with all applicable laws.

According to the Sentencing Guidelines, to have an effective compliance and ethics program, an organization must "exercise due diligence to prevent and detect criminal conduct" and "otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law".[xiii] Achieving this minimally requires implementing the essential elements of accountability as described in Section A of this paper.

- ***Leadership and Oversight***: The Sentencing Guidelines require an organization's governing authority to be knowledgeable about both the content and operation of the compliance program and to exercise reasonable oversight with respect to its implementation**.** Additionally, the Sentencing Guidelines mandate that overall responsibility for the compliance program be assigned to specific high-level personnel. Furthermore, personnel with operational responsibility must report periodically to such high-level personnel and, as appropriate, to the governing authority.

- ***Risk-Assessment***: The Sentencing Guidelines specify that in exercising due diligence to prevent and detect criminal conduct and in promoting an organizational culture that encourages ethical conduct and a commitment to compliance with the law, organizations must assess the risk of criminal conduct and take appropriate steps to design, implement or modify the requirements set out in Chapter Eight to reduce the risk of criminal conduct identified through the assessment.

- ***Policies and Procedures***: The Sentencing Guidelines require organizations to establish standards and procedures to prevent and detect criminal conduct.

- ***Transparency***: The Sentencing Guidelines oblige organizations to take steps to periodically communicate its policies and procedures, and other aspects of the compliance program, to all personnel, including high-level management and employees, and agents of the organization.

- ***Training and Awareness***: The Sentencing Guidelines note that communicating the policies and procedures to personnel and agents should be carried out through effective training programs and otherwise disseminating information appropriate to specific staff roles and responsibilities.

- ***Monitoring and Verification***: The Sentencing Guidelines require organizations to take steps to ensure the compliance program is followed, including monitoring and auditing to detect criminal conduct. In addition, organizations should periodically evaluate the effectiveness of the compliance program, and establish and make known a system for confidential reporting of misconduct and seeking guidance about potential misconduct.

- ***Response and Enforcement***: The Sentencing Guidelines specify that organizations should promote and enforce the compliance program through providing appropriate incentives to encourage compliance and taking appropriate disciplinary measures against those that fail to take reasonable steps to prevent or detect criminal conduct or for engaging in criminal conduct**.** Moreover, the organization must respond appropriately to criminal conduct once it has been

detected and take steps to prevent similar future reoccurrences, including through updating and modifying the compliance program, where necessary.

**4. *United States Department of Justice Criminal Division Guidance on the Evaluation of Corporate Compliance Programs***

As the previous three examples show, organizational accountability has been a feature of US corporate compliance for many years. However, it continues to be a modern focus in US regulation. As recently as April 2019, the Criminal Division of the United States Department of Justice (DOJ) released a guidance document for white-collar prosecutors on the evaluation of corporate compliance programs (DOJ Guidance).[xiv] This guidance updates a prior version issued by the Criminal Division's Fraud Section in February 2017.

The DOJ Guidance details the characteristics of a well-designed compliance program relating to risk assessment, company policies and procedures, training and communications, confidential reporting structures and investigation processes, third party management and mergers and acquisitions. It also specifies features of effective implementation of a compliance program, including commitment by senior and middle management, autonomy and resources and incentives and disciplinary measures.

Structured around a set of three questions put forward in Title 9 of the US DOJ Justice Manual,[xv] the DOJ Guidance aids prosecutors in deciding whether, and to what extent, an organization's compliance program was effective at the time an offense was committed and is effective at the time of a charging decision or resolution. The purpose of such an evaluation is to determine the appropriate form of any resolution or prosecution, compliance obligations contained in any corporate criminal resolution or monetary penalties. The three questions that prosecutors ask in conducting the evaluation are:

**(1) Is the corporation's compliance program well-designed?**

**(2) Is the corporation's compliance program being implemented effectively?**

**(3) Does the corporation's compliance program work in practice?**

Title 9 of the Justice Manual notes that "[i]n answering these questions, the prosecutor should consider the comprehensiveness of the compliance program".[xvi]

The DOJ Guidance outlines various characteristics of corporate compliance programs to consider under each question. These characteristics correspond with the essential elements of accountability discussed in Section A of this paper.

**(1) Is the corporation's compliance program well-designed?**

***Risk Assessment***:

- **Risk Assessment**: The DOJ Guidance notes that the starting point in the evaluation "is to understand the company's business from a commercial perspective, how the company has identified, assessed and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks".[xvii] In line with the Justice Manual,

prosecutors should consider whether the program is designed to detect the specific types of misconduct most likely to occur in a particular organization's line of business and complex regulatory environment. In conducting such an assessment, relevant factors to consider include the methodology the company has used to identify, analyze and address the particular risks it faces; whether the company gives greater scrutiny to high-risk transactions; and whether the risk assessment is current and subject to periodic review.

- **Third party Management**: According to the DOJ Guidance, a well-designed compliance program should also apply risk-based due diligence to its third party relationships.

***Policies and Procedures***:

- **Policies and Procedures**: The DOJ Guidance states that a well-designed compliance program necessitates having policies and procedures in place that give content and effect to ethical norms and that address and aim to reduce risks identified by the organization through its risk assessment processes. The Guidance further instructs prosecutors to examine whether the company has a code of conduct that commits to full compliance with relevant federal laws. Additionally, prosecutors should examine whether policies and procedures that incorporate a culture of compliance into the organization's day-to-day operations have been established.

***Training and Awareness***:

- **Training and Communications**: The DOJ Guidance advises prosecutors to assess whether the compliance program is communicated to and understood by employees in practice to determine whether the program is actually effective. This includes an assessment of steps taken by the organization to integrate policies and procedures throughout the organization, including through regular training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Furthermore, an assessment of the training programs themselves and whether they relay information appropriate to audience size, sophistication and expertise and whether they cover prior compliance incidents will be relevant factors in reviewing the program.

***Response and Enforcement***:

- **Confidential Reporting Structure and Investigation Process**: According to the DOJ Guidance, a key characteristic of a well-designed compliance program is the existence of trusted mechanisms for the anonymous and confidential reporting of breaches of the organization's code of conduct and/or policies or of suspected or actual misconduct. The assessment does not stop at whether there is a mechanism in place. Rather, prosecutors will also examine the processes for handling such reports, including the channeling of complaints to the right departments, conducting thorough and timely investigations and procedures for following up on the outcomes of investigations**.**

- **Mergers and Acquisitions**: The DOJ Guidance affirms that a key factor in determining whether a compliance program is able to effectively enforce its internal controls and remediate misconduct

at all levels of the organization is the extent to which the organization subjects acquisition targets to appropriate scrutiny in M&A contexts.

**(2) Is the corporation's compliance program being implemented effectively?**

***Leadership and Oversight***:

- **Commitment by Senior and Middle Management**: The DOJ Guidance rightfully notes that it is important for organizations to create and foster a culture of ethics and compliance with the law beyond compliance structures, policies and procedures alone**.** In other words, an effective compliance program requires a high-level commitment by senior management to implement a culture of compliance from the top. The Guidance details relevant factors to consider in assessing such a commitment, namely, how senior leaders have, through words and actions, encourage or discouraged compliance, including the type of misconduct involved in the investigation and what actions have been taken to demonstrate leadership in the organization's compliance and remediation efforts.

- **Autonomy and Resources**: According to the DOJ Guidance, effective implementation of the compliance program also requires those tasked with a program's day-to-day oversight to act with adequate authority and stature. Moreover, with respect to internal audits, prosecutors should examine whether audit functions are conducted at a level sufficient to ensure their independence and accuracy. Such an assessment can indicate whether compliance personnel are appropriately empowered and positioned to effectively detect and prevent misconduct.

***Response and Enforcement***:

- **Incentives and Disciplinary Measures**: Another key characteristic of effective compliance programs is the establishment of incentives for compliance and disincentives for non-compliance. The DOJ Guidance advises that prosecutors should assess whether an organization has clear disciplinary procedures in place, enforces them consistently and ensures that the procedures are commensurate with the violations. The Guidance further notes that some organizations have found that providing positive incentives, including promotions, rewards and bonuses for improving and developing a compliance program or demonstrating ethical leadership served as drivers of compliance.

**(3) Does the corporation's compliance program work in practice?**

***Monitoring and Verification***:

- **Continuous Improvement, Periodic Testing and Review**: The DOJ Guidance highlights the fact that an organization's business changes over time and so do the environments in which it operates, the nature of its customers and applicable laws and industry standards. As a result, the Guidance advises prosecutors to consider whether a company had engaged in efforts to review the compliance program to ensure it does not grow stale.

***Response and Enforcement***:

- **Investigation of Misconduct**: According to the DOJ Guidance, another key characteristic of an effective compliance program is the existence of mechanisms for thorough and timely investigations of misconduct by the company or its employees and agents. How the company responds to such investigations, including disciplinary action taken or remediation measures will be relevant considerations.

- **Analysis and Remediation of Any Underlying Misconduct**: Finally, the DOJ Guidance affirms that a key indicator of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and appropriately remediate to address the root causes.

**Regulatory Area: Anti-Money Laundering**

### 5. *Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Examination Manual*

The Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual[xviii] provides guidance to examiners for assessing the adequacy of a bank's BSA/AML compliance program (Examination Manual). The Examination Manual contains an overview of BSA/AML compliance program requirements, BSA/AML risks and risk management expectations, industry sound practices and information about examination procedures.

The Examination Manual provides that a BSA/AML compliance program must provide for the following minimum requirements:

***Leadership and Oversight, Risk Assessment, Policies and Procedures and Transparency***:

- **A system of internal controls to ensure ongoing compliance**: According to the Examination Manual, a review of the bank's written policies, procedures and processes is the first step in determining the overall adequacy of the BSA/AML compliance program. It is up to the board of directors and management to create a culture of compliance to ensure staff adherence to the bank's BSA/AML policies. Furthermore, internal controls should identify banking operations more vulnerable to abuse by money launderers and criminals, provide for periodic updates to the bank's risk profile and provide for a BSA/AML compliance program tailored to manage risks. Moreover, internal controls should identify reportable transactions and accurately file all required reports including suspicious activity reports (SARs), currency transaction reports (CTRs), and CTR exemptions.

- **Designation of an individual or individuals responsible for managing BSA compliance**: The Examination Manual instructs that the bank's board of directors must designate a qualified individual to serve as the BSA compliance officer. Such an officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance and for managing all aspects of the compliance program.

***Training and Awareness***:

- **Training for appropriate personnel**: According to the examination manual, banks must ensure that appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the bank's internal BSA/AML policies, procedures and processes.

***Monitoring and Verification and Response and Enforcement***:

- **Independent testing of BSA/AML compliance**: The Examination Manual specifies that independent testing (audit) should be conducted by the internal audit department, outside auditors, consultants or other qualified independent parties. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls. Moreover, the board or designated committee and the audit staff should track audit deficiencies and document corrective actions.

**Regulatory Area: Healthcare**

### 6. *Department of Health and Human Services Office of Inspector General Compliance Program Guidance for Hospitals*

For more than the past two decades, the Office of Inspector General (OIG) at the Department of Health and Human Services (HHS) has produced a set of compliance program guidance documents aimed at different segments of the healthcare industry (e.g. hospitals, nursing homes, third party billing services and medical equipment suppliers). Taking the 2005 compliance program guidance for hospitals[xix] as an example, the OIG puts forward seven elements that comprehensive hospital compliance programs should include. These elements are based on the United States Sentencing Commission Federal Sentencing Guidelines Manual outlined above and comprise:

***Leadership and Oversight***:

- The designation of a chief compliance officer and other appropriate bodies charged with the responsibility of operating and monitoring the compliance program.

***Risk Assessment***:

- A hospitals written policies and procedures should take into consideration the regulatory exposure for each function or department of the hospital (Subsumed under policies and procedures).

***Policies and Procedures***:

- The development and distribution of written standards of conduct, as well as written policies and procedures that promote the hospital's commitment to compliance.

***Transparency***:

- Standards of conduct should be distributed to, and comprehensible by, all employees (e.g. translated into other languages and written at appropriate reading levels) (Subsumed under policies and procedures).

***Training and Awareness***:

- The development and implementation of regular, effective education and training programs for all affected employees.

***Monitoring and Verification***:

- The use of audits and/or other evaluation techniques to monitor compliance and assist in the reduction of identified problem areas.

***Response and Enforcement***:

- The maintenance of a process to receive complaints and the adoption of procedures to protect the anonymity of complainants and to protect whistleblowers from retaliation.

- The development of a system to respond to allegations of improper illegal activities and the enforcement of appropriate disciplinary action against employees who have violated internal compliance policies, applicable statues, regulations or federal health care program requirements.

- The investigation and remediation of identified systemic problems and the development of policies addressing the non-employment or retention of sanctioned individuals.

## References

[i] Public Law 95-213: Foreign Corrupt Practices Act of 1977. (91 Stat. 1494; 1977), available at https://www.govinfo.gov/content/pkg/STATUTE-91/pdf/STATUTE-91-Pg1494.pdf.
[ii] United States Department of Justice and Securities and Exchange Commission Resource Guide to the US Foreign Corrupt Practices Act, November 2012, available at https://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf.
[iii] *Id.* at Chapter 5 - Guiding Principles of Enforcement, Corporate Compliance Program.
[iv] *Id*. at page 56.
[v] *Id*.
[vi] See CIPL white paper on "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.
[vii] *Supra* note ii at page 58.
[viii] *Id*. at page 59.
[ix] *Id*. at page 61.
[x] Public Law 107-204: Sarbanes-Oxley Act of 2002. (116 Stat. 745; 30 July 2002), available at https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf.
[xi] United States Sentencing Commission Federal Sentencing Guidelines Manual 2018, Chapter Eight: Sentencing of Organizations, 2018, available at https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf.
[xii] *Id*. at page 517.
[xiii] *Id*. at page 533.
[xiv] Evaluation of Corporate Compliance Programs, US Department of Justice Criminal Division, April 2019, available at https://www.justice.gov/criminal-fraud/page/file/937501/download.
[xv] Justice Manual, Title 9: Criminal, 9-28.800 Corporate Compliance Programs, US Department of Justice, available at https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.800.
[xvi] *Id*.
[xvii] *Supra* note xiv at page 2.
[xviii] Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2014, available at https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.
[xix] Compliance Program Guidance for Hospitals, Office of Inspector General, Department of Health and Human Services, 2005, available at https://oig.hhs.gov/authorities/docs/cpghosp.pdf.