Data Governance Program

by Exelegent & Microsoft

6 Time Gold Microsoft Partner

Exelegent

One of the highest ranked Security, Office365 and Azure Providers

http://www.exelegent.com/ · 51 - 200 employees · 36 W Main Street, Suite 300, Freehold, NJ, US 07728

CONTACT > Search for other providers

This provider has demonstrated competency in the following areas

Gold	Cloud Productivity
Gold	Windows and Devices
Gold	DevOps
Gold	Data Platform
Gold	Cloud Platform
Gold	Data Analytics

About us

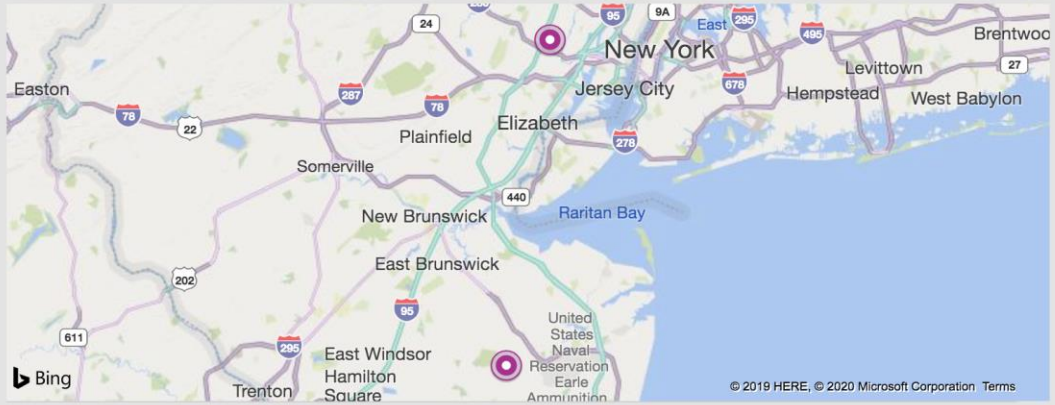
Exelegent is a cyber security and professional services company where efficiency is standard, and our customers are our partners. Headquartered in Freehold, NJ with supporting offices in Newark, NJ and L'viv Ukraine, Exelegent leverages years of experience to bring about a world-class experience for our clients.

Our specialties include:

- Office 365 Migration
- Security Audits
- Regulatory Compliance
- Vulnerability Remediation
- Digital Workplace
- Vendor Management
- Digital CTO
- Penetration Testing
- Full suite of MSP services including a 24x7 Helpdesk.

With clients in healthcare, financial services, life sciences, aerospace and defense, insurance and so many more; Exelegent is well equipped to tackle the challenges of modern businesses. As cybercrime becomes increasingly sophisticated it becomes more important to have companies like Exelegent dedicated to protecting your company's assets and information. Do not be caught off guard, give Exelegent a call.

Top locations



36 W Main Street, Suite 300, Freehold, NJ, US 07728

495 N 13th street, Newark, NJ, US 07107

Data Governance Program Requirements

Legislation and risk

- Existing and emerging regulation and policies are likely to have a huge impact on data governance, affecting patients' data privacy rights, healthcare organizations as well.
- Safeguarding and protection: everyone has the right to protection of personal date, and processing of such data must be fair - only carried out for specified purposes and with the consent of the person concerned.

Data sharing, security and cybersecurity

- Healthcare experiences twice the number of Cyber Attacks as other Industries. Cyber Security assessments provide an in-depth review of an organization's ability to protect its information assets and its preparedness against cyber attack.

Digital Workplace and Cloud Adoption

- Cloud based clinical software offers multiple accessibility options. To make the most of this exciting technology, re-assess existing use cases and future scenarios to ensure controls are in place and auditability is preserved
- Ensure there's visibility over any future activities that may result in the flow of data offshore.

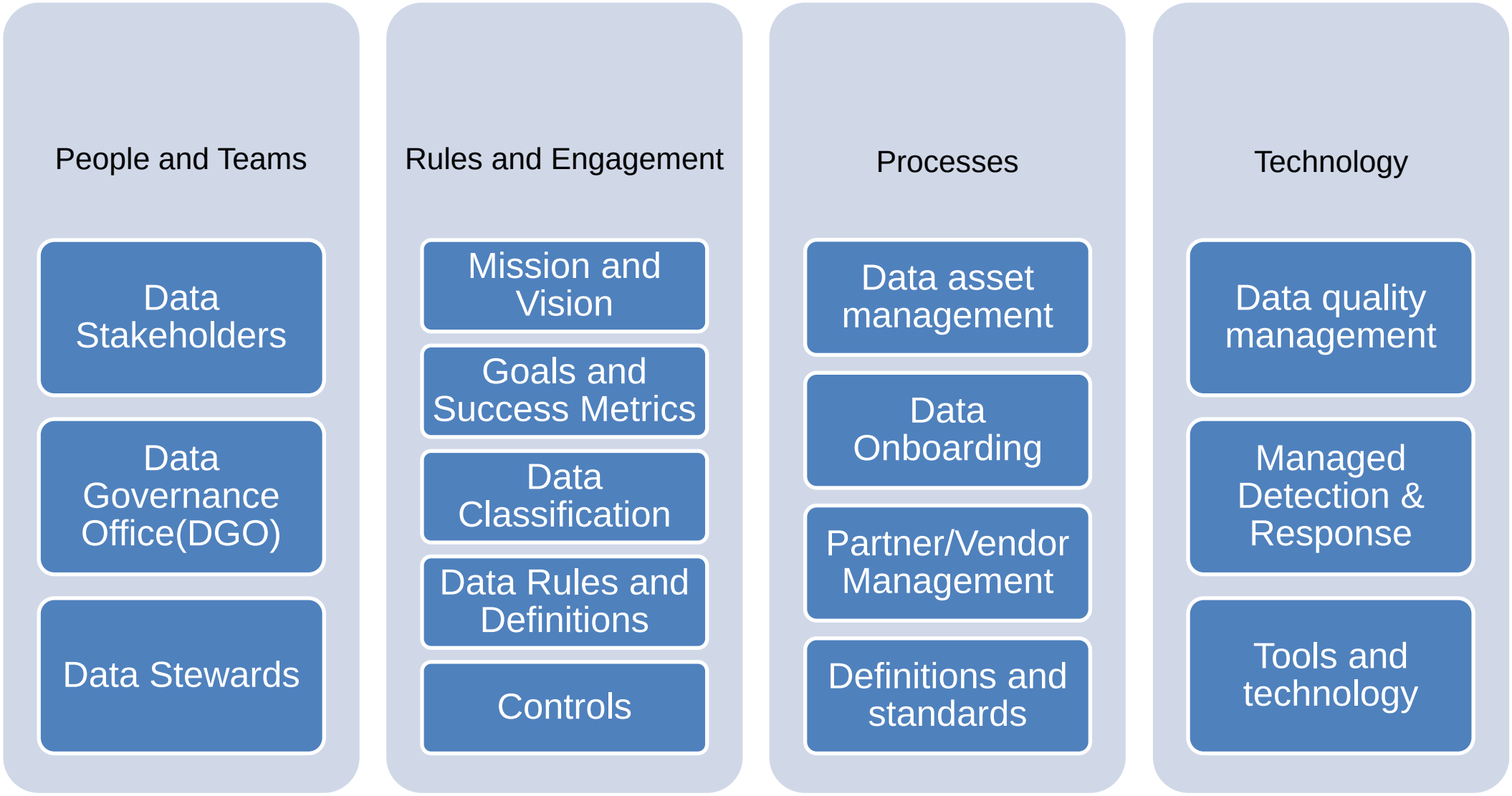
Enable conformance to data policies, standards, architecture and procedures - have a shared taxonomy and ensure compliance

Use a consistent framework to help organizations sponsor, track and oversee the delivery of data management projects and services in an increasingly complex environment

Create accountability and connectivity of roles, vertically and horizontally - enhancing organizational/system decision-making

Promote understanding of the value of data assets - maintain momentum in a data-driven digital economy

Healthcare Data Governance Approach



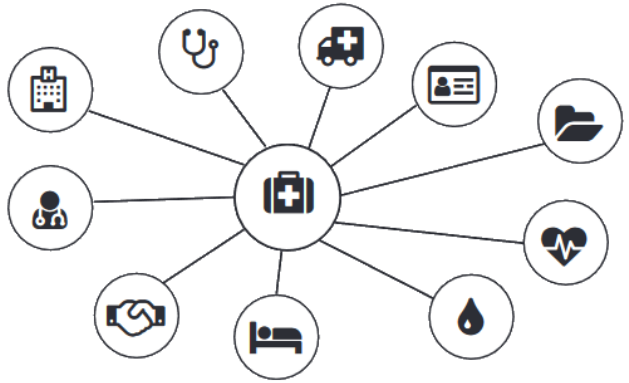
Data Governance - Rules and Engagement

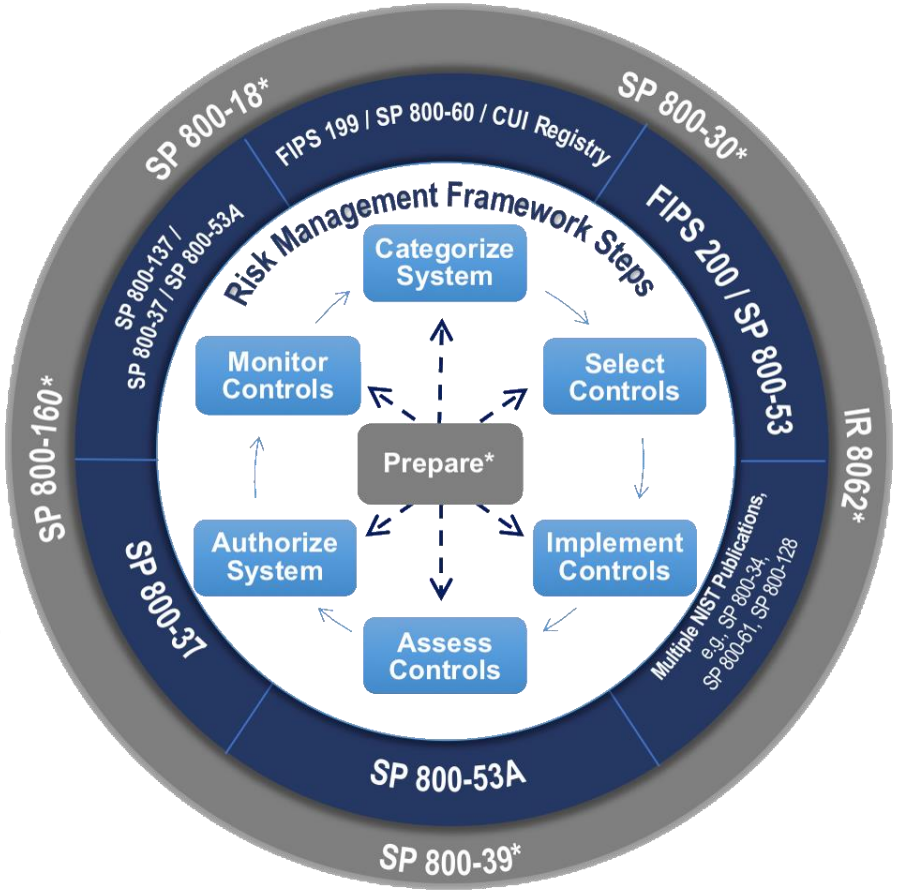
Controls

- Specifying, designing, implementing, or performing data related actions
- Can be automated, manual, or technology-enabled manual processes
- Based on **NIST Risk Management** Framework, **CIS**, **HIPAA** and **PDDQ**

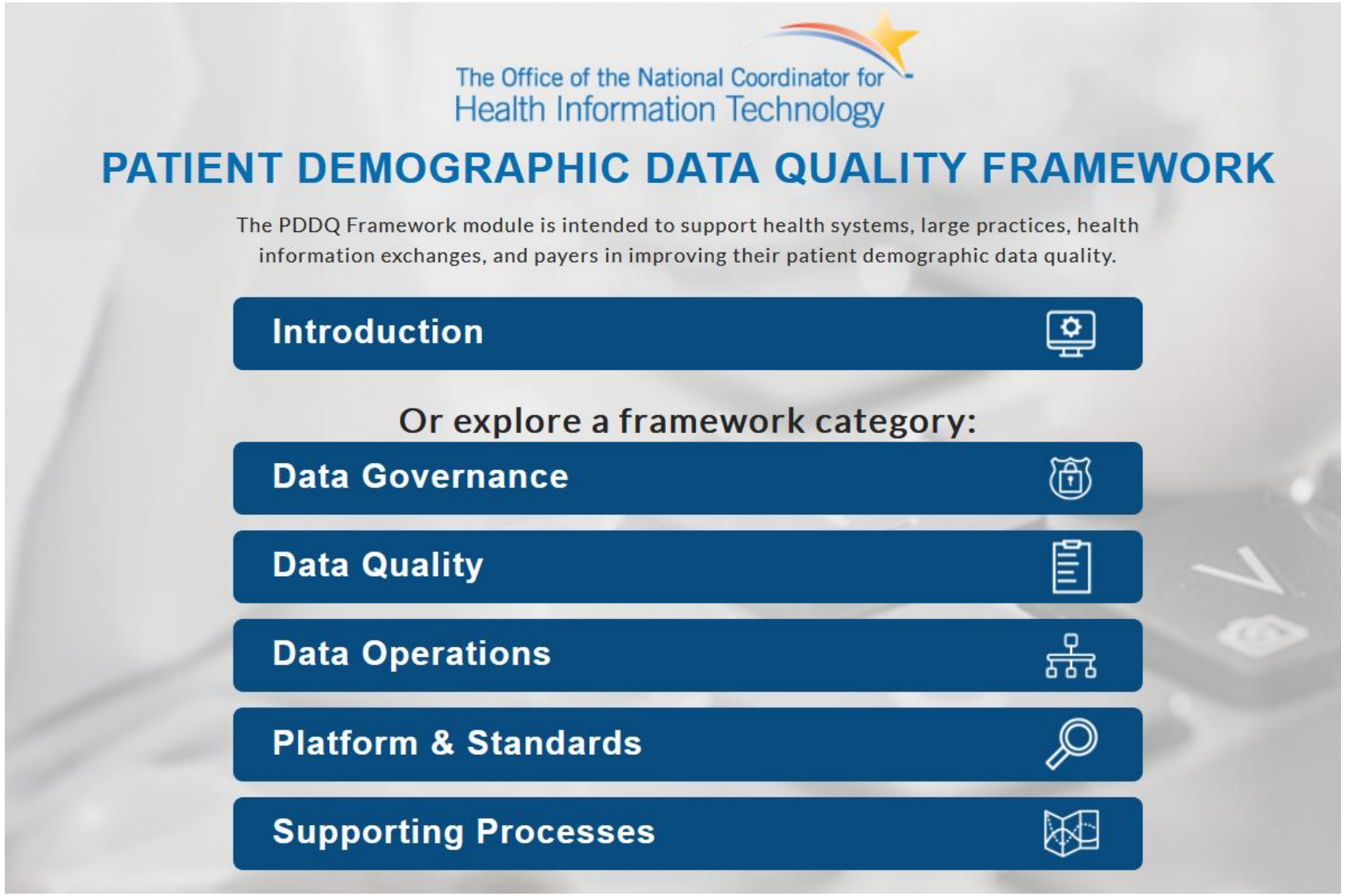
HIPAA

CIS Controls®





Patient Demographic Data Quality Framework



Patient Demographic Data Quality Framework

Addresses practical, proven activities needed to achieve and sustain effective management of an organization's patient demographic data.

Category	Process Area
Data Governance	Governance Management
	Communications
	Data Management Function
	Business Glossary
	Metadata Management
Data Quality	Data Quality Planning
	Data Profiling
	Data Quality Assessment
	Data Cleansing & Improvement
Data Operations	Data Requirements Definition
	Data Lifecycle Management
	Data Provider Management
Platform & Standards	Data Standards
	Data Management Platform
	Data Integration
	Historical Data, Archiving & Retention
Supporting Processes	Measurement & Analysis
	Process Management
	Process Quality Assurance

Governance Management

1.1 Data governance
2.1 Data governance policies and processes

Communication

1.1 Policies, processes and procedures communications plan

Business Glossary

1.1 Unique Names and Definitions for patient demographic business terms
3.1 Business terms in system requirements

Historical Data, Archiving, and Retention

2.1 Patient demographic data retention

Metadata Management

1.1 Metadata definition
3.1 Plan for capturing, maintaining, and governing metadata

Data Requirements Definition

2.1 Consistent Data requirements
2.2 Data requirements alignment with internal (or external) data model(s) and other related artifacts

Data Standards

1.1 Data representations, security, access, and provisioning definition

Cyber Security Frameworks & HIPAA Crosswalks

CIS Controls®	Policy	Implementation	Automation	Reporting
1. Inventory of Authorized and Unauthorized Devices				
1.1. Utilize an Active Discovery Tool	On All Systems	On All Systems	On All Systems	Not Implemented
1.2. Use a Passive Asset Discovery Tool	On All Systems	On All Systems	On All Systems	Not Implemented
1.3. Use DHCP Logging to Update Asset Inventory	On All Systems	On All Systems	On All Systems	Not Implemented
1.4. Maintain Detailed Asset Inventory	On All Systems			
1.5. Maintain Asset Inventory Information	On All Systems			
1.6. Address Unauthorized Assets	On All Systems			
1.7. Deploy Port Level Access Control	On All Systems			
1.8. Utilize Client Certificates to Authenticate Hardware Assets	On All Systems			

Category	Subcategory	Relevant Control Mappings[2]
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d) HIPAA
	ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E) HIPAA
	ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d) HIPAA

NIST

- The HIPAA Security Rule is designed to be flexible, scalable, and technology-neutral, which enables it to accommodate integration with more detailed frameworks
- Provides an informative tool to use to help more comprehensively manage security risks in their environments

Data Governance - Rules and Engagement

Data Classification

- the process of organizing data by relevant categories so that it may be used and protected more efficiently.
- Based on **NIST 800-60** & **FIPS 199**

Classification	Data Classification Description	
Restricted/Private	High Risk	**Data and systems are classified as High Risk if:** 1. Protection of the data is required by law/regulation, 2. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.
	Security Controls	**Apply SP 800-53 High security control set** for data and systems classified as Restricted.
	Examples	PHI, PII, PCI data, and confidential information.
Internal Use	Moderate Risk	**Data and systems are classified as Moderate Risk** if they are not considered to be High Risk, and: 1. The data is not generally available to the public, or 2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or
	Security Controls	**Apply SP 800-53 Moderate security control set** for data and systems classified as Internal Use.
	Examples	Non-public contracts, ( ) internal memos and email, non-public reports, budgets, plans, financial info, IT documentation.

Data Class	Ref	Sensitive Data Elements	Public	Internal Use	Restricted	Restricted (PHI/PII)
PII	PII-1	Name: full name, maiden name, mother's maiden name, or alias				X
	PII-2	Personal identification numbers: social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, or credit card number				X
	PII-3	Personal address information: street address, or email address				X
	PII-4	Personal telephone numbers				X
	PII-5	Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting				X
	PII-8	Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person		X		
	PII-9	Provider NPI, state license number, DEA, DOT cert number		X		

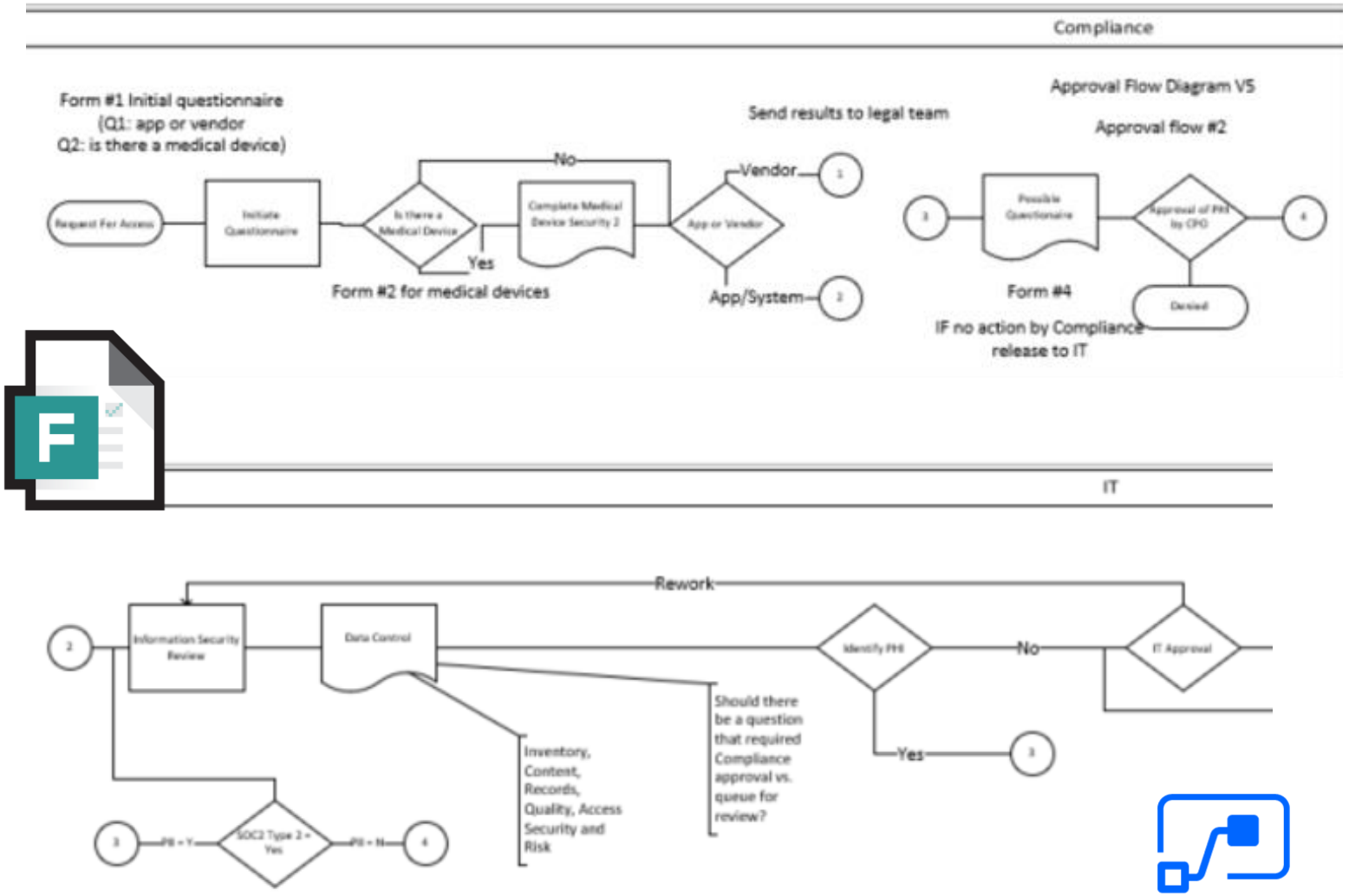
Main Components:

- **Data Labels**
- **Data Elements**

Data Governance - Processes

Data Onboarding

- Incorporates **identification and labeling of data** for strict **adherence to Data Governance Program**
- Based on **Power Automate** and **Microsoft Forms**



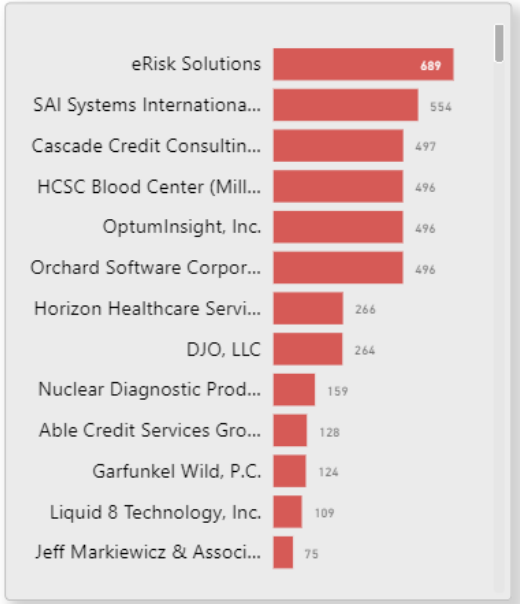
Data Governance - Processes

Partner/Vendor Management

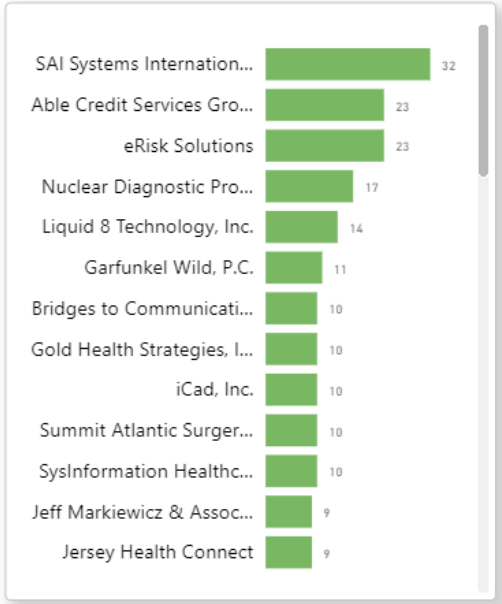
- **3rd-party vendors** typically **have access to sensitive data** like company, customer, and employee information
- align third-party vendor security programs with organization's risk appetite on an ongoing basis

Company	Company Domain	Has Access To System	Provides Data	Risk Score
A Walsh Imaging Inc	awalshimaging.com	ONEPACS	Restricted PHI	Low
A Walsh Imaging Inc	awalshimaging.net	ONEPACS	Restricted PHI	Medium
Alston & Bird, LLP	alston.com	GOOGLE DRIVE/GOOGLE TEAM DRIVE	Restricted	Medium

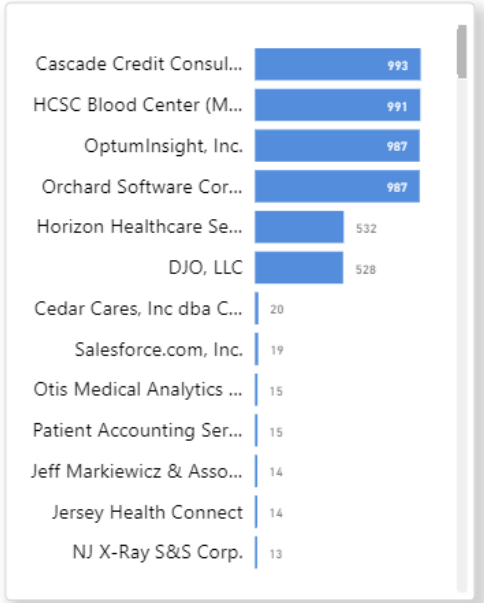
Suppliers Vulnerability Rating



Vulnerabilities



Open Ports



Data Governance – Tools & Technology

Azure Information Protection - Protect sensitive information anywhere it lives

Automatically apply data protection policies if a user's access to that data changes, the user becomes compromised or the data reaches a certain age.

Identify potentially sensitive information, like credit card or bank routing numbers, and automatically apply a sensitivity label and protection to the file.

Protect sensitive data when it travels outside of your organization via email, USB, or a 3rd party SaaS app.

Scan historical on-premises data files for potentially sensitive information before you move to the cloud.

Grant select partners and customers access rights to sensitive information.

Detect and protect sensitive data that falls under compliance regulations, such as GDPR.

Scan for sensitive files on-premises & cloud

Manage sensitive data prior to migrating to Office 365 or other cloud services

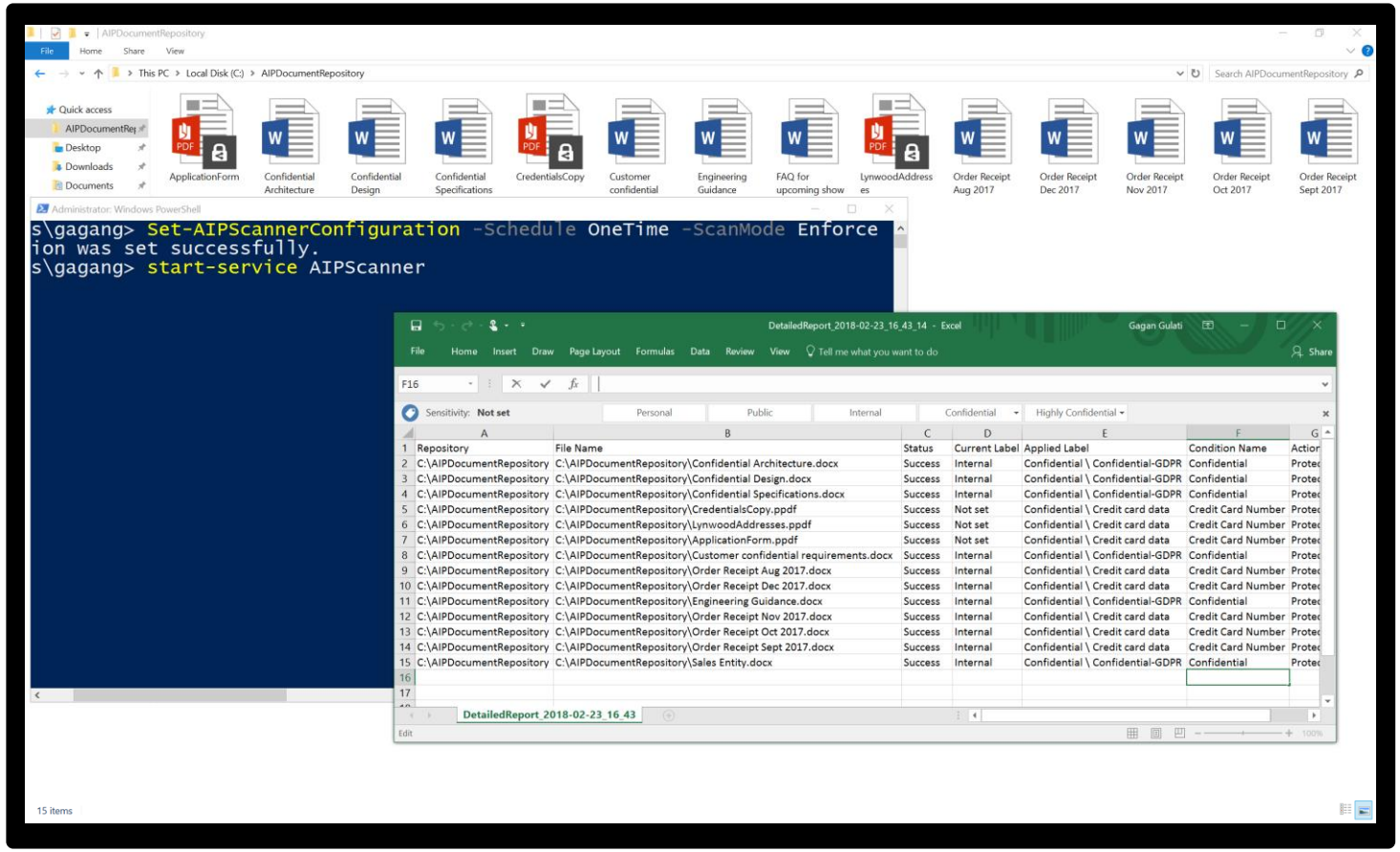
- Use discover mode to identify and report on files containing sensitive data
- Use enforce mode to automatically classify, label and protect files with sensitive data

Structured data – Azure Purview

- data that adheres to a strict schema
- all the data has the same fields or properties

Unstructured data – MIP/AIP

- unstructured data is ambiguous
- delivered in files



Exelegent

Information Protection Demo Results

Scan Time - <24hrs

Sensitive Info Types – 5

Sensitive Files Identified - 9214

ExelegentDemo - U.S. social security number (SSN) ExelegentDemo - U.S. social security number (SSN)	2,309 matches	Compliance	—	Sep 23, 2020
ExelegentDemo - Credit card number ExelegentDemo - Credit card number	1,258 matches	Compliance	—	Sep 23, 2020
ExelegentDemo - U.S. Passport Number ExelegentDemo - U.S. Passport Number	11 matches	Compliance	—	Sep 23, 2020
ExelegentDemo - U.S. driver's license number ExelegentDemo - U.S. driver's license number	4,484 matches	Compliance	—	Sep 23, 2020
ExelegentDemo - U.S. bank account number ExelegentDemo - U.S. bank account number	1,152 matches	Compliance	—	Sep 23, 2020

Data Governance – Typical Project

Goals and Success Metrics

- Clear program goals, scope and success criteria
- Typical Goals:
  - Enable better decision-making
  - Protect the needs of data stakeholders
  - Build standard, repeatable processes
  - Ensure transparency of processes

Milestones

1. **Environments and Requirements** – Identify teams and workstreams, prepare environments, define reporting
2. **Data Classification & Labels** – Define data elements taxonomy
3. **Systems and Apps Mapping** – Classify list of systems and apps based on data labels
4. **Azure Information Protection & Rights Management** – Implement cloud-based solution to classify and protect documents by applying classification labels and policies
5. **DSP controls implementation and effectiveness** – Reporting highlighting GAP analysis and internal/external vulnerability assessments
6. **Digital Vendor Data ownership profiles** – Classify vendors based on data labels, basic Digital Footprint
7. **Build Data Governance Processes** – Data Asset Management, Data Onboarding, Definitions and Standards

Typical Project Roadmap