Breakout Sessions – Series 2

BREACHES ABOUND

PROTECTING YOUR BUSINESS FROM INFORMATION INDISCRETION

Bruce A. Griggs (Moderator) – Ogletree Deakins (Austin)

Gary Berger – Ogletree Deakins (Greenville)

Danielle Vanderzanden – Ogletree Deakins (Boston/Portland (ME))
Data security continues to present a multitude of challenges for organizations of all sizes. To help you evaluate the legal risks your organization may face and the physical, technical, and administrative steps your company should consider in seeking to protect your information assets and the privacy of your customers and colleagues, we outline below and attach hereto a variety of materials. The materials will provide you with a brief overview of the cybersecurity frameworks, discuss developing state and international laws and sample checklists, and include guidelines and policies to help you assess your organization’s cybersecurity needs and ensure that your company is complying with local, state and national requirements.

1) Cybersecurity Frameworks: How Do You Pick One?

Selecting the appropriate framework to meet your organization’s cybersecurity needs is of the utmost importance. The most effective way to maintain an effective security programs is to apply a security framework that is customized to meet your organization’s business objectives to implement clear policies and procedures for managing controls. Your organization’s cybersecurity framework should be tailored to address specific security controls and regulatory compliance requirements. For smaller or unregulated businesses that require less coverage, the NIST Cybersecurity Framework often is an appropriate choice. Organizations with moderate coverage needs may select ISO 27002. Organizations with extensive coverage needs typically opt for the NIST 800-53 r4 framework. We have provided a map of these of the major cybersecurity frameworks and their compliance requirements, which differ significantly, to assist you in making a determination as to which cybersecurity framework fits the needs of your organization. Regardless of which framework you select, ensuring that your organization keeps its standards up to date and audits its compliance is essential.

2) Biometric Lawsuits: Have the Floodgates Opened?

The issue of standing – or lack thereof – has been a primary focus in data breach litigation since the dawn of information insecurity. In one of the latest chapters of this ongoing saga, the Supreme Court of Illinois has held that an individual may be considered an “aggrieved person” entitled to a private right of action pursuant the Biometric Information Privacy Act (“BIPA” of the “Act”) – even in the absence of actual harm. See in the matter of Rosenbach v. Six Flags Entm’t Corp., 2019 IL 123186. Pursuant to the Court’s unanimous decision, when a private entity collects biometric identifiers or information without consent, an individual may be considered an “aggrieved person” regardless of whether the individual suffered actual harm resulting from the collection.

BIPA regulates the “collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” A biometric identifier is defined as “a retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry” whereas biometric information is defined as “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifiers used to identify an individual.”

Illinois is one of three states, along with Washington and Texas, which has passed a BIPA. The Illinois BIPA is the most stringent of the three. As this area of law continues to develop, employers in each state should take steps to insulate themselves from liability, even if the state in which they operate does not currently have a law regarding biometric data use in place. Such steps include, but are not limited to, the following:
• Implement a clear policy that details what biometric data is being collected, the purpose for its collection and how the data will be used and destroyed once it is no longer needed;

• Obtain consent prior to any collection of biometric data;

• Before implementing any biometric technology, ensure that it is legal in the state in which the company operates and complies with any and all requirements, including data protection laws and state tort laws;

• Be aware of medical issues that could arise in the event the company’s biometric technology is based on data that would implicate an employee’s medical history;

• Businesses whose employees belong to unions must keep them apprised of any institution or change of a biometric policy, as it is a mandatory subject of collective bargaining and employers must first negotiate with the unions; and

• Ensure any vendors contracted to operate biometric systems have compliant policies of their own and the proper software and equipment to handle the data.

3) 201 CMR 17.00 Compliance Checklist.

Massachusetts was the first state to enact information security requirements at the state level, and the requirements associated with establishing a Written Information Security Program (“WISP”) provide helpful guidance. The Massachusetts Office of Consumer Affairs and Business Regulation compiled this checklist to help small businesses develop a compliant WISP. Although the requirements of other states and federal laws are similar, this checklist focuses on the Massachusetts Regulations. It should be noted that the Massachusetts Regulations apply to organizations that own or license personal information of Massachusetts residents, regardless of whether the organization is in Massachusetts.

4) GDPR Compliance Checklist for Human Resources Data.

The General Data protection Regulation (GDPR) requires that all organizations protect the privacy and personal data of European Union citizens regarding transactions that take place within the European Union member states. This regulation applies to all organizations that conduct business in Europe and to those that process data regarding EU residents. This checklist will help your organization evaluate whether it is subject to GDPR and commence or audit its GDPR compliance journey.

5) GDPR Privacy Policy for Human Resources Data.

Privacy policies disclose how organizations collect, store and release personal information. This Privacy Policy for Human Resources Data addresses personal information of employees. In addition to disclosing how personal information is collected, stored and released, a privacy policy should detail how personal information is protected. Please note that this is a sample policy and it is not intended for use, as it may not adequately address the needs of your organization. Counsel should be consulted to assist your organization with the implementation of any privacy policy.

On June 28, 2018, California Governor Jerry Brown signed the California Consumer Privacy Act (CCPA), which will go into effect on January 1, 2020. The CCPA addresses Californians’ rights regarding their personal information. Specifically, the right to know what personal information is being collected, whether their personal information is sold or disclosed and to whom, the right to refuse to submit to the sale of personal information, the right to access personal information and the right to equal service and price regardless of whether they have exercised their privacy rights.

The CCPA applies to numerous entities, including, but not limited to, any for-profit entity that collects consumers’ personal information, does business in California and either has an annual gross revenue in excess of twenty-five million dollars ($25,000,000.00), “alone or in combination, annually buys, receives for the business’ commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices” or derives 50 percent or more of its annual revenues from the sale of consumers’ personal information. It should be noted that an entity that controls or is controlled by a company engaged in the activity above will need to comply with the CCPA as well.

If your organization fits the above criterion, you must begin preparing your organization for compliance immediately. Though the CCPA does not go into effect until January 1, 2020, the law requires that organizations provide a 12-month lookback for consumer requests that will require data analysis such as tracking and mapping. The California Consumer Privacy Act: Getting a Head Start on Compliance provides a brief overview of the new law including the CCPA’s definition of personal information, consumer rights and business obligations created by the CCPA and exposure for noncompliance with the CCPA.
The California Consumer Privacy Act (CCPA) is a new law that California Governor Jerry Brown signed on June 28, 2018, and will become effective on January 1, 2020. Amendments to the law are still being proposed, and the law will likely be amended and clarified. Here is what we know today.

The law was written to ensure the following rights:

1. “The right of Californians to know what personal information is being collected about them.”
2. “The right of Californians to know whether their personal information is sold or disclosed and to whom.”
3. “The right of Californians to say no to the sale of personal information.”
4. “The right of Californians to access their personal information.”
5. “The right of Californians to equal service and price, even if they exercise their privacy rights.”

When to Start Thinking About the CCPA

The CCPA will become effective January 1, 2020. However, businesses will need to begin data analysis, including tracking and mapping, by January 1, 2019, to comply with the 12-month lookback provision for consumer requests.

Who Needs to Comply?

Entities that need to comply include, but are not limited to, any for-profit entity that collects consumers' personal information, does business in the State of California, and satisfies one or more of the following thresholds:

1. Has an annual gross revenues in excess of twenty-five million dollars ($25,000,000)....
2. “Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.”
3. “Derives 50 percent or more of its annual revenues from selling consumers' personal information.”

An entity that controls or is controlled by a business that does any of the above would also need to comply.
What Is a Consumer?

The CCPA is drafted to protect consumers. According to the CCPA, a “consumer” is a “natural person who is a California resident,” as defined by the California Code of Regulations. According to Section 1798.14 of Title 18 of the California Code of Regulations, a California resident is “[1] every individual who is in the State for other than a temporary or transitory purpose, and [2] every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose.”

What Is Personal Information?

Unlike protected health information (PHI) in the HIPAA context or personally identifiable information (PII) in the context of the California Online Privacy Protection Act (CalOPPA), the CCPA’s definition of “personal information” (PI) is very broad. Indeed, it does not take a vivid imagination to expand the definition of PI under the CCPA to include everything.

Under the CCPA, “[p]ersonal information means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked directly or indirectly, with a particular consumer or device.”

The following are some examples of PI, according to the CCPA:

- Identifiers such as a real name, alias, postal address, unique personal identifiers, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
- Characteristics of protected classifications under California or federal law.
- Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with a website, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information.

PI does not include publicly available information. For these purposes, “publicly available information” means information that is lawfully made available from federal, state, and local government records, or that is available to the general public. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge. Information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and
made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is de-identified or aggregate consumer information.

**Consumer Rights/Business Obligations Created by the CCPA**

The CCPA creates many new rights for consumers, which in turn create many new obligations for businesses. The following are the top 11 to keep in mind:

1. "A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer… the categories… and specific pieces of personal information it has collected about that consumer."

2. "A business that collects a consumer’s personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."

3. "A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period."

4. "A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."

5. "A business that collects personal information about consumers shall disclose… the consumer’s rights to request the deletion of the consumer’s personal information."

6. "A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information. This right may be referred to as the right to opt out."

7. "A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out."

8. "A business that sells consumers’ personal information to third parties must provide notice to consumers… that this information may be sold and that consumers have the right to opt out of the sale of their personal information."

9. "A business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights under this title…"

10. "A business shall, in a form that is reasonably accessible to consumers... provide a clear and conspicuous link on the business’s Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer’s personal information."
11. "A consumer may authorize another person solely to opt out of the sale of the consumer’s personal information on the consumer’s behalf, and a business shall comply with an opt out request received from a person authorized by the consumer to act on the consumer’s behalf, pursuant to regulations adopted by the Attorney General."

**Exposure for Noncompliance**

Consumer civil actions are limited to security breaches involving a consumer’s PI. Damages are limited to $750 per consumer per incident or actual damages, whichever is greater. Although this number may seem small in comparison to the General Data Protection Regulation’s (GDPR) €20 million or 4 percent of annual global revenue, whichever is greater, keep in mind that the EU does not allow collective, or class, actions. A class of 1 million people under the CCPA would equal $750,000,000 in potential exposure.
The Illinois Supreme Court issued its long-awaited ruling in *Rosenbach* and reversed the appellate court's decision that technical violations of the Illinois Biometric Information Privacy Act ("BIPA" or "Act") without "some actual injury or harm" are not actionable:

Contrary to the appellate court's view, an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.


With this ruling, the Illinois Supreme Court has likely unleashed another wave of class action litigation. These class actions could transfer millions of dollars from companies that do business in Illinois into the pockets of the plaintiffs' class action bar. While no one can dispute BIPA's good intentions, biometric technology has evolved far beyond 2008, when the law was enacted. The biometric equipment in use today transforms the biometric identifier into an encrypted mathematical algorithm that renders it unreadable and unidentifiable. These safeguards prevent the harms contemplated by BIPA. In *Rosenbach*, Judge Edmond Chang explained that laws such as BIPA (with their statutory damages and fee-shifting) are an imperfect fit and cannot keep pace with technological advances: "The difficulty in predicting technological advances and their legal effects is one reason why legislative pronouncements with minimum statutory damages and fee-shifting might reasonably be considered a too-blunt instrument for dealing with technology." *Rosenbach*, 2018 WL 6830332, fn. 20 (N.D. Ill. Dec. 29, 2018).

*Rosenbach* is not a positive development for Illinois' business economy, especially when no BIPA lawsuit has pled any unauthorized disclosure of biometric data to the public, any illegal hacking, or other actual injury. Unless the Illinois legislature promptly amends BIPA, these BIPA class actions have the potential to bankrupt some Illinois businesses and discourage future business investment in Illinois.

*BIPA's History and Key Provisions*
In 2008, Illinois became the first state to regulate a private entity’s collection, use, transmission, and destruction of “biometric identifiers” such as retina or iris scans, fingerprints, voiceprints, or hand or facial geometry scans. BIPA also protects “biometric information,” which includes “any information . . . based on an individual’s biometric identifier used to identify an individual.”

Section 15 of BIPA prohibits a private entity from collecting a person’s or customer’s “biometric identifier” or “biometric information” unless it first informs them of the “specific purpose and length of term for which [it] is being collected, stored and used” and obtains their executed release or consent. Section 15 also requires private entities to develop a written policy that establishes a retention schedule and guidelines for the timely destruction of biometric data in compliance with BIPA.

Section 20 gives any “person aggrieved” by a violation of the Act a private “right of action” to sue for statutory damages of $1,000 per negligent violation, $5,000 per intentional violation, actual damages (if greater than the statutory damages), injunctive relief, attorney’s fees and costs.

Class Actions and Rosenbach

The consumer class actions began in 2015. The employer class actions followed two years later in 2017, nine years after BIPA’s enactment. Rosenbach is a putative consumer class action. Stacy Rosenbach, as mother and next friend of Alexander Rosenbach, filed suit against Six Flags after her son visited the amusement park on a school field trip. Ms. Rosenbach learned that Six Flags scanned her son’s thumbprint to allow him access to the amusement park on a season pass. The lawsuit did not allege any actual harm to her son. It alleged that Six Flags failed to inform Alexander or his mother of the specific purpose and length of term for which his fingerprint had been collected, and failed to obtain his written consent or hers prior to collecting it.

When Six Flags’ initial motion to dismiss was denied, the amusement park sought interlocutory review of the denial. On appeal, the appellate court sided with Six Flags and held that plaintiff must allege some actual harm—not just a violation of the Act—to be a “person aggrieved by a violation of this Act.” If every technical violation of BIPA was actionable, it would render “superfluous” the requirement that a person be “aggrieved by a violation of this Act.” Rosenbach v. Six Flags Entertainment Corp., 2017 Il. App.(1st) 1702717, ¶ 23.

The Illinois Supreme Court rejected the appellate court’s ruling that actual injury is a prerequisite to the recovery of statutory damages under BIPA. It said this was “antithetical to the Act’s preventative and deterrent purposes” and held that a violation of BIPA’s notice and consent provisions was a “real and significant” injury:

When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, “the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.” This is no mere “technicality.” The injury is real and significant.

Id. at ¶34 (citation omitted).

Call to Action: Lessons Learned From the FACTA Class Action Debacle
In Rottner, No. 15 CH 16695 (Ill. Cir. Ct. Dec. 20, 2016), Circuit Judge Mikva struck the liquidated damages prayer for relief and explained that the legislative intent of BIPA was not to bankrupt companies:

[The legislative intent was not to put companies out of business but to keep companies in compliance with the law.]


The Fair and Accurate Credit Transactions Act of 2003 ("FACTA") is an excellent example of how the business community united when hit with a plethora of seven-figure class actions based on technical violations and no actual injury. In the FACTA cases, class action attorneys sued retailers under FACTA for not having coordinated with their credit card vendors to ensure that sales receipts redacted both a customer's credit card number and the expiration date. Because of a grammatical misinterpretation of the statute, most businesses redacted one but not the other. The business community responded in a communal uproar, contacted their legislators, and were successful in getting FACTA amended. Here, the Illinois Supreme Court may be construing BIPA in a manner that the Illinois legislature did not intend or foresee in 2008—just as many courts misread FACTA contrary to Congress' intent.

Given the Rosenbach ruling, Illinois companies and those who do business in Illinois will want to lobby the Illinois legislature to amend BIPA. For example, biometric data is not covered by a number of analogous data breach notification laws if it is encrypted or otherwise altered such that the data is unreadable. In many BIPA cases, the biometric scanner transforms the finger scan into an encrypted mathematical algorithm that is unreadable and unidentifiable. Crippling liability for mere technical violations could not be what the legislature intended.

This "call to action" also applies to companies currently in compliance with BIPA. Companies may want to periodically audit their compliance at each facility or store in Illinois, as the slightest misstep could result in class actions, despite years of compliance.
201 CMR 17.00 COMPLIANCE CHECKLIST

The Office of Consumer Affairs and Business Regulation has compiled this checklist to help small businesses in their effort to comply with 201 CMR 17.00. This Checklist is not a substitute for compliance with 201 CMR 17.00. Rather, it is designed as a useful tool to aid in the development of a written information security program for a small business or individual that handles “personal information.” Each item, presented in question form, highlights a feature of 201 CMR 17.00 that will require proactive attention in order for a plan to be compliant.

The Comprehensive Written Information Security Program (WISP)

☐ Do you have a comprehensive, written information security program (“WISP”) applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts (“PI”)?

☐ Does the WISP include administrative, technical, and physical safeguards for PI protection?

☐ Have you designated one or more employees to maintain and supervise WISP implementation and performance?

☐ Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain personal information?

☐ Have you chosen, as an alternative, to treat all your records as if they all contained PI?

☐ Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?

☐ Have you evaluated the effectiveness of current safeguards?

☐ Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?
☐ Does the WISP include disciplinary measures for violators?

☐ Does the WISP include policies and procedures for when and how records containing PI should be kept, accessed or transported off your business premises?

☐ Does the WISP provide for immediately blocking terminated employees, physical and electronic access to PI records (including deactivating their passwords and user names)?

☐ Have you taken reasonable steps to select and retain a third-party service provider that is capable of maintaining appropriate security measures consistent with 201 CMR 17.00?

☐ Have you required such third-party service provider by contract to implement and maintain such appropriate security measures?

☐ Is the amount of PI that you have collected limited to the amount reasonably necessary to accomplish your legitimate business purposes, or to comply with state or federal regulations?

☐ Is the length of time that you are storing records containing PI limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with state or federal regulations?

☐ Is access to PI records limited to those persons who have a need to know in connection with your legitimate business purpose, or in order to comply with state or federal regulations?

☐ In your WISP, have you specified the manner in which physical access to PI records is to be restricted?

☐ Have you stored your records and data containing PI in locked facilities, storage areas or containers?

☐ Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?

☐ Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?

☐ Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?

**Additional Requirements for Electronic Records**

☐ Do you have in place secure authentication protocols that provide for:
○ Control of user IDs and other identifiers?

○ A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?

○ Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect?

○ Restricting access to PI to active users and active user accounts?

○ Blocking access after multiple unsuccessful attempts to gain access?

☐ Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?

☐ Do you assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?

☐ Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?

☐ Do you, to the extent technically feasible, encrypt all PI stored on laptops or other portable devices?

☐ Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?

☐ On any system that is connected to the Internet, do you have reasonably up-to-date firewall protection for files containing PI; and operating system security patches to maintain the integrity of the PI?

☐ Do you have reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions?

☐ Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?
GDPR COMPLIANCE CHECKLIST FOR HUMAN RESOURCES DATA

☐ Map HR Data to determine:
  ☐ Types of HR data processed
  ☐ Types and locations of databases
  ☐ Identification and locations of persons and entities with access

☐ Determine Country-Specific Requirements:
  ☐ Article 88 requirements
  ☐ Labor law and record retention requirements
  ☐ Collective & works council agreement requirements

☐ Minimize data collection and processing
  ☐ Privacy by design
  ☐ Privacy by default

☐ Determine and document legal basis
  ☐ Avoid consent
  ☐ Necessary for performance of the employment contract
  ☐ Necessary to comply with EU legal obligation
  ☐ Legitimate interest v. employee privacy right
    ☐ Conduct privacy impact assessments for legitimate interest processing

☐ Determine legal basis for processing special categories of data (racial and ethnic origin, trade union membership, political opinions, religious or philosophical beliefs, health data, sex life or sexual orientation data, genetic or biometric data, and criminal convictions and offenses)
☐ Necessary to carry out obligations and rights in the field of employment and social security and social protection law

☐ Necessary to protect the vital interest of the employee/applicant

☐ Processing related to data made public by employee/applicant

☐ Establishment, exercise or defense of legal claims

☐ Preventive or occupational medicine, medical diagnosis, provision of health or social care or treatment or management of health or social care systems

☐ Authorized by EU law or carried out under the control of official authority regarding criminal convictions and offenses

☐ Prepare Data Privacy Policies for HR Data

☐ Acceptable use policy for company supplied computers and devices

☐ BYOD policy

☐ Employee monitoring and surveillance policy

☐ Employee hotline and/or online complaint policies and procedures

☐ Prepare privacy notices

☐ Applicant

☐ Employee/Former employee

☐ Conduct DPIAs for all processes that involve:

☐ Evaluation of performance

☐ Systematic monitoring

☐ Sensitive or special categories of data

☐ Cross-border transfers

☐ Automated decisions

☐ Prepare Article 30 Processing Records for the following HR functions:

☐ Recruitment/onboarding
- Entering into and performing the employment contract
- Management, Planning, and Organization
- Exercise and Enjoyment of Employment Benefits
- Compliance with laws and collective agreements
- Equality and diversity
- Health and safety
- Protection of Company and Customer Property, Equipment and Information
- Discipline and termination of Employment Relationship
- Establishment, Exercise or Defense of Legal Claims

- Prepare for employee data subject access rights

- Develop verification process

- Develop Procedure for processing requests
  - Access and rectification
  - Erasure (right to be forgotten)
  - Restriction of processing
  - Notice of rectification, erasure and restriction
  - Portability
  - Object to legitimate interest
  - Object to automated individual decision-making

- Prepare procedure for delivering responses

- Develop Request logs and documentation

- Prepare HRIS security program to reflect:
  - Pseudonymization and encryption
☐ Ensure ongoing confidentiality, integrity, availability & resilience

☐ Restoration of data

☐ Regular testing, assessing and evaluating effectiveness

☐ Prepare HR data breach notification procedures

☐ Process to analyze breach and notify DPAs within 72 hours

☐ Process to analyze breach and notify employees/applicants without undue delay

☐ Prepare data breach notification forms

☐ Determine legal basis for cross-border data transfers

☐ Adequate countries

☐ Standard contract clauses – but

☐ EU-U.S. Privacy Shield

☐ Binding Corporate Rules

☐ Codes and certifications

☐ Derogations

☐ Vet and revise HR vendor agreements to reflect:

☐ Subject matter and duration of processing

☐ Nature and purposes of processing

☐ Types of data and categories of data subjects

☐ Obligations and rights of controller

☐ Processing based on controller’s instructions

☐ Confidentiality

☐ Assist controller with data subject rights
☐ Deletion or return of data

☐ Audits and inspections

☐ Security and data breach notification

☐ Consult works councils, where applicable, regarding:
  
  ☐ Employee monitoring
  
  ☐ DPIAs
  
  ☐ Revision of current agreements to comply with GDPR

☐ Train employees
  
  ☐ Develop role-specific training
  
  ☐ Train U.S. employees handling EU HR data

Document training
PRIVACY POLICY FOR HUMAN RESOURCES DATA

[COMPANY NAME], and its operating groups, subsidiaries and divisions within the European Union, (the “Company”) are committed to protecting the privacy and security of Personal Data and/or personal data (“Personal Data”) of prospective, current and former employees (“Employees”). The Company collects, processes, and transfers Personal Data of Employees in connection with its human resources activities. The Company is committed to complying with the EU General Data Protection Regulation, effective May 25, 2018; and all data protection laws, labor laws, and collective agreements in the countries in which it employs employees and does business regarding Employees’ Personal Data.

[The Company’s Data Protection Officer (“DPO”) is responsible for implementing the Company’s Global Data Privacy Policy for Human Resources Data (“HR Data Privacy Policy”). All questions, concerns, or complaints should be directed to the Company’s DPO at:

DPO Contact Information]

OR

[The Company has appointed [name and job title] as the person with responsibility for data protection compliance within the Company. He/she can be contacted at email address. Questions about this policy, or requests for further information, should be directed to him/her.]

Definitions

“Personal data,” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, but only to the extent such personal data pertain residents of the European Economic Area (EEA) or are otherwise subject to the GDPR.

“Personal data breach,” means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

“Process” or “processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Special personal data,” includes, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data concerning sex life or sexual orientation of an individual, and data relating to criminal convictions and offenses.
"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Privacy Principles

The Company complies with the following data privacy principles with respect to personal data:

- **Lawfulness, Fairness, and Transparency.** The Company processes Personal Data lawfully, fairly and in a transparent manner in relation to Employees. The Company will process Personal Data only if and to the extent that (1) Employees have provided valid consent, (2) the Processing is necessary for the performance of an employment contract, (3) the Processing is necessary for compliance with a legal obligation to which the Company is subject, (4) the Processing is necessary to protect the vital interests of Employees or other persons, (5) the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company, or (6) the Processing is necessary to further a legitimate interest of the Company or third party except where such interest is outweighed by the rights and freedoms of Employees. The Company will provide appropriate notice to Employees regarding the Processing of their Personal Data prior to such Processing or as soon as possible thereafter.

- **Purpose Limitation.** The Company collects Personal Data for specified, explicit and legitimate purposes set forth in this policy and does not further process Personal Data in a manner that is incompatible with those purposes;

- **Data Minimization.** The Company processes Personal Data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

- **Accuracy.** The Company processes Personal Data that is accurate and, where necessary, kept up to date; and takes all reasonable steps to ensure that any inaccurate Personal Data is erased or rectified without delay;

- **Storage Limitation.** The Company keeps Personal Data in a form which permits identification of Employees for: (1) the period of time that it is necessary to process the Personal Data for the purposes for which it was collected and processed, (2) the period required under record retention laws, (3) the applicable statute of limitations for labor and employment claims, or (4) the necessary period of time to establish, exercise, or defend legal claims; and

- **Integrity and Confidentiality.** The Company processes Personal Data in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and protection against accidental loss, destruction or damage by using appropriate technical and organizational measures.
The Purpose and Legal Basis for Processing Personal Data

The Company processes the following personal data regarding employees for the following purposes and based upon the following legal bases in furtherance of its human resources activities.

- **Recruitment/Onboarding:** The Company processes personal data such as name; contact information, education, languages, special competencies, certification information; employment history; work experience; military service information; background check information; and criminal convictions and offenses to fulfill its legitimate interest in hiring the most qualified applicants. The processing of criminal convictions and offenses in connection with the Company's recruitment and human resources activities will be carried out only under the control of official authority or when authorized by EU and EU Member State law. The Company may collect recruitment-related personal data from third parties such as recruiters, background check companies, healthcare professionals, government authorities, former employers and references you provide. The Company may also collect personal data from publicly accessible sources such as public social media profiles.

- **Performance of an employment contract:** The Company processes personal data such as job title and duties; compensation and benefits information; terms and conditions of employment; tax and banking details related to payroll, type and duration of employment, probationary period; and other information necessary to perform the terms of an employment contract. The Company may collect such information from third parties such as payroll and benefits vendors, and government authorities.

- **Compliance with obligations under applicable law and collective agreements:** The Company processes personal data such as national and governmental identification information; passport information; birth date and birth place; citizenship information; immigration information; drivers' license information; tax withholding information, trade union membership; and other information necessary to comply with its obligations under applicable law and collective agreements. The Company may collect such information from third parties such as government authorities, trade unions, and works councils or other employee representatives.

- **Management, planning and organization:** The Company processes personal data such as business contact information; job type or code; business site or location; work schedule, job assignments; promotions and transfers; job performance; awards and accomplishments; training and development information; emergency contacts; photographic image; skills, talents, and career goals; appraisal ratings; hours worked and attendance; employee policy acknowledgments, position profile data; vacancies, and geographic indicators to fulfill its legitimate interests in managing the employment relationship.
• **Equality and diversity:** The Company processes Personal Data such as racial or ethnic origin, gender; disability information, and other characteristics protected by law to comply with obligations and specific rights in the field of employment and social security and social protection law that is authorized by EU or EU Member State law or a collective agreement, and to fulfill the Company’s legitimate interest in maintaining a diverse workplace free from improper discrimination.

• **Health and safety:** The Company processes Personal Data regarding medical or health conditions, drug testing information, and health insurance information for the purposes of preventive or occupational medicine, assessment of your working capacity, medical diagnosis, or the provision of health or social care or treatment, management of health or social care systems and services or pursuant to a contract with a health professional who is subject to the obligation of professional secrecy, protection of your vital interests or the vital interests of another person, compliance with obligations and specific rights in the field of employment and social security and social protection law that is authorized by EU or EU Member State law or a collective agreement and compliance with legal obligations to provide a safe workplace. The Company may collect such information from third parties such as health care providers, third party benefits administrators, and government authorities.

• **Protection of Company and customer property, equipment and confidential information:** The Company processes the following Personal Data on company computer systems and mobile devices used for business purposes to fulfill its legitimate interest in protecting the Company and customer property, equipment, and confidential information: business e-mails, videos, photographs, and documents; user computer ID, user computer IP addresses, passwords; company web/media access information, instant messenger data; texts; log-in information; location; user computer browser version and browser add-in versions, and user computer software versions; traveler preferences, travel itinerary preferences; Company computer information and/or information related to personal computer devices used for business purposes, such as user computer ID, user computer IP addresses, and passwords; corporate credit card numbers, traveler preferences, travel itinerary preferences, Company web/media access information, user computer MAC address, user computer OS, user computer browser version and browser add-in versions, user computer software versions, dependent information for benefits purposes, and beneficiary designations for benefits purposes. The Company may collect such information from third parties such as computer vendors, internet services providers, and electronic communications vendors. The Company may also monitor employee use of company-provided equipment or the business information on personal devices to fulfill its legitimate interest in protecting company and customer property, equipment and confidential information.

• **Exercise and enjoyment of rights and benefits related to employment:** The Company processes Personal Data such as marital status, family status, and dependent information for benefits purposes; beneficiary designations for benefits purposes;
leave of absence and holiday information; data regarding the company car leasing program and records; credit card and business expense reimbursement information; and frequent flyer/traveler membership/reward program numbers to fulfill its legitimate interest to provide employees with employment related rights and benefits.

- **Discipline and termination of employment relationship:** The Company processes Personal Data regarding compliance with employment policies, internal investigation information; complaint and grievance information; and reasons for termination to fulfill its legitimate interest in administering its employment policies and providing an orderly and proper transition from employment.

- **Defense of legal claims:** The Company processes Personal Data necessary for the establishment, exercise or defense of legal claims.

**Recipients of Personal Data**

Personal Data may be disclosed as follows:

- **Internal disclosure.** Personal Data may be disclosed to management personnel, human resources (HR) personnel and information technology (IT) personnel located at the Employees’ place of employment who have a need to know about the Personal Data.

- **Disclosure to Company entities.** Personal Data may be disclosed to management personnel, HR personnel and IT personnel located at the Company Regional headquarters in Luxembourg who have a need to know about your Personal Data. Additionally, Personal Data may be disclosed to management personnel, HR personnel and IT personnel located at the Company headquarters in the United States who have a need to know about the Personal Data. The Company has implemented appropriate safeguards for the transfer of Personal Data to the U.S. through [standard contract clauses or self-certification under the EU-U.S. Privacy Shield].

- **Disclosure to Third Parties.** Personal Data may be disclosed to third party processors such as payroll and benefits vendors, background check companies, computer and internet service providers, government authorities and the like who have a need to process the Personal Data for employment purposes pursuant to the written instructions of the Company. The Company will use only third party processors providing sufficient contractual guarantees to implement appropriate technical and organizational measures to comply with applicable data protection laws and ensure the protection of Employees’ privacy rights. To the extent that such third party processors are located outside of the EU, The Company has implemented appropriate safeguards for the transfer of your Personal Data to these countries through [standard contract clauses or self-certification under the EU-U.S. Privacy Shield for Personal Data transferred to the U.S.].
Disclosure to public authorities. Additionally, The Company may be required to disclose Personal Data in response to lawful requests by public authorities to comply with national security or law enforcement requirements.

Employee Data Subject Rights

Employees, as a data subjects, have the following rights regarding their Personal Data:

- **Right of Access:** Employees have the right to obtain confirmation from the Company as to whether or not Personal Data concerning you is being processed. You also have the right to obtain the following information unless providing such Personal Data adversely affects the rights and freedoms of others: (1) purpose of the processing, (2) categories of Personal Data concerned, (3) the recipients or categories of recipients to whom your Personal Data has or will be disclosed, (4) the envisaged period for which your personal data will be stored, (5) your right to request rectification or erasure of your Personal Data or restriction of processing of Personal Data, (6) your right to lodge a complaint with a supervisory authority, (7) the source from which your Personal Data was obtained if you did not provide the Personal Data, (8) the existence of any automated decision-making, including profiling, the logic involved in such decision-making, and the significance and consequences of such processing, and (9) the country to which your Personal Data is transferred if it is transferred to a third country. The Company may charge a reasonable fee to provide such Personal Data. The Company will provide a copy of the Personal Data being processed in a commonly used electronic form where you have made your access request by electronic means.

- **Right to Rectification:** You have the right to request and obtain the rectification of inaccurate Personal Data and the completion of incomplete Personal Data including providing a supplementary statement. The Company will notify any recipients of your Personal Data regarding the rectification unless such notification involves disproportionate effort. The Company will inform you about such recipients upon your request.

- **Right to Erasure (Right to be Forgotten):** You have the right to request and obtain erasure of personal data concerning you under the following circumstances: (1) the Personal Data is no longer necessary for the purposes for which it was collected or processed, (2) you have withdrawn consent for any processing for which you provided consent, (3) you object to the processing of your Personal Data based on The Company’s legitimate interest and there are no overriding legitimate ground for the processing, (4) your Personal Data has not been lawfully processed, or (5) the Personal Data is required to be erased based on The Company’s legal obligation to erase the Personal Data. However, your right to erasure does not apply where the processing is necessary for (1) exercising the right of freedom of expression and information, (2) The Company has a legal obligation requiring the processing of your Personal Data, (3) for reasons of public interest or public health, or (4) for the
establishment, exercise or defense of legal claims. The Company will notify any recipients of your Personal Data regarding the erasure unless such notification involves disproportionate effort. The Company will inform you about such recipients upon your request.

- **Right to Restrict Processing:** You have the right to obtain a restriction on the processing of your Personal Data under the following circumstances: (1) during the period of time for The Company to verify the accuracy of your Personal Data where you have objected to its accuracy, (2) the processing is unlawful and you do not want the Personal Data erased, (3) The Company no longer needs the Personal Data for the purposes for which it was processed but you require The Company to retain the information for the establishment, exercise or defense of legal claims, (4) you have objected to The Company’s legitimate interest for processing the data and then for the period of time that The Company determines whether the legitimate interest overrides your privacy rights. While the restriction is in place, The Company will store and process the Personal Data subject to the restriction; process such Personal Data with your consent, for the establishment, exercise or defense of legal claims, to protect the rights of others, or for reasons of important public interest. Further, The Company will provide you with prior notice if the restriction is being lifted. The Company will notify any recipients of your Personal Data regarding the restriction unless such notification involves disproportionate effort. The Company will inform you about such recipients upon your request.

- **Right to Portability:** You have the right to receive Personal Data that you have provided to The Company and transmit such Personal Data to another controller where the processing of such Personal Data is based on consent and is processed by automated means. Additionally, you have the right to require The Company to transmit such Personal Data directly to another controller, where technically feasible. This right is not applicable if it adversely affects the rights and freedoms of others.

- **Right to Object:** You have the right to object to the processing of your Personal Data if the processing is based upon The Company’s legitimate interest, including any profiling based on such processing. The Company will cease processing such Personal Data unless The Company can demonstrate a compelling legitimate ground for the processing that outweighs your interest, rights or freedoms; or unless continued processing is necessary for the establishment, exercise or defense of legal claims.

- **Right not to be Subject to Automated Decision-Making, Including Profiling:** You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or significantly affects you. The Company will provide a person to whom you can express your point of view and to contest the decision. This right does not apply if the decision is necessary to enter into or perform a contract between you and The Company, is authorized by applicable law, or is based on your explicit consent.
To make a subject access request, you should send the request to the Company’s [DPO at email address] OR [name and email address]. In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform you if it needs to verify your identity and the documents it requires.

The Company normally will respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of an individual's personal data, it may respond within three months of the date the request is received. The Company will write to you within one month of receiving the original request to tell you if this is the case.

If an employee’s access request is manifestly unfounded or excessive, the Company is not required to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an employee submits a request that is unfounded or excessive, the Company will notify the employee that this is the case and whether or not it will respond to it.

Data Security

The Company takes the security of HR-related personal data seriously. The Company has internal policies and technical measures in place to protect personal data against loss, accidental destruction, misuse or disclosure. Such internal policies and technical measures include:

- [The use of pseudonymization and encryption of personal data where appropriate];
- [Procedures and controls to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services];
- [Procedures and controls to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident];
- [Procedures for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing]; and
- [Procedures to ensure that data is not accessed, except by employees in the proper performance of their duties].

Where the Company engages third parties to Process Personal Data on its behalf, such parties are (1) required by contract to process the personal data based on the Company’s written instructions, (2) are under a duty of confidentiality, and (3) are required to implement appropriate technical and organizational measures to ensure the security of the personal data.
Impact Assessments

Some of the Processing that the Company carries out may result in risks to privacy. Where Processing would result in a high risk to individual's rights and freedoms, the Company will carry out a Data Protection Impact Assessment (DPIA) to determine the necessity and proportionality of processing. The DPIA will consider the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data Breach Notification

If the Company discovers that there has been a breach of HR-related Personal Data that poses a risk to the rights and freedoms of individuals, it will report such breach to the appropriate data protection authority within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will notify affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

[The organisation will not transfer HR-related personal data to countries outside the EEA.

OR

[HR-related personal data may be transferred to countries outside the EEA to [specify purpose]. Data is transferred outside the EEA on the basis of [specify relevant safeguards eg declaration of adequacy, binding corporate rules or other safeguards].

OR

Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details. Individuals may have access to the personal data of other individuals [and of our customers and clients] in the course of their [employment, contract, volunteer period, internship or apprenticeship]. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff [and to customers and clients].

Individuals who have access to personal data are required:
to access only data that they have authority to access and only for authorised purposes;

not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;

to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

not to store personal data on local drives or on personal devices that are used for work purposes.

[Further details about the organisation's security procedures can be found in its data security policy.]

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process [and at regular intervals thereafter]. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

QUESTIONS AND COMPLAINTS

Questions or complaints regarding the processing of your Personal Data should be directed to your local HR representative. Additionally, complaints may be submitted pursuant to grievance procedures under applicable trade union contracts. If the inquiry cannot be answered or the complaint is not resolved locally, please direct the matter to The Company by telephone, internet or regular mail as follows:

[Contact Information]

You also have the right to lodge a complaint with the local or national data protection authority in the jurisdiction where you work. A listing of the EU Data Protection Authorities ("DPAs") is

I have received, carefully read and sufficiently understood the above Privacy Notice and information contained therein.

<table>
<thead>
<tr>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Signature:</td>
</tr>
</tbody>
</table>

33625752.1
Which one do I choose? NIST Cybersecurity Framework vs ISO 27002 vs NIST 800-53

Picking a cybersecurity framework is more of a business decision and less of a technical decision. Realistically, this should be driven by compliance requirements where understanding what you need to address from a statutory, regulatory and contractual perspective should create the minimum set of compliance requirements. Understanding that baseline makes it pretty easy to understand where on the "compliance spectrum" you need to focus.

**NIST CSF < ISO 27002 < NIST 800-53 < Secure Controls Framework**

If you ask a cybersecurity professional to identify their preferred best practice, it generally comes down to NIST or ISO. If you look at this from the perspective of a debate over which soft drink tastes best (e.g., Coke vs Pepsi), it comes down to personal preferences, since both products are essentially sugary, carbonated drinks and only differ slightly in flavor and packaging. The same arguments can be made for IT security's two heavy hitters – NIST 800-53 and ISO 27002. These leading cybersecurity frameworks both cover the same fundamental building blocks of a cybersecurity program, but differ in some content and layout. Both can be great solutions, but it is important to understand that each one has its benefits and drawbacks. Therefore, choice should be driven by the type of industry your business is in. Gaining popularity is the NIST Cybersecurity Framework (NIST CSF), but it lacks appropriate coverage out of the box to be considered a comprehensive cybersecurity framework.

A key consideration for picking a cybersecurity framework comes down to the level of content the framework offers, since this governs what you can natively comply without having to bolt-on content to make it work:

**NIST Cybersecurity Framework (NIST CSF)** has the least coverage of the major cybersecurity frameworks. It works great for smaller or unregulated businesses.

**ISO 27002** is an internationally-recognized cybersecurity framework that provides coverage for many common requirements (e.g., PCI DSS, HIPAA, etc.). It is important to note that companies cannot certify against ISO 27002, just ISO 27001. ISO 27001 Appendix A contains the basic overview of the security controls needed to build an Information Security Management System (ISMS), but ISO 27002 provides those specific controls that are necessary to actually implement ISO 27001.

**NIST 800-53** includes what both ISO 27002 and NIST CSF addresses, as well as a whole host of other requirements. The Secure Controls Framework (SCF) is a "best in class" approach that covers NIST 800-53, ISO 27002 and NIST CSF. Being a hybrid, it allows you to address all three frameworks at once.

What Documentation Do I Need To Comply With NIST CSF, ISO 27002 or NIST 800-53?

To do NIST CSF, ISO 27002 or NIST 800-53 properly, it takes more than just a set of policies and standards. While those are foundational to building a cybersecurity program aligned with that framework, there is a need for program-specific guidance that helps operationalize those policies and standards (e.g., risk management program, third-party management, vulnerability management, etc.). It is important to understand what is required to be in compliance with NIST CSF vs ISO 27002 vs NIST 800-53, since there are significantly different levels of expectation.

When you look at the compliance bundles we created to help comply with NIST CSF, ISO 27002 and NIST 800-53, you will see that each has a different selection of products. These products listed below map directly to the section of NIST CSF vs ISO 27002 vs NIST 800-53. As depicted in the spectrum graphic at the top of this page, there are less requirements to comply with the NIST Cybersecurity Framework, while ISO 27002 has more requirements. However, ISO 27002 has less requirements than NIST 800-53.

<table>
<thead>
<tr>
<th>ComplianceForge Products</th>
<th>NIST CSF</th>
<th>ISO 27002</th>
<th>NIST 800-53 r4</th>
<th>NIST 800-171 r4</th>
<th>EU GDPR</th>
<th>PCI DSS</th>
<th>29 NYCRR 500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written Information Security Program (WISP) or Digital Security Program (DSP)</td>
<td>ID.0V-1</td>
<td>5.1.1</td>
<td>PM-1</td>
<td>252.204-7008</td>
<td>Art 5</td>
<td>12.1</td>
<td>500.03</td>
</tr>
<tr>
<td>Vendor Compliance Program (VCP)</td>
<td>ID.0G-4</td>
<td>15.1.1</td>
<td>PS-7</td>
<td>252.204-7012</td>
<td>Art 25</td>
<td>12.8</td>
<td>500.11</td>
</tr>
<tr>
<td>Cybersecurity Risk Management Program (RMP)</td>
<td>ID.0M-1</td>
<td>11.1.4</td>
<td>RA-9</td>
<td>252.204-7008</td>
<td>Art 28</td>
<td>12.2</td>
<td>500.09</td>
</tr>
<tr>
<td>Cybersecurity Risk Assessment Template (CRA)</td>
<td>ID.0M-1</td>
<td>11.1.4</td>
<td>RA-9</td>
<td>252.204-7008</td>
<td>Art 28</td>
<td>12.2</td>
<td>500.09</td>
</tr>
<tr>
<td>Vulnerability &amp; Patch Management Program (VPMP)</td>
<td>ID.0I-1</td>
<td>12.6.1</td>
<td>SI-2</td>
<td>252.204-7008</td>
<td>Art 35</td>
<td>8.6</td>
<td>500.05</td>
</tr>
<tr>
<td>Cybersecurity Incident Response Program (CIRP)</td>
<td>ID.0I-1</td>
<td>16.1.1</td>
<td>IR-1</td>
<td>252.204-7008</td>
<td>Art 35</td>
<td>12.3.3</td>
<td>500.16</td>
</tr>
<tr>
<td>Security &amp; Privacy By Design (SPBD)</td>
<td>N/A</td>
<td>N/A</td>
<td>Privacy Section SA-3</td>
<td>252.204-7008</td>
<td>Art 25</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>System Security Plan (SSP) &amp; POA&amp;M</td>
<td>N/A</td>
<td>N/A</td>
<td>PL-2</td>
<td>252.204-7008</td>
<td>Art 32</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Cybersecurity Standardized Operating Procedures (CSOP)</td>
<td>PL.0P-1</td>
<td>12.1.1</td>
<td>PL-7</td>
<td>252.204-7008</td>
<td>Art 32</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Continuity of Operations Plan (COOP)</td>
<td>RC.0P-1</td>
<td>17.1.2</td>
<td>CP-1</td>
<td>252.204-7008</td>
<td>Art 32</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Secure Baseline Configurations (SBC)</td>
<td>RL.0P-1</td>
<td>14.1.1</td>
<td>CM-2</td>
<td>252.204-7008</td>
<td>Art 32</td>
<td>1.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Control Validation Testing (CVT)</td>
<td>N/A</td>
<td>14.2.8</td>
<td>CA-1</td>
<td>252.204-7008</td>
<td>Art 32</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Not Sure Which Cybersecurity Framework Your Company Needs?

To help visualize it, the fourteen (14) sections of ISO 27002 security controls fit within the twenty-six (26) families of NIST 800-53 rev4 security controls. ISO 27002 is essentially a subset of NIST 800-53.

The NIST Cybersecurity Framework (NIST CSF) takes parts of ISO 27002 and parts of NIST 800-53, but is not inclusive of both. That makes the NIST CSF better for smaller companies that need a best practice framework to align with, where ISO 27002 and NIST 800-53 are better for larger companies or those that have unique compliance requirements. Unfortunately, common requirements such as the Payment Card Industry Data Security Standard (PCI DSS) are more comprehensive than the NIST CSF, so you would need to use ISO 27002 or NIST 800-53 to meet PCI DSS as a framework, unless you want to


2/6
bolt-on additional controls to the NIST CSF to make that work. Is that wrong? No, but it is just messy when you start bolting onto frameworks. Think of it along the lines of gnawing off the square sides of a peg to make it fit into a round hole, where it will eventually fit but it likely will not look very good.

One thing to keep in mind is that NIST 800-53 is a super-set of ISO 27002 - that means you will find all the components of ISO 27002 covered by NIST 800-53. However, ISO 27002 does not cover all of the areas of NIST 800-53. The following diagram provide a good representation of the additional compliance requirements that can be addressed with NIST over ISO. This shows how:

Regardless of what flavor cybersecurity program you need or want to have, ComplianceForge has a solution that can work for you. We are here to help make comprehensive cybersecurity documentation as easy and as affordable as possible. We serve businesses of all sizes, from the Fortune 500 all the way down to small businesses, since our cybersecurity documentation products are designed to scale for organizations of any size or level of complexity. Our affordable solutions range from cybersecurity policies & standards documentation, to NIST 800-171 compliance checklists, to program-level documentation, such as "turn key" incident response, risk management or vulnerability management program documents. Our focus is on helping you become audit ready!
Secure Controls Framework (SCF) Overview

If you are not familiar with the Secure Controls Framework (SCF), it was developed with the ambitious goal of providing a comprehensive catalog of cybersecurity and privacy control guidance to cover the strategic, operational and tactical needs of organizations, regardless of its size, industry or country of origin. By using the SCF, your IT, cybersecurity, legal and project teams can speak the same language about controls and requirement expectations!

The SCF is an open source project that provides free cybersecurity and privacy controls for business. The SCF focuses on internal controls, which are the cybersecurity and privacy-related policies, standards, procedures and other processes that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected.

On the comprehensive side of the spectrum, the Secure Controls Framework (SCF) provides coverage for NIST 800-53, ISO 27002 and the NIST Cybersecurity Framework, since it is a best-in-class hybrid. The Digital Security Program (DSP) has 1-1 mapping with the SCF, so the DSP provides the most comprehensive coverage of any ComplianceForge product.

NIST 800-53 Overview

The National Institute of Standards and Technology (NIST) is on the fourth revision (rev4) of Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Notice that doesn’t mention anything about private industry – NIST designed this framework to protect the US federal government. However, due to the significant outsourcing to private companies, as well as extensive regulation for businesses, NIST 800-53 best practices have become the de facto standard for private businesses that do business with the US federal government.

The Federal Information Security Management Act (FISMA) and the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) rely on the NIST 800-53 framework, so vendors to the US federal government must meet those same requirements in order to pass these rigorous certification programs. Additionally, for NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, NIST 800-53 is called out as the best practices for government contractors to secure their systems. That further helps strengthen NIST 800-53 as a best practice within the US, especially for any government contractors.

One great thing about NIST 800-53, and it applies to all NIST publications, is that it is freely available, at no cost to the public - http://csrc.nist.gov/publications/PubsSPs.html.

ISO 27002 Overview

The International Organization for Standardization (ISO) is a non-governmental organization that is headquartered in Switzerland. ISO can be a little more confusing for newcomers to IT security or compliance, since a rebranding occurred in 2007 to keep ISO's IT security documents in the 27000 series of their documentation catalog - ISO 17799 was renamed and became ISO 27002. To add to any possible confusion, ISO 27002 is a supporting document that aids in the implementation of ISO 27001.

To keep things simple, just remember that ISO 27001 lays out the framework to create an “Information Security Management System” (e.g., a comprehensive IT security program), whereas ISO 27002 contains the actual “best practices” details of what goes into building a comprehensive IT security program. Since ISO's information security framework has been around since the mid-1990s. It was in "right time at the right place" to evolve into the de facto IT security framework outside of the United States. You will find ISO 27002 extensively used by multinational corporations and for companies that do not have to specifically comply with US federal regulations. ISO 27002 is also "less paranoid" than NIST 800-53, which has an advantage of being less complex and therefore easier implement.

One unfortunate thing about ISO 27002, and it applies to all ISO publications, is that ISO charges for its publications - http://www.iso.org/iso/home/store.htm.

NIST Cybersecurity Framework Overview

The NIST Cybersecurity Framework (NIST CSF) does not introduce new standards or concepts, but leverages and integrates industry-leading cybersecurity practices that have been developed by organizations like NIST and ISO. The CSF comprises a risk-based compilation of guidelines that can help organizations identify, implement, and improve cybersecurity practices, and creates a common language for internal and external communication of cybersecurity issues.

The NIST CSF is designed to evolve with changes in cybersecurity threats, processes, and technologies. Essentially, the NIST CSF envisions effective cybersecurity as a dynamic, continuous loop of response to both threats and solutions.

The downside to the NIST CSF is that its brevity makes it incompatible with common compliance requirements, such as NIST 800-171, PCI DSS, and HIPAA. For those, more comprehensive frameworks, such as NIST 800-53 or ISO 27002 are required.

Government or DoD Contractor? FAR & DFARS Implications

NIST 800-171 isn't just for Department of Defense (DoD) contractors. Representatives from the National Institute of Standards and Technology (NIST) and DoD officials have recently been putting this information out in webinars and other training seminars on NIST 800-171. Many of our clients who need to address DFARS 252.204-7012 also have to address FAR 52.204-21. One common question we receive from clients pertains to aligning with the correct security framework to ensure they have the proper coverage for compliance. This generally revolves around aligning with ISO 27001/27002, the NIST Cybersecurity Framework or NIST 800-53, since those are the most common security frameworks.

The bottom line is that utilizing the NIST Cybersecurity Framework or ISO 27001/27002 as a security framework does not directly meet the requirements of NIST 800-171. In fact, NIST 800-171 (Appendix D) maps out how the CUI security requirements of NIST 800-171 relate to NIST 800-53 and ISO 27001/27002 security controls. This includes callouts where the ISO 27001/27002 framework does not fully satisfy the requirements of NIST 800-171. Therefore, policies and standards based on NIST 800-53 are what is needed to comply with NIST 800-171.

This means that only the NIST 800-53 framework is going to meet FAR requirements of NIST 800171 - ISO 27002 and the NIST Cybersecurity Framework are going to be insufficient in coverage.

Not sure what CUI is or if you have CUI on your network? We have several free guides and videos that you can use to educate yourself on the matter or you can go to the US Government's authoritative source, the US Archives CUI Registry at https://www.archives.gov/cui/registry.
Breaches Abound: Protecting Your Business from Information Indiscretion

Presenters
Gary Berger (Director of Information Security, Greenville)
Danielle Vanderzanden (Boston/Portland, ME)

Moderator
Bruce A. Griggs (Austin)

Security and Privacy Trends and Statistics

2018 Statistics

- As of 2018, there were 42 people and groups on the FBI’s Cyber Most Wanted list.
- New malware variants for mobile devices are increasing, and 99.9% of them came from third-party app stores.
- The U.S. government budgeted $15 billion dollars for cyber security-related issues for fiscal year 2019.
- A 2018 study from Juniper Research predicted that 12 billion records would be stolen in 2018.
2019: Threats Experts Predict

- **Biometric Data**: Cybercriminals will focus on exposing vulnerabilities in touch ID sensors, facial recognition, and passcodes.
- **Card Skimming**: Cybercriminals will skim thousands of credit cards from online shopping sites with a simple undetectable malware download resulting in millions of dollars of losses.
- **Wireless Carrier**: Cybercriminals will attack a major wireless carrier, steal personal information from millions of consumers, and potentially disable wireless communications in the U.S.
- **The Cloud**: A top vendor will suffer a breach thereby compromising sensitive information of major companies.

2019: Defenses to Existing and Predicted Threats

- **Employee Engagement**: Human transgressions (often employees) remain the primary source of information insecurity.
- **Regulatory Awareness**: Keeping up with the constant barrage of changing laws could be a full-time job.
- **Defensible Information Security Practices**: Informed security resources are essential.
- **Coordinating Your Effort**: Getting your team in the same room and on the same page is essential.
- **Physical, Technical, and Administrative Measures**: Each of your employees is part of your administrative layer of protection.
What is the Largest Cybersecurity Threat Companies Face?

- Malicious employee attacks
- Careless or uninformed employees
- Threats from outsiders
- Technical issues

What is the Largest Vulnerability?

- Poor IT management
- Inadequate investments in security
- Business email compromise
- Lost or stolen devices
- Lack of oversight or accountability
Avoiding the Phish

What elements of the preceding email look real?

- Appearance of signature block
- Accuracy of phone numbers, contact information, etc.
- Factual circumstances/type of thing employment lawyers do in the ordinary course of business
- Familiarity of sender/recipient
Avoiding the Phish (cont.)

- What elements of the preceding email raise red flags?
  - None
  - It seeks highly sensitive PII (tax ID numbers)

Avoiding the Phish (cont.)

- What should our associate do when she receives this request?
  - Delete the email immediately
  - Call to check on authenticity
  - Attach the W-4 and W-9 and email immediately to the client
  - Obtain the information and share it via secure link/encrypted email
Avoiding the Phish (cont.)

What elements of the preceding email raise red flags?

- Typo in “All mailbox user’s are required to validate their account for proper access.”
- Lack of identifying information
- Addressed to “User”
- Absence of signature block and credential information
- @Help-Desk Server
Avoiding the Phish (cont.)

**Microsoft Outlook Office365**

*Your New Password Request*

Your password reset is in process and your current password will be disabled shortly. The password reset link will be forwarded to the new optional email address submitted.

Ignore this email notification your request will take effect shortly.

If you did not request this password reset, use the Cancel Request button to cancel the password reset and keep your current password.

Cancel Request

This message will take a brief period before this request takes effect. This is a mandatory communication about the service. To set communication preferences for other cases.

Avoiding the Phish (cont.)

---

**Office 365**

Dear User,

Your Microsoft Outlook Account Requires an Urgent Validation to ensure it would not be deactivated within 24 hours. Please proceed to the Microsoft Outlook Validation page by clicking on the icon below to get started.

Get Started

Thank you for using Microsoft Outlook.

To stop receiving mail that is marked as clutter, go to Options. To stop receiving notifications about clutter, go to Options and turn them off. This system notification isn't an email message and you can't reply to it.

---
Why Are We Tormenting HR Professionals With These Issues

- Employees are your first line of defense (and the most common source of information exfiltration)
- Courts are imposing liability on employers when data breaches occur
- Training and auditing are necessary components of any information security program
- Policies regarding the use of employer-owned and employee-owned devices are critical
- Employers must restrict access to company information from unauthorized storage repositories and devices

How Can HR Help Solve These Problems

- Training and awareness
  - Ensuring employees know that safe and secure practices are their responsibility. (Job descriptions, performance, accountability, discipline)
  - Need more than a checklist/checkbox approach
  - Sending 30-minute video once per year doesn’t fulfill the intent
  - Program can be completely ineffective if it’s just a checkbox
  - Training needs to be entertaining
    - Folks have put together short clips with professional actors/others and humorous
    - Cartoon approach
  - Make it interactive – if people are reading email or doing other things, you get nowhere
What Does HR Need to Know About Security

- Frameworks
- ISO
- NIST
- CSI
- COBIT
- ITIL

What Essential Controls Should Your Organization Apply

- Governance and BOD involvement
- Reviews and audits
- Vulnerability assessments
- Penetration tests
- 3rd party involvement
What Are the Legal Standards and Expectations/Who Enforces Them

- Unfair and Deceptive Trade Practices (FTC)
- Health Insurance Portability and Accountability Act (HHS Office for Civil Rights)
- Family Educational Rights and Privacy Act (Family Compliance Office in DOE)

What Are the Legal Standards and Expectations/Who Enforces Them (cont.)

- Gramm-Leach Bliley Act (FTC)
- European Union General Data Protection (EU Member State Data Protection Authorities (DPAs))
- Children’s Online Privacy Protection Act (FTC)
- State Attorneys General (e.g., Illinois BIPA, Massachusetts WISP, etc.)
What Are the Areas of High Risk on Which HR Should Focus

- BYOD
- Personal email
- Cloud usage
- Inadequate controls on data access
- External storage devices

Breaches Abound: Protecting Your Business from Information Indiscretion

Presenters
Gary Berger (Director of Information Security, Greenville)
Danielle Vanderzanden (Boston/Portland, ME)

Moderator
Bruce A. Griggs (Austin)