

Class 10

Application Security

MIS5214

Agenda

- Emerging issues in Application Security
 - GDPR Background
 - Principles for Privacy by Design
 - Key requirements
 - Approaches to meeting requirements
 - Assessing information system documentation
 - Data lineage (“provenance”) metadata
 - Assessing a metadata approach
- A few other frameworks for application security assessment
- Some best practices for secure application development
- Test areas for auditing applications

General Data Protection Regulation (GDPR)



Created by the European Parliament, Council of the European Union, and European Commission to strengthen and unify data protection for all individuals within the European Union (EU)

- Based on beliefs:
 - Privacy is a fundamental human right
 - Privacy protection is an essential element in the functioning of democratic societies
- Goals are:
 1. To give control back to citizens and residents over their personal data
 2. To simplify the regulatory environment for international businesses by unifying regulation within the EU
- Applies to organizations based outside the European Union collecting or processing personal data of EU residents, or exporting EU residents' personal data outside the EU

GDPR's authors recognize



The existence of a “massive power imbalance between data processing entities, which determine what and how data is processed, and the individuals whose data is at stake,

i.e., whose lives might be influenced by decisions based on automated data analysis, or by failures to adequately protect private information.

...when using a specific service, many individuals are often unaware of the data processing and its consequences. Moreover, the user’s subsequent control over the nature of the processing that happens to their personal data once it is given away is limited.

“take it or leave” applications’ User License Agreements

Lastly, penalties for infringements of legal data protection obligations usually take effect only after the fact, i.e. if a breach or misuse of data has occurred already.”

Personal Data

Any information relating to an identified or identifiable natural person ('data subject'), whether it relates to his or her private, professional or public life

Can be a:

- Name
- Home address
- Email address
- Photo
- Medical information
- Bank details
- Unique identifiers
- Posts on social networking websites
- Browsing history
- Computer's IP address
- ...



GDPR Actors

- **Data subject** an identifiable natural person, based in the EU, who can be identified directly or indirectly 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
- **Data controller** is an organization that collects data from or pertaining to a data subject
- **Data processor** is an organization that processes data pertaining to a data subject on behalf of data controller (e.g. cloud service providers)
- **Data Protection Officer (DPO)** is an expert with knowledge of data protection law and information security practices that assists the controller or processor with monitoring internal compliance with GDPR

DPO is expected to be proficient in managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues pertaining to holding and processing personal and sensitive data

Privacy and Data Protection by Design

Privacy needs to be considered from the very beginning of application development.

- The term “Privacy by Design” was coined to indicate that GDPR expects privacy to be taken into account throughout the entire engineering process from the earliest design stages to the operation of the productive application system.
- “Privacy by Design” = “Data Protection by Design”

Achieving “Privacy by Design” in application systems is difficult

Privacy in itself is a complex, multifaceted and contextual notion

Additionally, it is generally not the primary requirement of an application and may come into conflict with other (functional or non-functional) requirements

GDPR seeks to remedy the current situation...

...privacy and data protection features are, on the whole, ignored by traditional software applications engineering approaches when implementing the desired functionality.

- This ignorance is caused and supported by limitations of awareness and understanding of applications developers and data developers as well as lacking tools to realize the principles of privacy by design.

Privacy and Data Protection by Design

Although the concept has found its way into legislation as the... Health Insurance Portability and Accountability Act (HIPAA) and the new European General Data Protection Regulation (GDPR), **its concrete implementation in creating secure applications remains un-clear at the present moment**

Privacy protection principles involved in Privacy by Design go beyond Article 25 to meet GDPR requirements

- Lawfulness
- Consent
- Purpose binding
- Necessity and data minimization
- Transparency and openness
- Rights of the individual
- Information Security
- Accountability
- Data protection by design and default

Art. 25 GDPR

Data protection by design and by default

- (1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
- (2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
- (3) An approved certification mechanism pursuant to [Article 42](#) may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Lawfulness

Processing of personal data is forbidden unless there is an explicit permission, e.g. by the individual's consent or by statutory provisions

- Processing of personal data is only allowed if
 - a) The individual whose personal data are being processed (“data subject”) has unambiguously given consent

or processing is necessary for

- b) Performance of a contract
- c) Compliance with a legal obligation the data controller is subject to
- d) Protection of vital interests of the data subject
- e) The public interest or in exercise of official authority vested in controller
- f) Legitimate interests pursued by data processing entities if such interests are not overridden by the fundamental rights and freedoms of the data subject

Consent

- Individuals have the right to informational self-determination
- To enable lawful data processing of an individual's personal identifiable information, individuals need to give specific, informed and explicit consent to the processing of their data
 - A declaration of consent is invalid if not all these requirements are met
 - **Transparency** of data collection and use is a prerequisite for consent
- Consent can be withdrawn with effect for the future

Purpose limitation

- Personal data obtained for one purpose must not be processed for other purposes that are not compatible with the original purpose
- The purpose has to be legitimate, and it has to be specified and made explicit to the data subject before collecting personal data

In many countries outside Europe, data is often persisted and used for multiple purposes and the principle of purpose limitation (purpose “binding”) is unknown

Necessity and data minimization

- Collection of personal data must be fully avoided or minimized at the earliest stage of processing
- Personal data must be erased (or effectively anonymized) as soon as it is not needed anymore for the given purpose

Transparency and Openness

- Relevant stakeholders are provided sufficient information about the collection and use of their personal data
 - They need to be able to understand possible risks induced by the processing and actions they can take to control the processing
- Transparency is a necessary requirement for fair data processing
 - **Data subjects** need information to exercise their rights
 - **Data controllers** need information to evaluate their processors
 - **Data Protection Officers** and other authorities need to monitor according to their responsibilities

Rights of the individual

Individuals have right to access, review and rectify, as well as block access, constrain use, and erase their personal data

- Data subjects have the right to withdraw given consent with effect for the future

These rights should be supported in a way that individuals can effectively and conveniently exercise their rights

*The implementation and support of these rights is promoted by the **privacy by design** principles that demands considering the user and stipulates **privacy by default***

Information Security

Appropriate technical and organizational safeguards for privacy and data protection must be applied

- **Confidentiality** requires that unauthorized access and processing, manipulation, loss, destruction and damage are prevented
- **Integrity** requires that data have to be accurate
- **Availability** requires organizational and technical processes for appropriately handling the data and providing the possibility for individuals to exercise their rights have to be available whenever necessary

Accountability

Data privacy risk assessment and data protection impact assessment (DPIA) provides a basis for planning and implementing controls and is necessary for demonstrating compliance

- Compliance with privacy principles and legal requirements, data protection controls, and incident management (breach notifications) needs to be determined
 - Data Protection Officers may be installed to perform internal audits and handle complaints
- Implies
 - **Monitoring**
 - **Clear identification of responsibilities for internal and external auditing**
 - **Assessment and assurance of information security controls applied to all data processing**

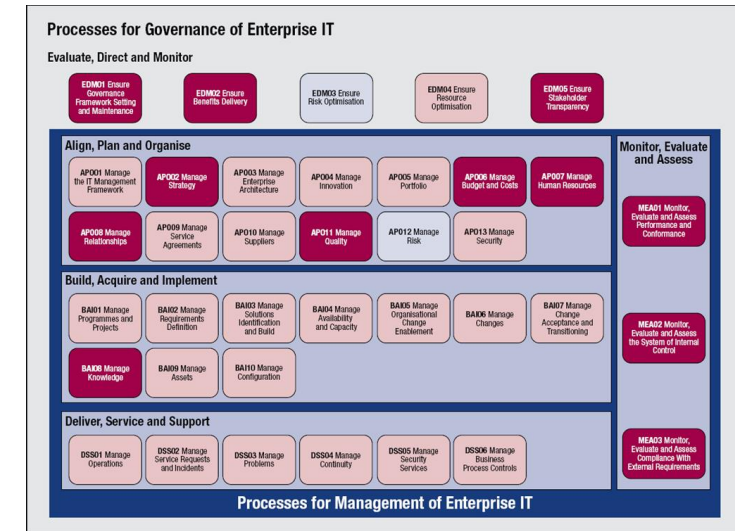
GDPR expects standard approaches to protecting confidentiality, integrity and availability to be in place

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

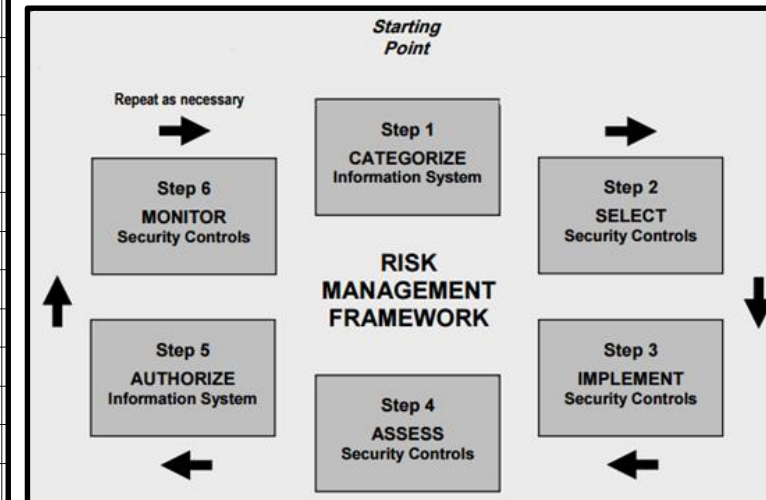
NIST Framework for Improving Critical Infrastructure Cyber Security

CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

NIST Security Control Catalog (SP 800-53, SP 800-53A)



ISACA's COBIT 5 for RISK



NIST Risk Management Framework (SP 800-30, SP 800-37r1, 800-39)

Privacy by design...

- Goes beyond the standard approaches
- Is about building in additional privacy features into information systems that work from the very beginning of data processing and implement privacy controls that protect individuals' personal data by default
- Much work on Privacy by Design has focused on "Big Data" systems

Danezis, G. et al. (2014) "Privacy and Data Protection by Design", European Union Agency for Network and Information Security (ENISA)

D'Acquisto, G. et al. (2015) "Privacy by design in big data", European Union Agency for Network and Information Security (ENISA)

	BIG DATA VALUE CHAIN	KEY PRIVACY BY DESIGN STRATEGY	IMPLEMENTATION
1	Data acquisition/collection	MINIMIZE	Define what data are needed before collection, select before collect (reduce data fields, define relevant controls, delete unwanted information, etc), Privacy Impact Assessments.
		AGGREGATE	Local anonymization (at source).
		HIDE	Privacy enhancing end-user tools, e.g. anti-tracking tools, encryption tools, identity masking tools, secure file sharing, etc.
		INFORM	Provide appropriate notice to individuals – Transparency mechanisms.
		CONTROL	Appropriate mechanisms for expressing consent. Opt-out mechanisms. Mechanisms for expressing privacy preferences, sticky policies, personal data stores.
2	Data analysis & data curation	AGGREGATE	Anonymization techniques (Data acquisition/coll differential privacy).
		HIDE	Searchable encryption, privacy preserving computations.
3	Data storage	HIDE	Encryption of data at rest. Authentication and access control mechanisms. Other measures for secure data storage.
		SEPARATE	Distributed/ de-centralised storage and analytics facilities.
4	Data use	AGGREGATE	Anonymization techniques. Data quality, data provenance.
5	All phases	ENFORCE/ DEMONSTRATE	Automated policy definition, enforcement, accountability and compliance tools.

Key requirements fall outside standard information security approaches considered in some industries

1. **Collection** of personal data is **fully avoided or minimized** at the earliest stage of processing
2. Data subjects give **specific, informed and explicit consent** to the processing of their data
 - Legitimate processing is specified and made explicit to the data subject before collecting personal data
 - Data subjects understand possible risks induced by the processing
 - Data subjects understand actions they can take to control the processing
3. Data subjects have **right to access, review and rectify** their personal data
4. Data subjects have the **right to withdraw given consent** with effect for the future and block access, constrain processing and use, and erase their personal data
5. Personal **data obtained for one purpose must not be processed for other purposes** not compatible with the original purpose

Some similarity to health information privacy requirements of Health Insurance Portability and Accountability Act (HIPAA) of 1996

Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI

Covered entities must:

- Ensure the **confidentiality, integrity, and availability** of all e-PHI they create, receive, maintain or transmit
- **Identify and protect against reasonably anticipated threats to the security or integrity** of the information
- **Protect against** reasonably anticipated, **impermissible uses or disclosures**
- Ensure compliance by their workforce

Data subject (or their personal representative) has the right to access their personal data records

Data subject can request a change or amendment to correct their data record

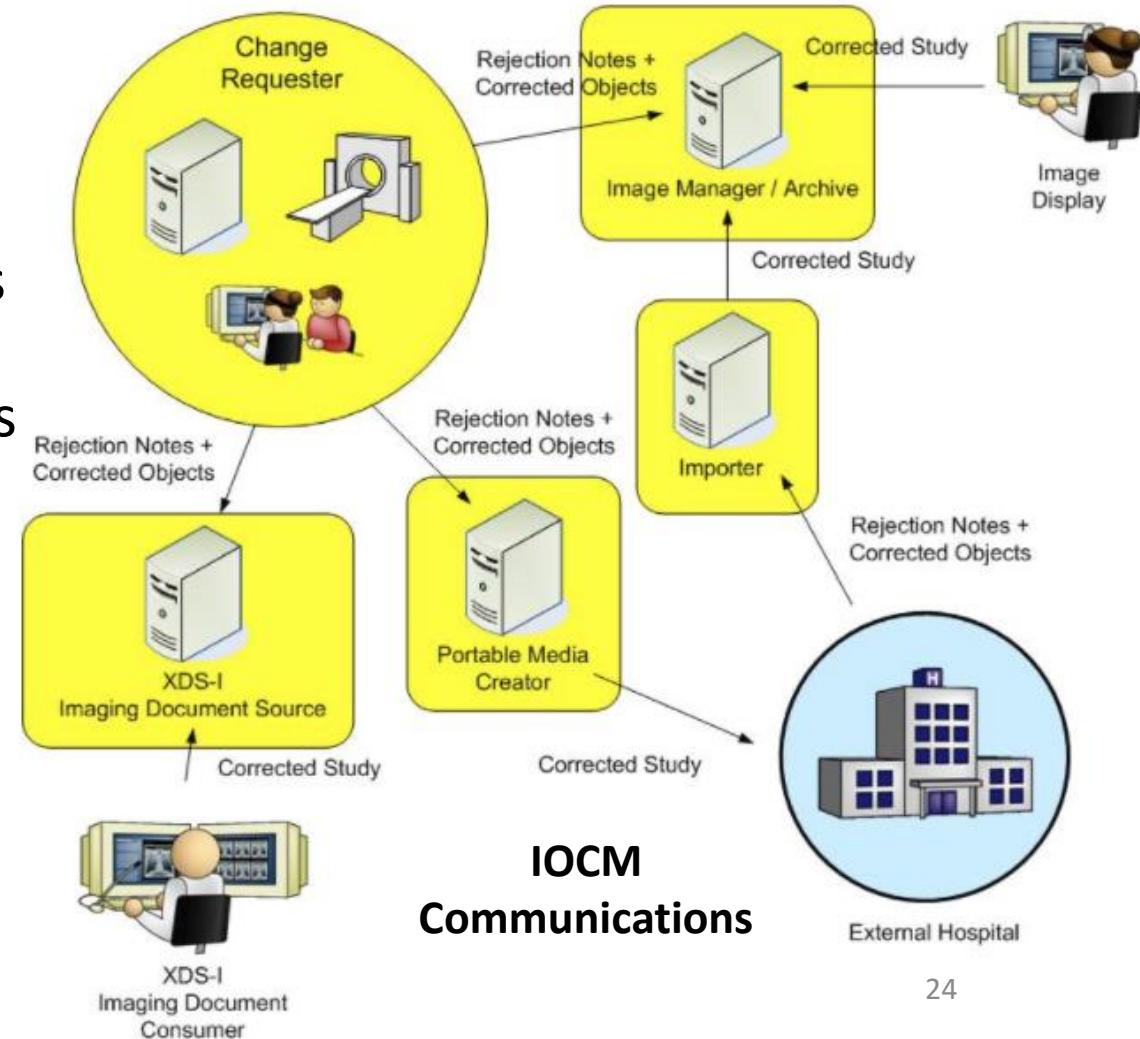
- Health care provider or health plan must respond to their request. If it created the information, it must amend inaccurate or incomplete information
- If provider or plan does not agree with the request, data subject has the right to submit a statement of disagreement that the provider or plan must add to the data subject's record

Imaging Object Change Management (IOCM)

Information system-based communication protocol to meet HIPPA requirements for changing or deleting a patient's data record ("image object")

Includes support for:

1. Correction or rejection of imaging instances for quality reasons
2. **Correction or rejection** of imaging instances for patient safety reasons
3. Correction of Modality Worklist selection
4. **Data retention expiration**



Agenda

- Emerging issues in Application Security
 - ✓ GDPR Background
 - ✓ Principles for Privacy by Design
 - ✓ Key requirements
 - ✓ Approaches to meeting requirements
 - Assessing information system documentation
 - Data lineage (“provenance”) metadata
 - Assessing a metadata approach
- A few other frameworks for application security assessment
- Some best practices for secure application development
- Test areas for auditing applications

One approach to assessing if key requirements are met

- *“A type 1 SOC 2[®] engagement is an **examination of**”*
 1. *“A service organization’s description of its system and the”*
 2. *“**Suitability of the design of its controls** that are relevant to security, availability, processing integrity, confidentiality, or privacy.”*
- *A type 2 SOC 2[®] engagement addresses the same subject matter as a type 1 SOC 2[®] engagement but **also includes an examination of the**”*
 3. *“**Operating effectiveness of the controls.**”*

A service auditor’s type 2 SOC 2[®] report includes a detailed description of the service auditor’s tests of controls and the results of those tests.”

How to assess key Privacy by Design requirements

Examine the organization's

1. Description of its system

2. Suitability of the design of its controls

1. Relevant to key privacy and protection by design principles

2. Relevant to security of confidentiality, availability, and processing integrity

3. Operating effectiveness of the controls

i.e. Auditor's tests of controls and the results of those tests

Assess whether privacy protection controls/services are included:

- 1. Is the collection of personal data fully avoided or minimized at the earliest stage of processing ?**
- 2. Are data subjects able to give specific, informed and explicit consent to the processing of their data ?**
 - Is legitimate processing specified and made explicit to the data subject before collecting personal data ?
 - Can data subjects understand possible risks induced by the processing ?
 - Can data subjects control the processing? And if so, can they understand actions they can take to control the processing ?
- 3. Can data subjects access, review and rectify their personal data?**
- 4. Are data subjects able to withdraw given consent with effect for the future by:**
 - a. Blocking access to their personal data?
 - b. Constraining processing and usage of their personal data?
 - c. Erasing their personal data?
- 5. Are capabilities provided with which personal data obtained for one purpose are blocked and restricted from processing for other purposes not compatible with the original purpose?**

Description of the system should include:

- Types of services provided
- Components of the system used to provide the services
 - Infrastructure
 - Software
 - People
 - Procedures
 - Data
- Boundaries of the systems covered by the description
- Information exchanges, i.e. how data are received into and provided out of the system
 - Complementary controls included in the design of the system
 - Procedures to determine that the information and its processing, maintenance, and storage are subject to appropriate controls

Where to look in the description of an organization's system for data subject's personal information?

Descriptions of the following system components are expected

- **Infrastructure.** The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks)
- **Software.** The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- **People.** The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- **Procedures.** The automated and manual procedures.
- **Data.** Transaction streams, files, **databases, tables,** and output used or processed by the system."

Example – Looking for documentation of data subjects' personal information in an enterprise information system



www.navigationdatacenter.us/ports/ports.htm

Welcome to the US Army Corps of Engineers
Navigation Data Center

[NDC Home Data](#)

Ports and Waterways Facilities

[Mission](#)

[Port Facility Spreadsheet](#)

[Complete Dock List](#)

[Master Docks Plus Public Extract](#)

[Download shape files: Shape Files](#)

The Navigation Data Center maintains a database (**Master Docks Plus**) of over 40,000 port-and-waterway facilities and other navigation points of interest. The data describe the physical and inter-modal (infrastructure) characteristics of the coastal, Great Lakes, and inland ports of the United States. Data are also included for facilities in Alaska, Hawaii, Puerto Rico, the U.S. Virgin Islands, and the trust territories of the Pacific. The data include, but are not limited to location (latitude/longitude, waterway, mile, and bank); operations (name, owner, operator, purpose, handling equipment, rates, and details of open-and-covered storage facilities); type and dimension of construction (length of berthing space for vessels and/or barges, depth, apron width, deck elevation, and details of rail-and-highway access); and utilities available (water, electricity, and fire protection).

The data are available in several formats.

The **Complete Dock List** spreadsheet contains a list of all facility types (dock, anchorage, mile point, etc) that may be reported as the origin or destination of commercial waterborne vessel moves. Attributes included in the list are the unique navigation-unit identifier, official name, facility type, latitude/longitude, United Nations Location Code, service initiation date, service termination date, port name, waterway name, and mile. Data included is for all facility types that were available for use during the previous two years.

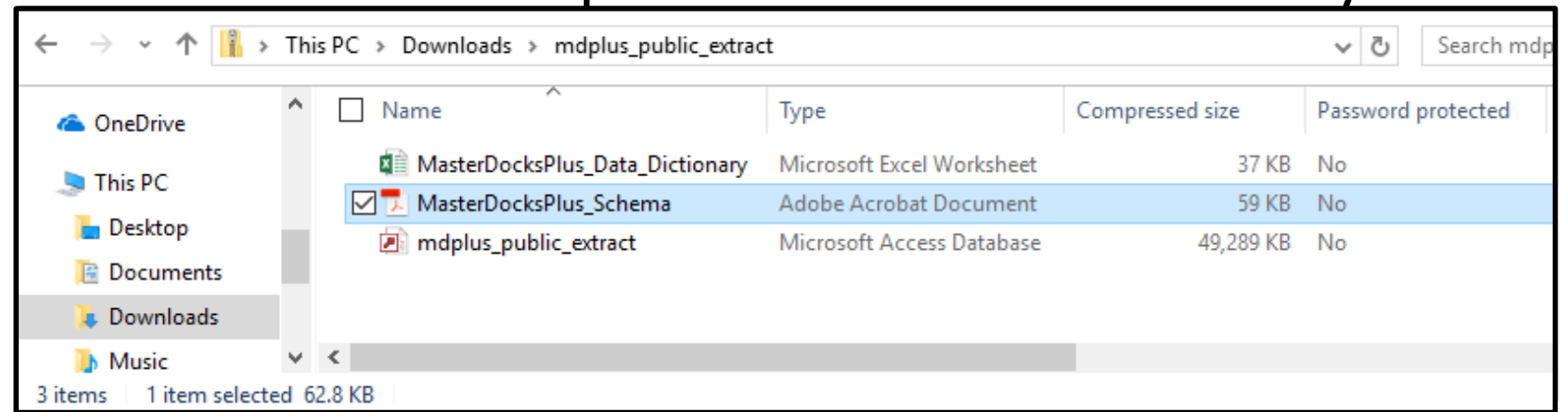
The **Port Facility** spreadsheet is similar to the **Complete Dock List** but has an expanded list of attributes not including mile points. The additional attributes include a location description, street address, city, state, zip code, county, congressional district, owners, operators, highway-and-railway connections, commodities, type of construction, cargo-handling equipment, water depth alongside the facility, berthing space, and deck height. Data included is for all facility types (except mile points) that were available for use during the previous two years.

The **Master Docks Plus Public Extract** database is a Microsoft Access database that contains a complete extract of the Navigation Data Center's dock database with all data that may be released to the public.

The **Port Boundary** Data identifying port boundaries are extracted from Master Dock Plus and converted into a GIS layer called **Port Boundary**. This GIS layer is a kmz format shape file utilizing Google Earth Pro. The port boundary is represented by the geographic location of docks and other navigation points of interest. Each facility carries essential information like Longitude, Latitude, Port ID, Mile Point, Location Code, Dock Code, Waterway, Port Facility Type and Official Dock Name. Color coded icons are used to identify the facility locations for an individual port.

Comments or Questions Contact:
CEWR
USACE Home
7701 Telegraph Rd., Casey Bldg.
Alexandria, VA 22315
This document was last revised:
9/12/2011

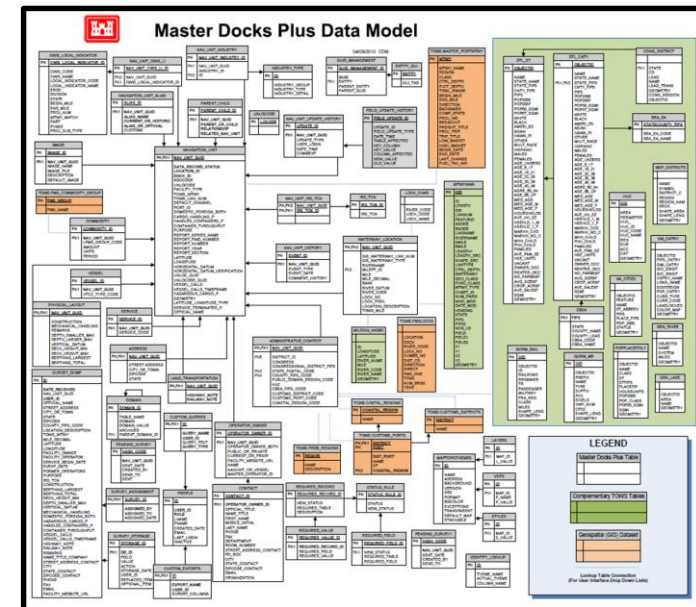
USACE Home
Div D I s t C t r L a b F O A
Civil Works



This PC > Downloads > mdplus_public_extract

Name	Type	Compressed size	Password protected
MasterDocksPlus_Data_Dictionary	Microsoft Excel Worksheet	37 KB	No
<input checked="" type="checkbox"/> MasterDocksPlus_Schema	Adobe Acrobat Document	59 KB	No
mdplus_public_extract	Microsoft Access Database	49,289 KB	No

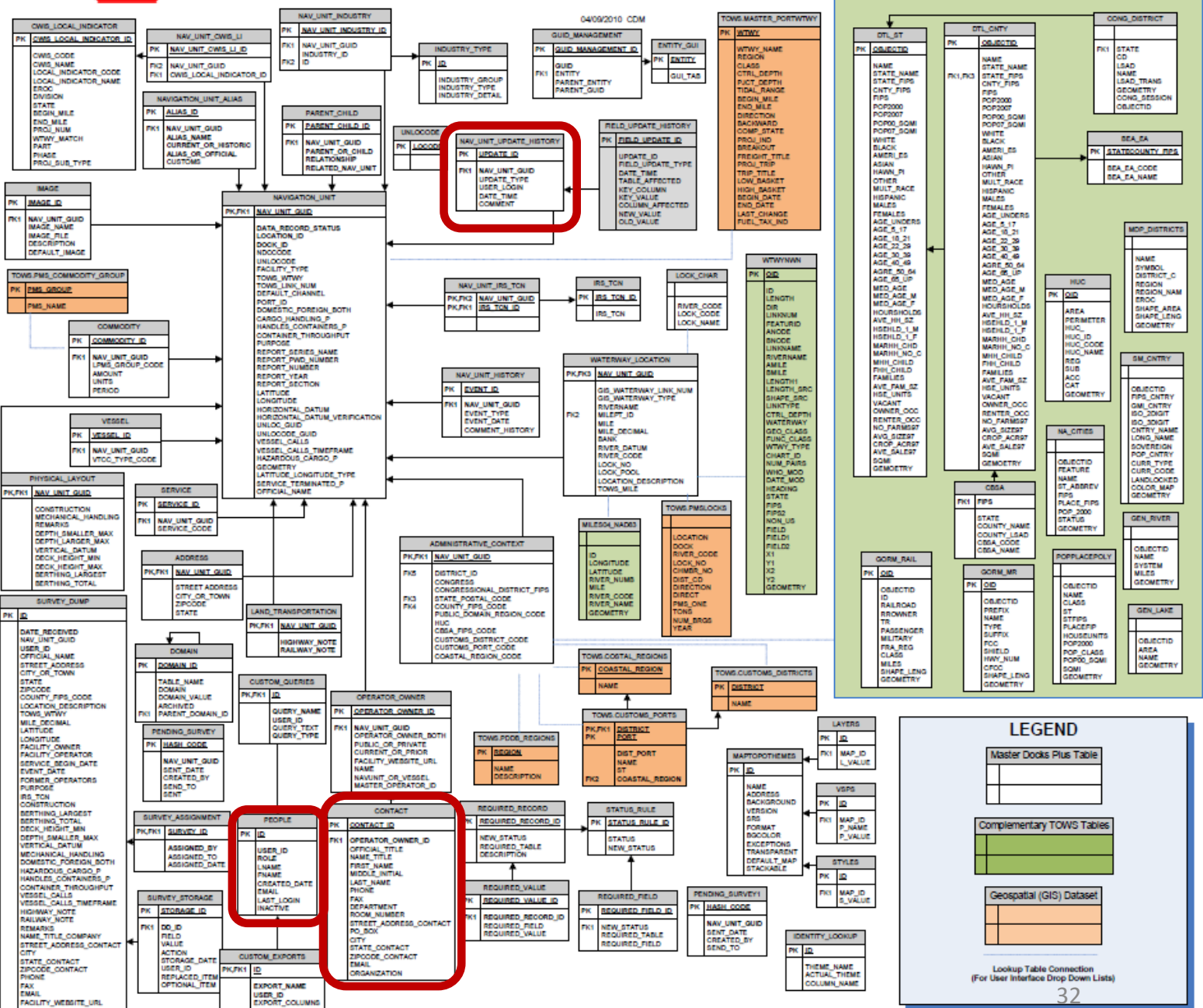
3 items | 1 item selected | 62.8 KB





Master Docks Plus Data Model

How to document where data subjects' personal information is stored and how it is used within a database ?



Legend

Personal information stored here



LEGEND

Master Docks Plus Table

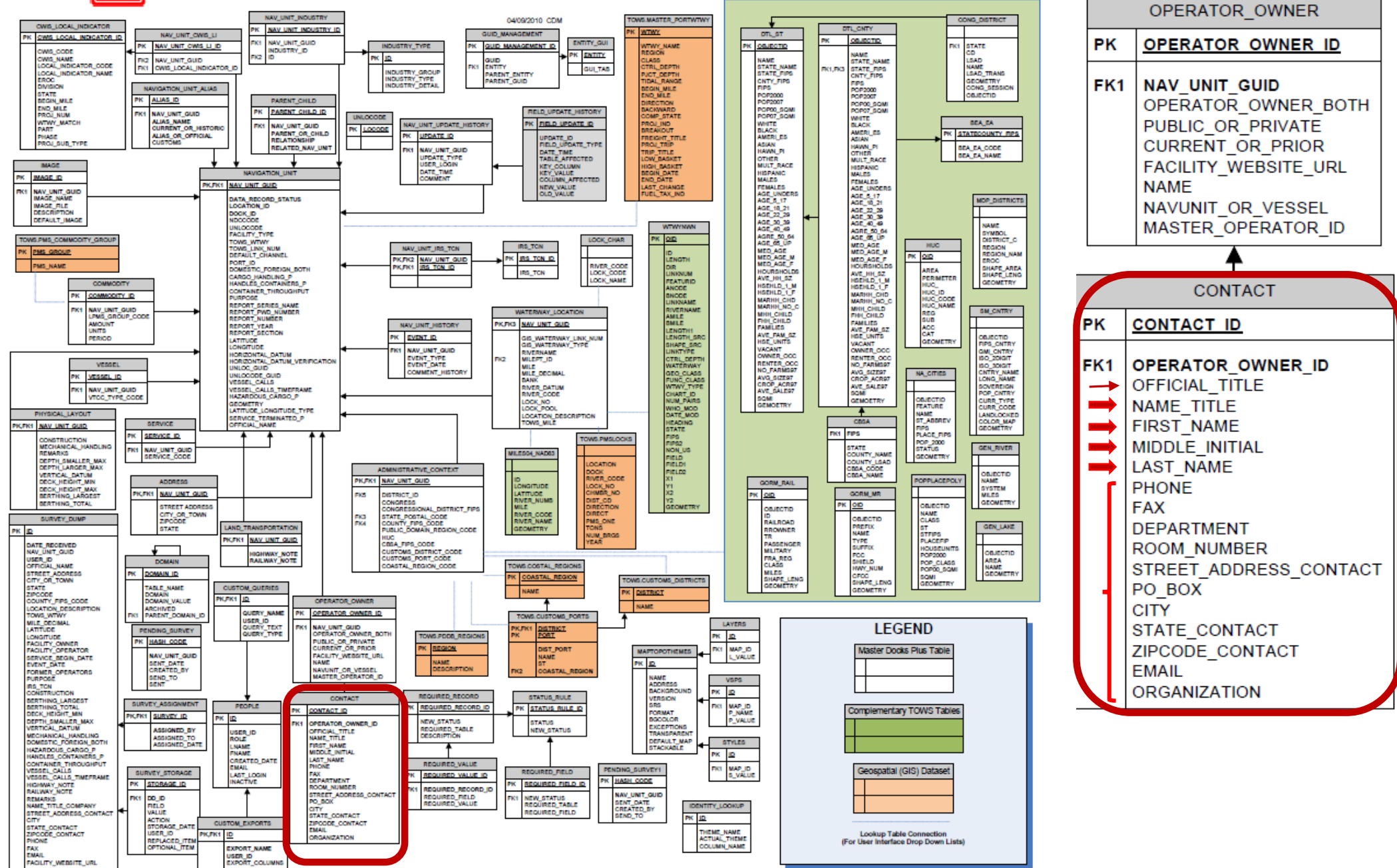
Complementary TOWS Tables

Geospatial (GIS) Dataset

Lookup Table Connection (For User Interface Drop Down Lists)



Master Docks Plus Data Model



How to document where data subjects' personal information is stored and how it is used within a database?

Personal data in Information System Database Data Dictionary

MasterDocksPlus_Data_Dictionary [Read-Only] - Excel

MD+ Field Name	MD+ Field Type	MD+ Field Size	Suggested Field Size	Primary Key	Foreign Key	Notes	Domain Values	Constraints	Filemaker Migration Field	TOWS Migration Field
Table Name: Contact										
Contact info for an owner or operator of a navigaton unit. Each owner or operator may have multiple contact records. This data was migrated from Filemaker										
Contact_ID	Number	38	12,0	Y		Unique identifier for contact records		Not Null	none	none
Operator_Owner_ID	Number	38	12,0		Y	Identifies the associated operator_owner record.	Operator_Owner_ID from mdpclient.operator_owner	Not Null	none	none
City	Character	100	100						city_mail	
Department	Character	150	150						department	
Email	Character	150	150						email_facility	
Fax	Character	50	50						fax	
First_Name	Character	50	50						first_name	
Last_Name	Character	60	60						last_name	
Middle_Initial	Character	30	1						mi	
Name_Title	Character	40	40						mr_or_mrs	
Official_Title	Character	100	100						title	
Phone	Character	50	50						phone	
PO_Box	Character	50	50						po_box_no	
Room_Number	Character	50	50						room_no	
State_Contact	Character	2	2				State_Abbr from mdpgis.mdp_states		state_for_mail	
Street_Address_Contact	Character	100	100						street_only	
Zipcode_Contact	Character	31	10						zip	
Organization	Character	150	150			The organization that this contact belongs to.			organization	

Personal data attributes can be classified based on disclosure potential:

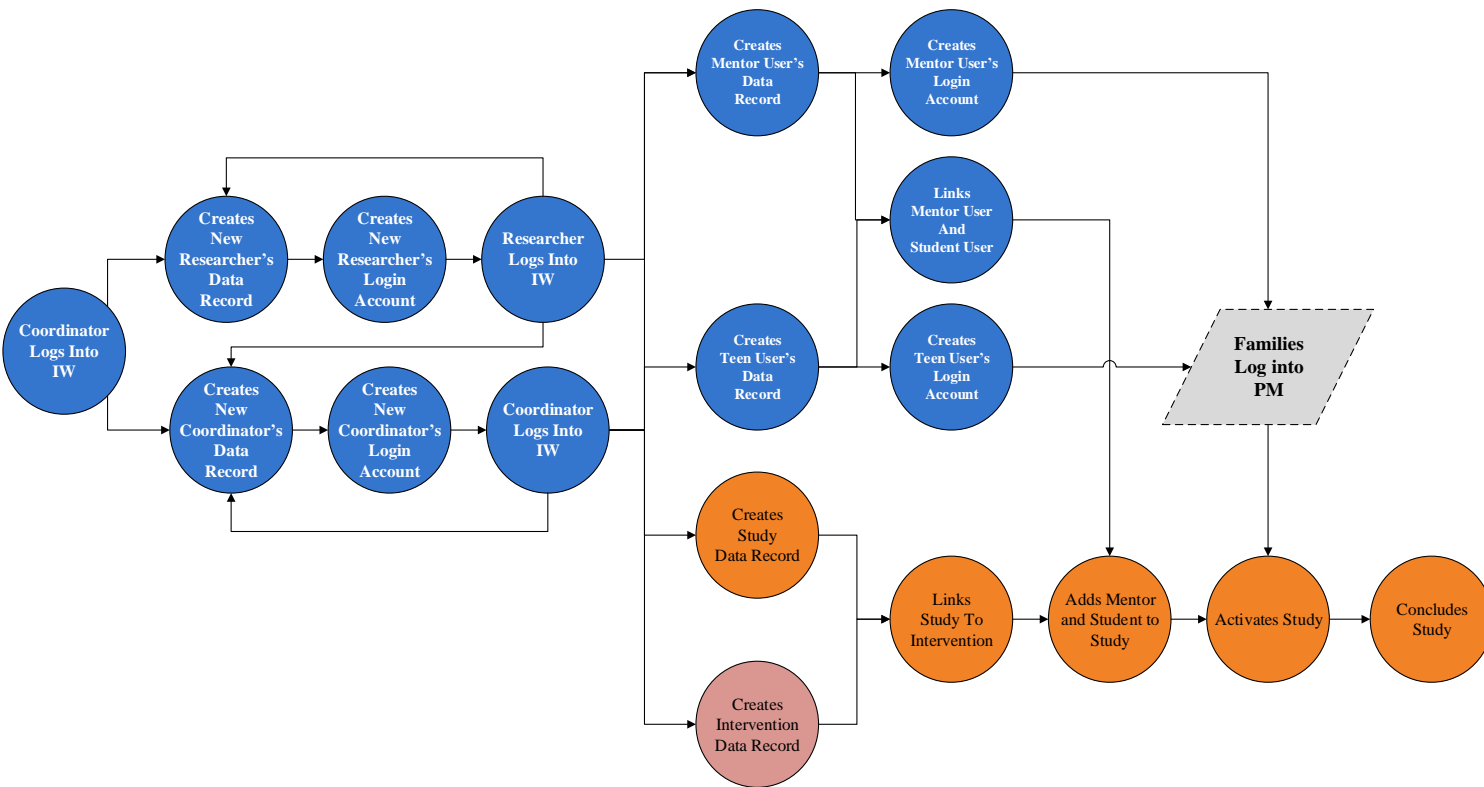
- **Identifiers.** Attributes that unambiguously identify the subject (e.g. passport no., social security no., name-surname, etc.)
- **Quasi-identifiers or key attributes.** They identify the subject with some ambiguity, but their combination may lead to unambiguous identification (e.g. address, gender, age, tele-phone no., etc.)
- **Confidential outcome attributes.** They contain sensitive subject information (e.g. salary, religion, diagnosis, etc.)
- **Non-confidential outcome attributes.** Other attributes which contain non-sensitive subject entity information

“Better” documentation identifies and classifies personal data in data dictionary

GDPR Concern	MD+ Field Name	MD+ Field Type	MD+ Field Size	Suggested Field Size	Primary Key	Foreign Key	Notes	Domain Values
	Table Name: Contact							
	Contact info for an owner or operator of a navigaton unit. Each owner or operator may have multiple contact records. This data was migrated from Filemaker							
Quasi-identifier	Contact_ID	Number	38	12,0	Y		Unique identifier for contact records	
Quasi-identifier	Operator_Owner_ID	Number	38	12,0		Y	Identifies the associated operator_owner record.	Operator_Owner_ID from mdpclient.operator_owner
Quasi-identifier	City	Character	100	100				
Quasi-identifier	Department	Character	150	150				
Identifier	Email	Character	150	150				
Quasi-identifier	Fax	Character	50	50				
Identifier	First_Name	Character	50	50				
Identifier	Last_Name	Character	60	60				
Identifier	Middle_Initial	Character	30	1				
Quasi-identifier	Name_Title	Character	40	40				
Quasi-identifier	Official_Title	Character	100	100				
Quasi-identifier	Phone	Character	50	50				
Quasi-identifier	PO_Box	Character	50	50				
Quasi-identifier	Room_Number	Character	50	50				
Quasi-identifier	State_Contact	Character	2	2				State_Abbr from mdpgis.mdp_states
Quasi-identifier	Street_Address_Contact	Character	100	100				
Quasi-identifier	Zipcode_Contact	Character	31	10				
Quasi-identifier	Organization	Character	150	150			The organization that this contact belongs to.	

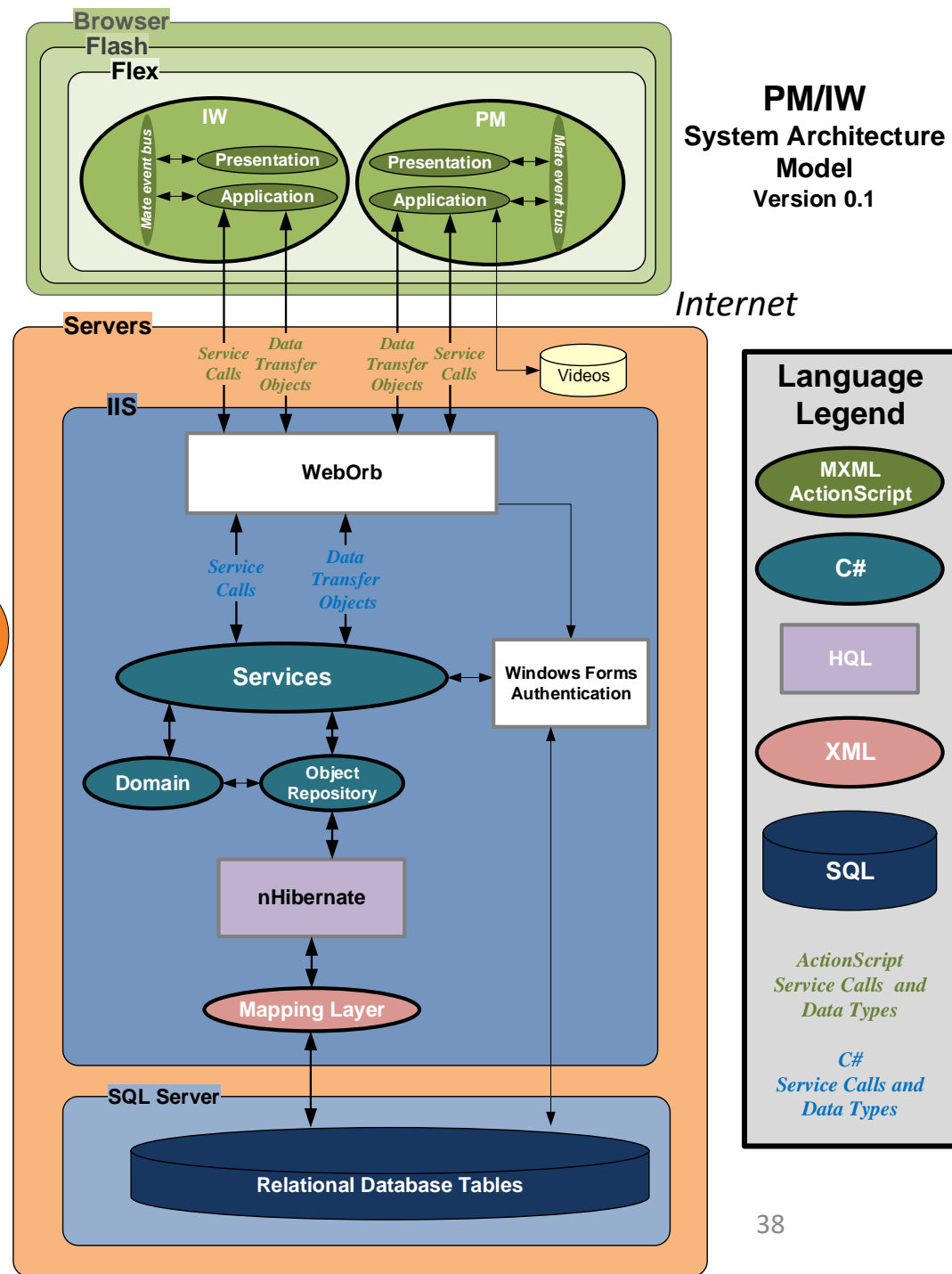
Is information available for meeting the following privacy by design requirements:

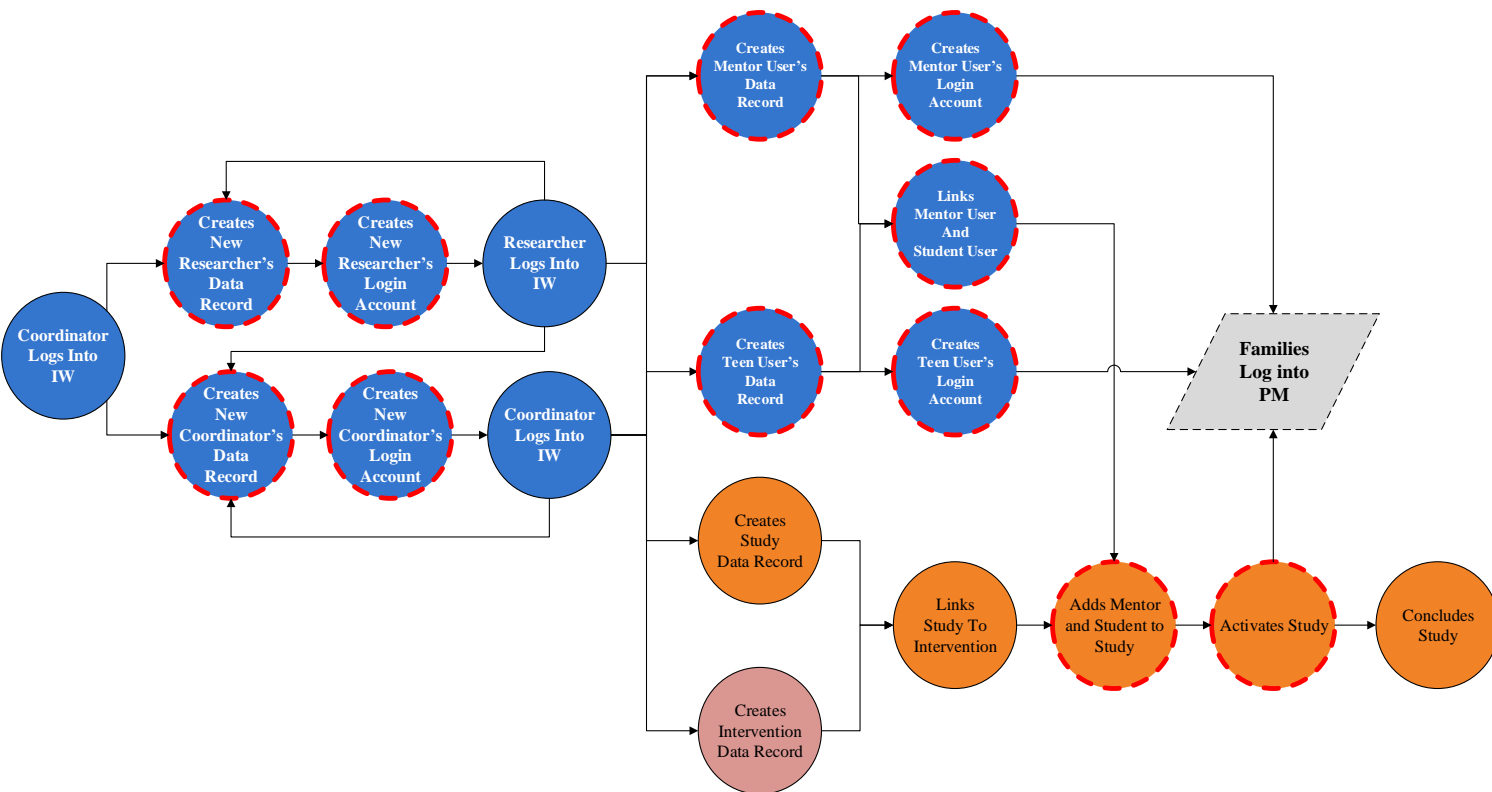
1. Is the collection of personal data fully avoided or minimized at the earliest stage of processing ?
2. Are data subjects able to give specific, informed and explicit consent to the processing of their data ?
 - Is legitimate processing specified and made explicit to the data subject before collecting personal data ?
 - Can data subjects understand possible risks induced by the processing ?
 - Can data subjects control the processing? And if so, can they understand actions they can take to control the processing ?
- 3. Can data subjects access, review and rectify their personal data?**
- 4. Are data subjects able to withdraw given consent with effect for the future by:**
 - a. Blocking access to their personal data?**
 - b. Constraining processing and usage of their personal data?**
 - c. Erasing their personal data?**
5. Are capabilities provided with which personal data obtained for one purpose are blocked and restricted from processing for other purposes not compatible with the original purpose?



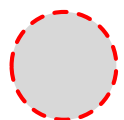
IW/PM Information System Workflow Model

Can you determine where personal data is processed in the information systems...

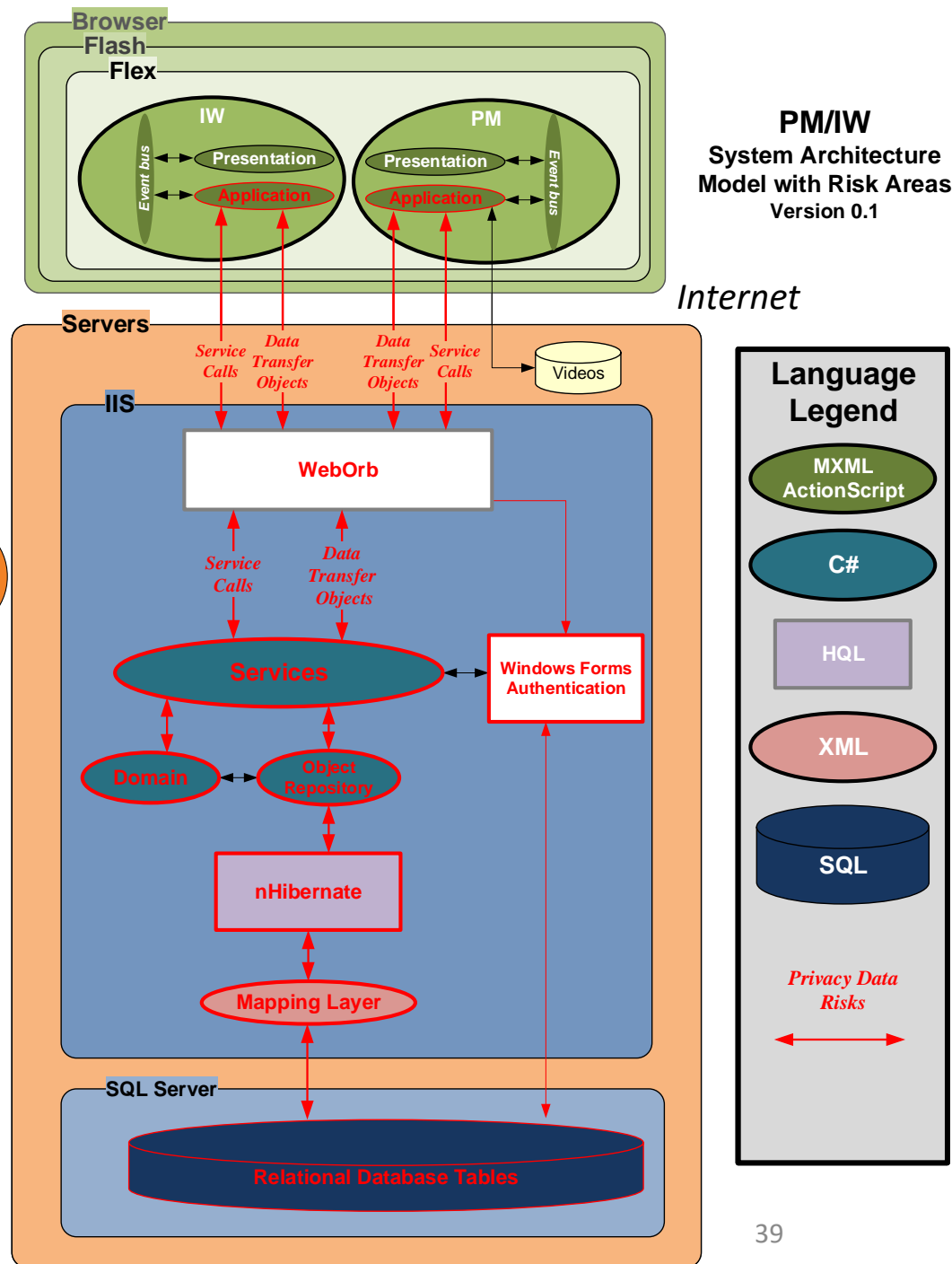




IW Information SubSystem Workflow Model



...now you can begin to identify where personal data is processed in the information system



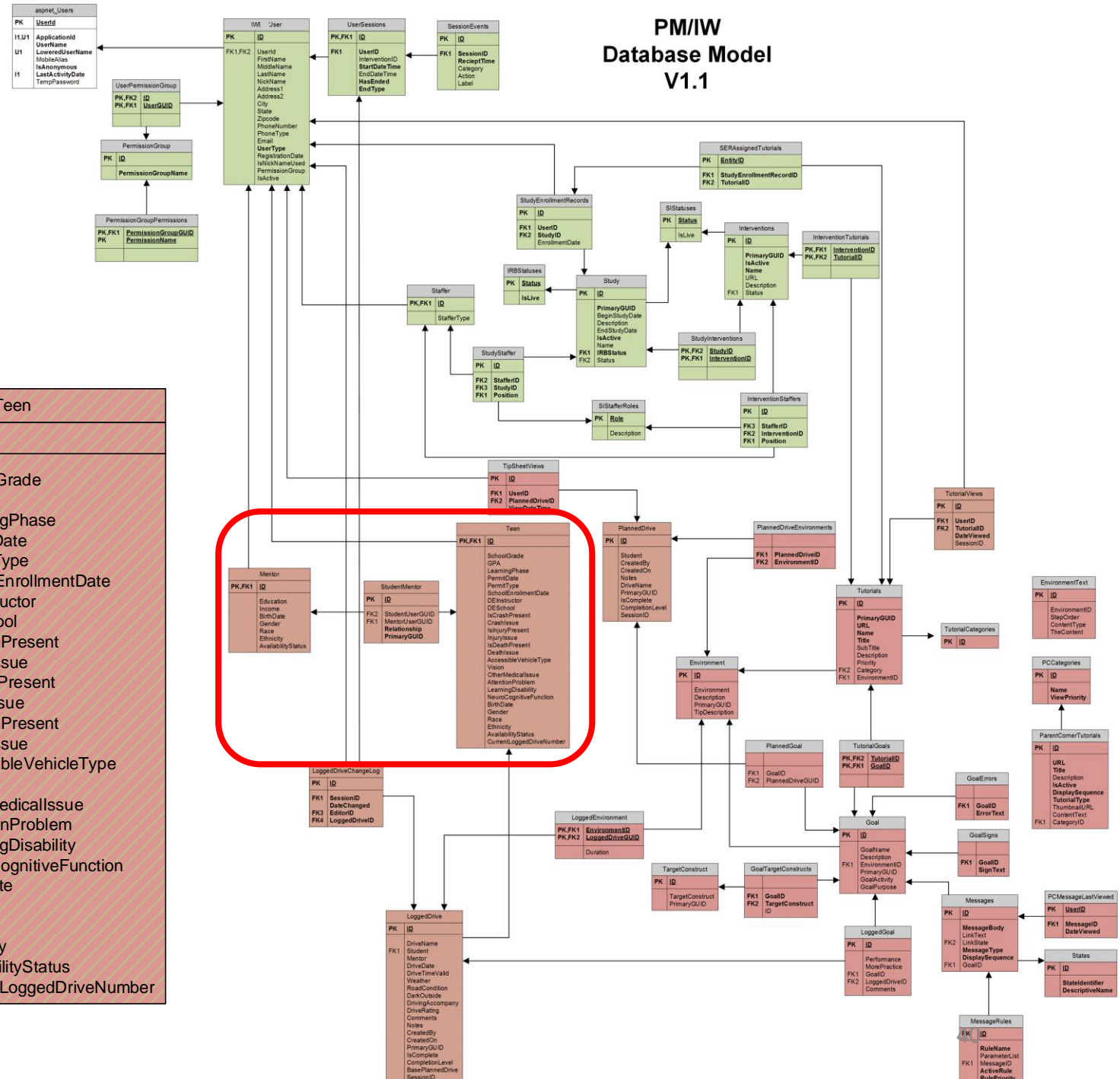
Is personal data identified in the database documentation?

Mentor	
PK,FK1	ID
Education	
Income	
BirthDate	
Gender	
Race	
Ethnicity	
AvailabilityStatus	

StudentMentor	
PK	ID
StudentUserGUID	FK2
MentorUserGUID	FK1
Relationship	
PrimaryGUID	

Teen	
PK,FK1	ID
SchoolGrade	
GPA	
LearningPhase	
PermitDate	
PermitType	
SchoolEnrollmentDate	
DEInstructor	
DESchool	
IsCrashPresent	
CrashIssue	
IsInjuryPresent	
InjuryIssue	
IsDeathPresent	
DeathIssue	
AccessibleVehicleType	
Vision	
OtherMedicalIssue	
AttentionProblem	
LearningDisability	
NeuroCognitiveFunction	
BirthDate	
Gender	
Race	
Ethnicity	
AvailabilityStatus	
CurrentLoggedDriveNumber	

PM/IW Database Model V1.1



Can you determine if data subjects' personal data is included in the data dictionary?

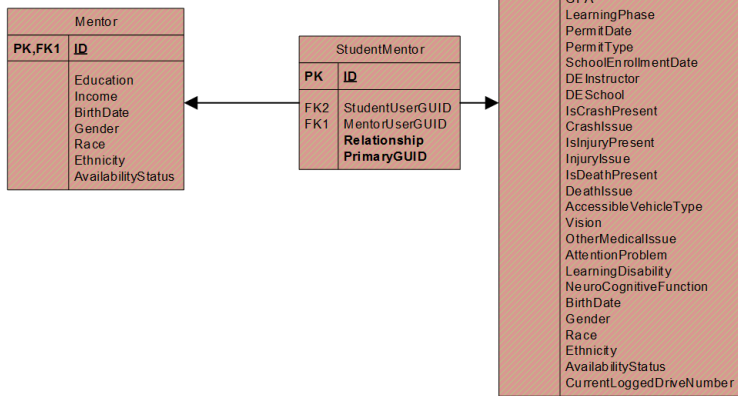
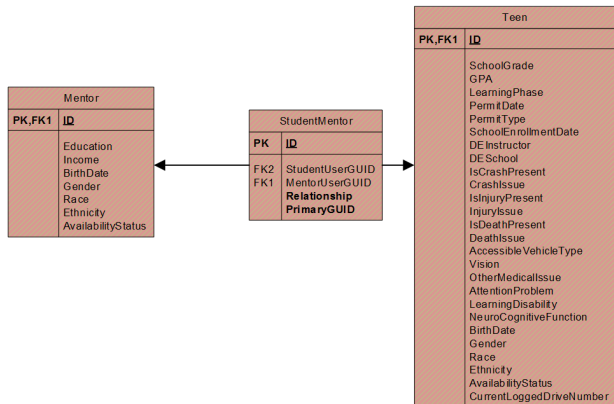


Table	Attribute	Primary Key	Foreign Key	Description
StudentMentor	StudentUserGUID		Yes	The student that is related to a mentor
StudentMentor	MentorUserGUID		Yes	The mentor that is related to a student
StudentMentor	Relationship			A description of the relationship of the mentor to the student
StudentMentor	ID	Yes		The ID of the relationship between the student and the mentor
StudentMentor	PrimaryGUID			A global unique identifier for the relationship
Mentor	ID	Yes	Yes	The ID of the mentor (and FK to USER)
Mentor	Education			The mentor's level of education
Mentor	Income			The mentor's level of income
Mentor	BirthDate			The birthdate of the mentor
Mentor	Gender			The mentor's gender
Mentor	Race			The mentor's race
Mentor	Ethnicity			The ethnicity of the mentor
Teen	ID	Yes	Yes	The ID of the teen/student - also the FK into the users table
Teen	SchoolGrade			The numeric school grade level at the time of enrollment
Teen	GPA			The decimal GPA of the teen at the time of enrollment
Teen	LearningPhase			Not implemented
Teen	PermitDate			The date that the teen's driving permit was issued
Teen	PermitType			The type of driving permit the teen has
Teen	SchoolEnrollmentDate			The date that the teen enrolled in driving school
Teen	DEInstructor			The teen's driving education instructor
Teen	DESchool			The name of the teen's driving school
Teen	IsCrashPresent			Indicates if the teen has a crash issue
Teen	CrashIssue			The nature of the crash issue
Teen	IsInjuryPresent			Indicates if an injury issue is present
Teen	InjuryIssue			The nature of the injury issue
Teen	IsDeathPresent			Indicates if a death issue is present
Teen	DeathIssue			The nature of the death issue
Teen	AccessibleVehicleType			Teens access to a vehicle
Teen	Vision			The nature of any vision related issues
Teen	OtherMedicalIssue			The nature of any unclassified medical issues
Teen	AttentionProblem			Description of any attention deficit related issues
Teen	LearningDisability			Description of any learning disabilities
Teen	NeuroCognitiveFunction			Description of any neurocognitive function issues
Teen	BirthDate			The teen's birthdate
Teen	Gender			The teen's physical gender
Teen	Race			The race the teen most closely fits
Teen	Ethnicity			Indicates the teen's ethnicity - hispanic or not
Teen	CurrentLoggedDriveNumber			The number of logged drives associated with this teen as the driver

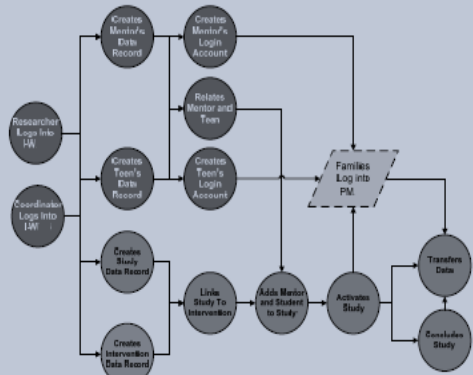
An improvement in identifying personal data and their classification in the data dictionary



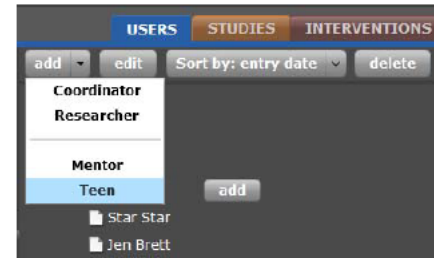
GDPR Concern	Table	Attribute	Primary Key	Foreign Key	Description
Quasi-identifier	StudentMentor	StudentUserGUID		Yes	The student that is related to a mentor
Quasi-identifier	StudentMentor	MentorUserGUID		Yes	The mentor that is related to a student
Confidential	StudentMentor	Relationship			A description of the relationship of the mentor to the student
Quasi-identifier	StudentMentor	ID	Yes		The ID of the relationship between the student and the mentor
Quasi-identifier	StudentMentor	PrimaryGUID			A global unique identifier for the relationship
Quasi-identifier	Mentor	ID	Yes	Yes	The ID of the mentor (and FK to USER)
Confidential	Mentor	Education			The mentor's level of education
Confidential	Mentor	Income			The mentor's level of income
Confidential	Mentor	BirthDate			The birthdate of the mentor
Confidential	Mentor	Gender			The mentor's gender
Confidential	Mentor	Race			The mentor's race
Confidential	Mentor	Ethnicity			The ethnicity of the mentor
Quasi-identifier	Teen	ID	Yes	Yes	The ID of the teen/student - also the FK into the users table
Confidential	Teen	SchoolGrade			The numeric school grade level at the time of enrollment
Confidential	Teen	GPA			The decimal GPA of the teen at the time of enrollment
Non-confidential	Teen	LearningPhase			Not implemented
Quasi-identifier	Teen	PermitDate			The date that the teen's driving permit was issued
Non-confidential	Teen	PermitType			The type of driving permit the teen has
Quasi-identifier	Teen	SchoolEnrollmentDate			The date that the teen enrolled in driving school
Confidential	Teen	DEInstructor			The teen's driving education instructor
Quasi-identifier	Teen	DESchool			The name of the teen's driving school
Confidential	Teen	IsCrashPresent			Indicates if the teen has a crash issue
Confidential	Teen	CrashIssue			The nature of the crash issue
Confidential	Teen	IsInjuryPresent			Indicates if an injury issue is present
Confidential	Teen	InjuryIssue			The nature of the injury issue
Confidential	Teen	IsDeathPresent			Indicates if a death issue is present
Confidential	Teen	DeathIssue			The nature of the death issue
Confidential	Teen	AccessibleVehicleType			Teens access to a vehicle
Confidential	Teen	Vision			The nature of any vision related issues
Confidential	Teen	OtherMedicalIssue			The nature of any unclassified medical issues
Confidential	Teen	AttentionProblem			Description of any attention deficit related issues
Confidential	Teen	LearningDisability			Description of any learning disabilities
Confidential	Teen	NeuroCognitiveFunction			Description of any neurocognitive function issues
Quasi-identifier	Teen	BirthDate			The teen's birthdate
Quasi-identifier	Teen	Gender			The teen's physical gender
Confidential	Teen	Race			The race the teen most closely fits
Confidential	Teen	Ethnicity			Indicates the teen's ethnicity - hispanic or not
Non-confidential	Teen	CurrentLoggedDriveNumber			The number of logged drives associated with this teen as the driver

Does the system's user guide(s) describe capabilities for controlling and protecting subjects' privacy data?

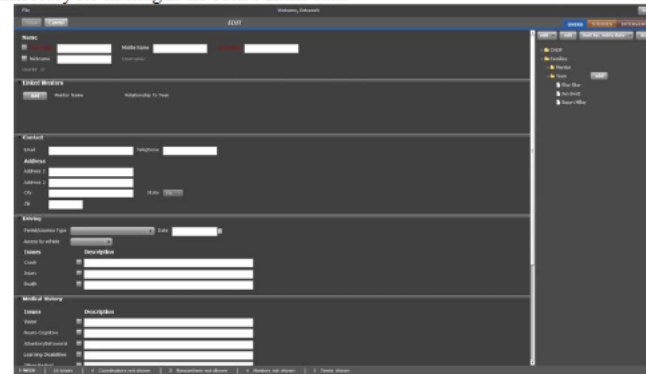
IW User Guide



IW User Guide



In response to the "add", IW presents the user with a form (displayed below) in the Left Panel ready for entering in the Teen's intake data.



The display of the scroll bar between the Left and Right panels indicates that there are more data entry fields below those currently displayed. Click the mouse on the scrollbar, hold down to scroll the Left Panel to reveal the additional fields, as illustrated below.

IW User Guide

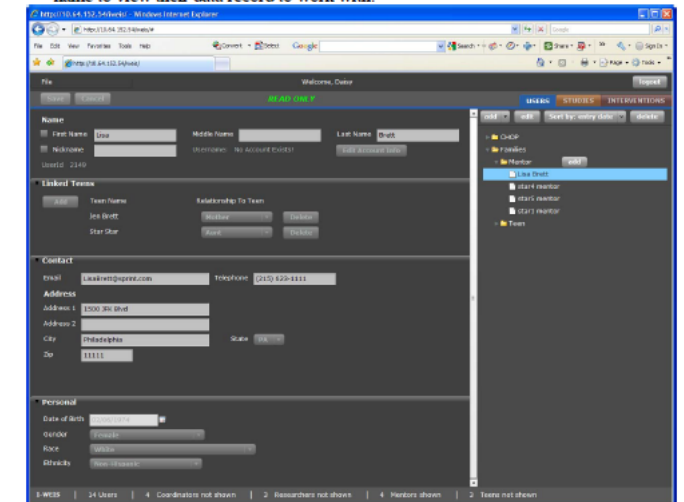
Clicking on the 'edit' button in the Users Tab Control Bar in the Right Panel, will put the form in edit mode for data entry and editing.

Step 5: Linking a Mentor to a Teen

In this section you will learn how to link a Mentor to their Teen, and update the Linked Teens section of the Mentor's user data. This will also automatically add the mentor to the Linked Mentors section of the Teen's user data.

Linking a Mentor and Teen's data records to one another will enable them, after they both are enrolled in a PM related research study, to both access, view, and work with their common PM plan, learn, and log data.

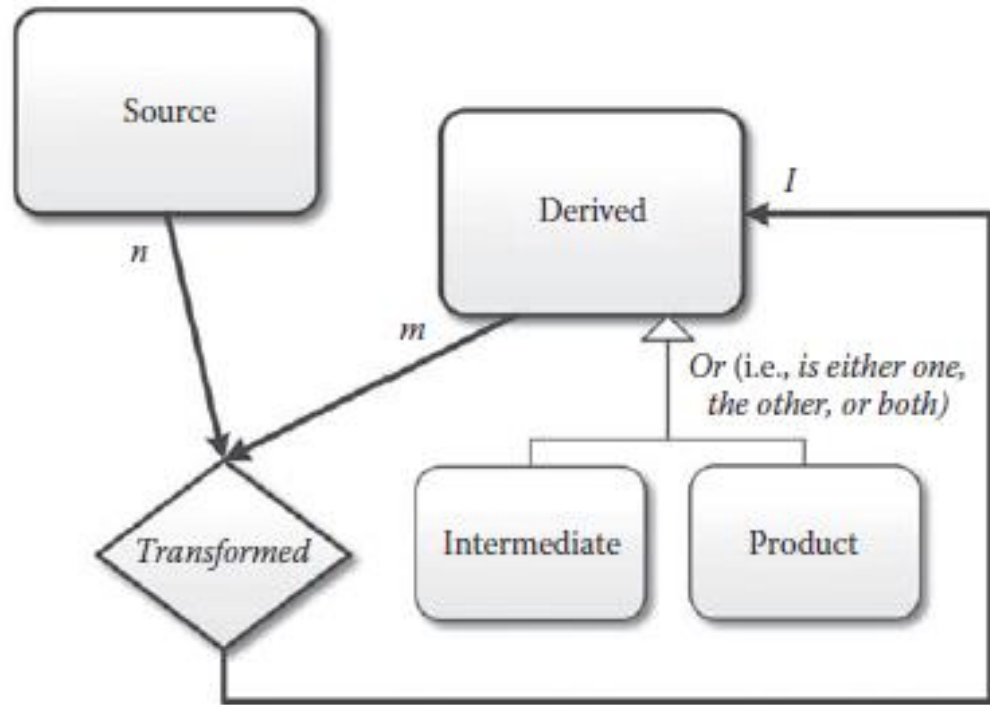
A. Using the tree menu, find the mentor (i.e. Lisa Brett in this example) and click on their name to view their data record to work with.



Data lineage metadata may hold the answer to meeting a number of challenging data privacy by design requirements

Data lineage (or 'data provenance') includes a description of the source material from which data were derived, and the methods of derivation, including all transformations involved in producing the final digital data records

A data lineage model provides concepts and vocabulary that help communicate how data is processed in an information system and aids thinking how to meet privacy by design requirements



Relationship among source and derived datasets, where each instance of the latter may be either an intermediate or product dataset, or both

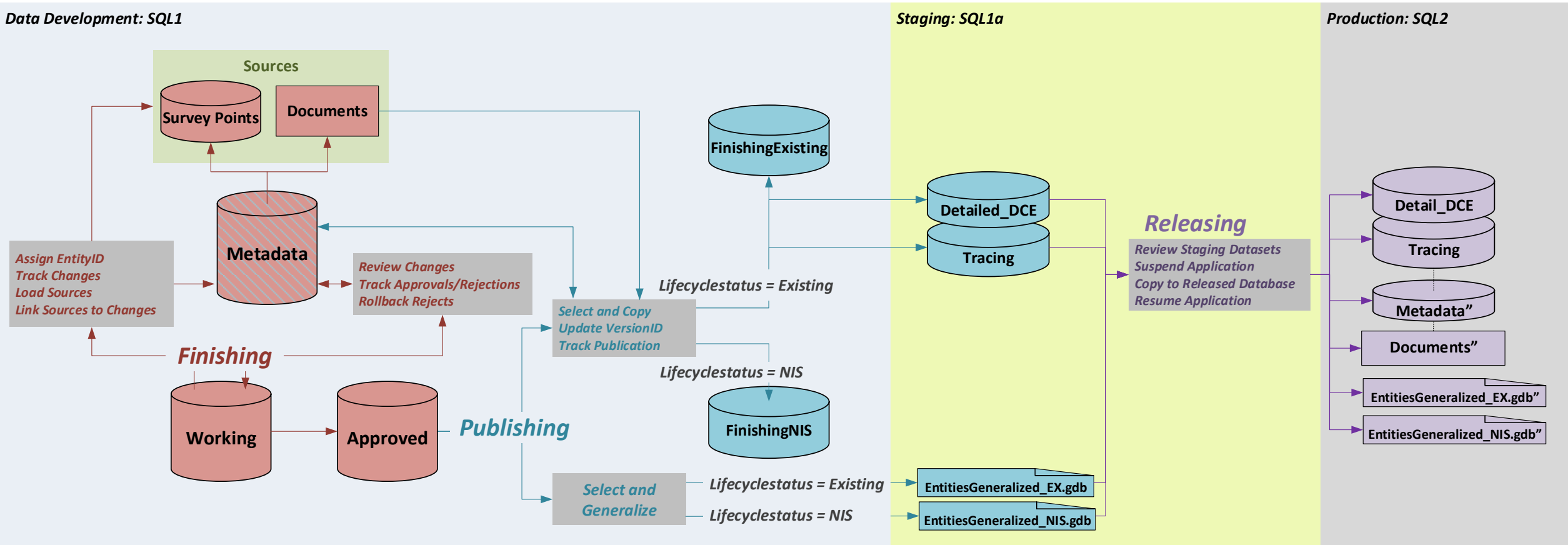
Source datasets containing personal data can be entered into a system in a number of ways

Initially, a data subject's personal data is only available in source datasets ($n \geq 1, m = 0$)

Subsequently, this data is copied or transformed to produce a new **“derived” dataset**

Later, new datasets can be generated exclusively from derived datasets ($n = 0, m \geq 1$) or can be derived from inputs that include sources, derived, or both ($n + m > 1$) using multi-input transformations such as relational database joins and relates or arithmetic, statistical, and logical transformations.

Example: Data update propagation documentation



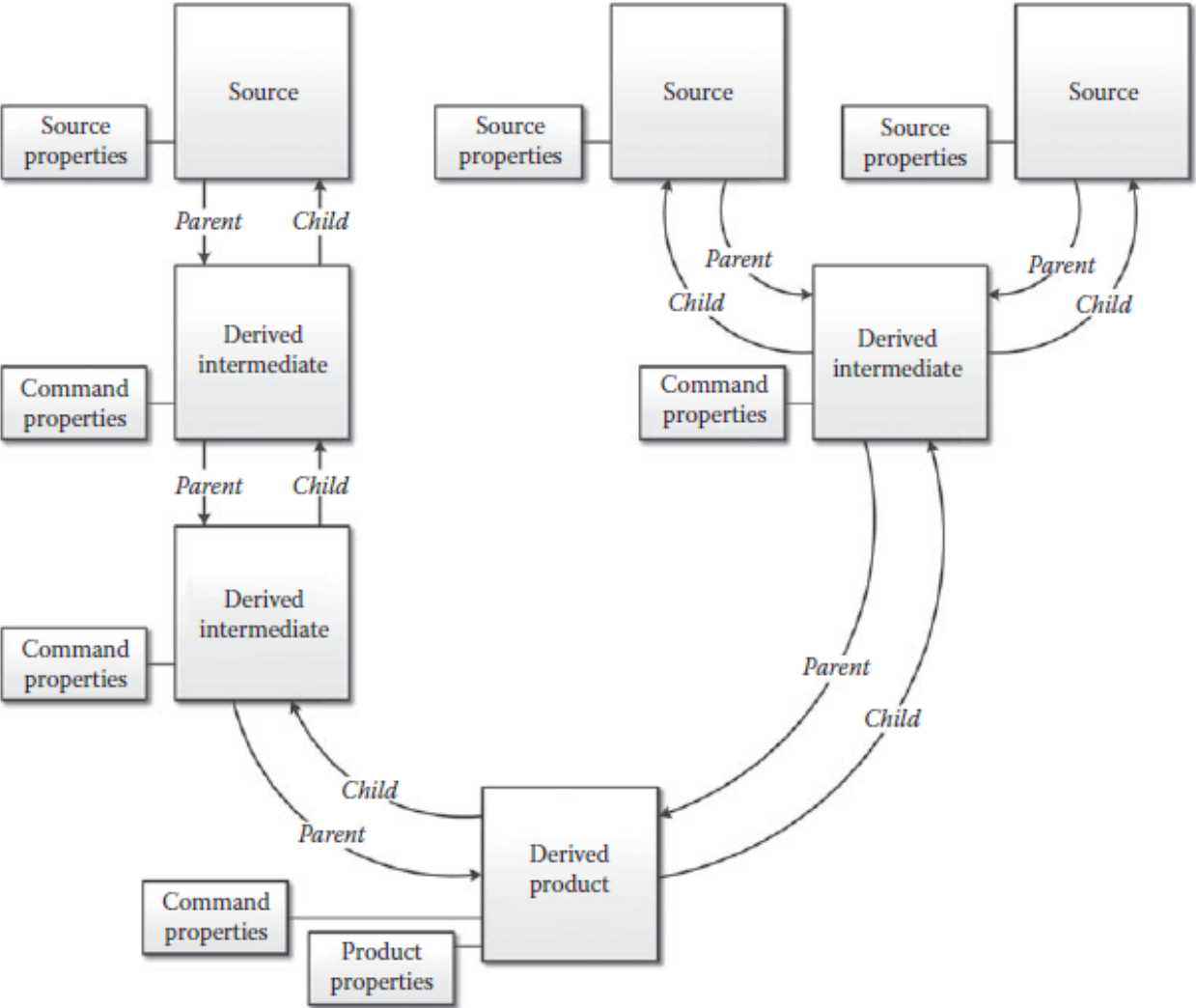
Datasets can be classified into **source, intermediate, and product types** and related as input and outputs of each data processing step of an application

Input datasets are given parent links pointing to output datasets they are used to create (Who am I the parent of?)

Output datasets are given child links connecting them back to their input datasets (Who am I the child of?)

Child links connect outputs to their inputs enable automatic deduction of which datasets within the database are sources and which are derived

Derived datasets are connected to their inputs by child links, sources lack such links.

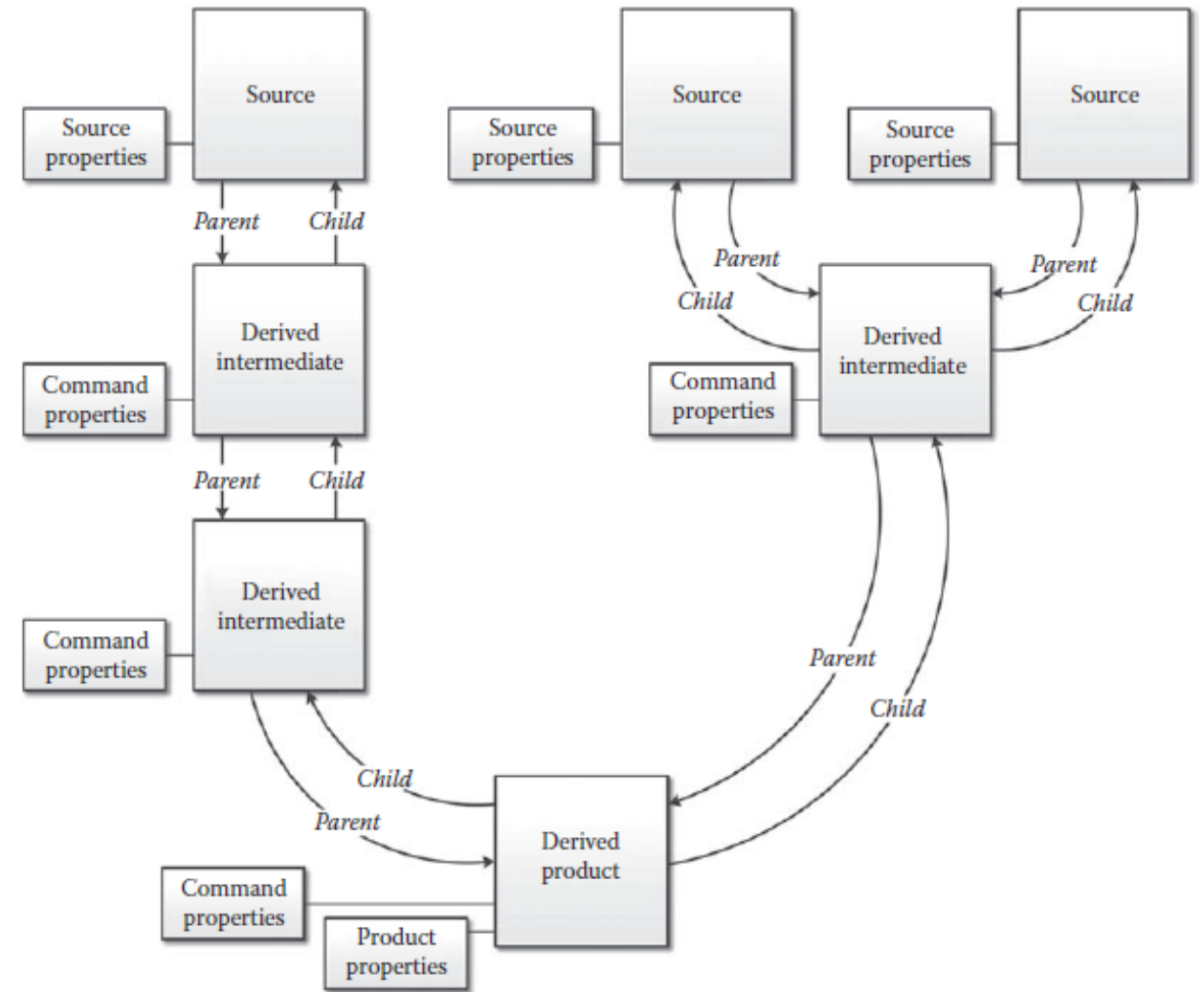


child operator takes a derived dataset, accesses its child links, and identifies the inputs used to create it.

ancestors algorithm applies the *child* operator and recursively traces child links to identify input datasets used to create a derived dataset, including sources used.

parent operator takes a source or derived dataset as input, accesses its parent links, and identifies all outputs directly derived from it.

descendants function recursively traces parent links and identifies all datasets derived from a source or other derived input dataset used within the application.

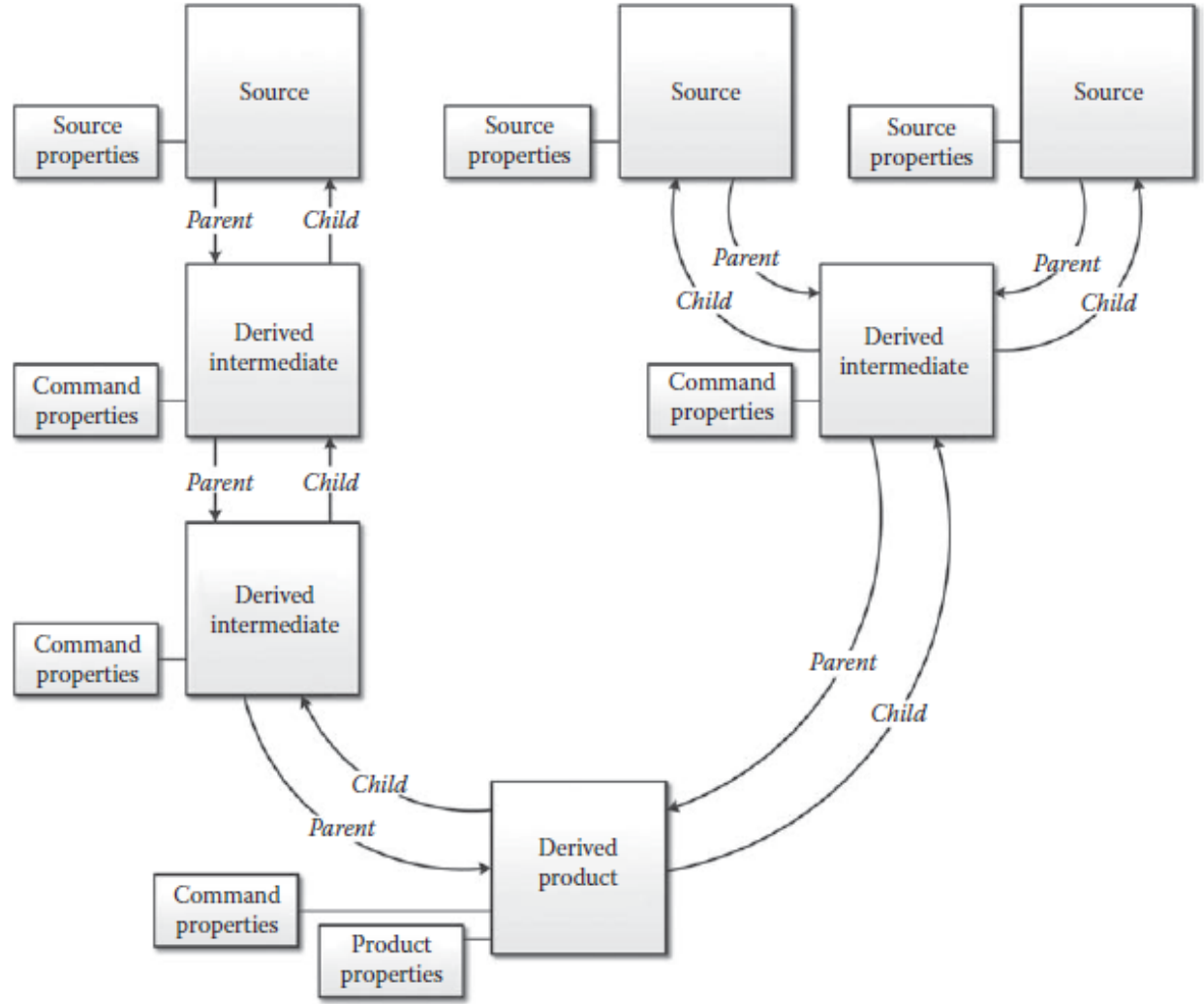


Classifying datasets into source, intermediate and product paves the way to storing additional lineage metadata attributes to document properties of source, intermediate and product dataset types.

source dataset is provided a “frame” data structure that organizes knowledge about the **origin, content, accuracy and sensitivity of the attributes**

derived dataset is provided a frame for storing detailed metadata elements about **where it is physically stored, the processing command** applied to the inputs to derive it, who derived it, and other aspects of the derivation

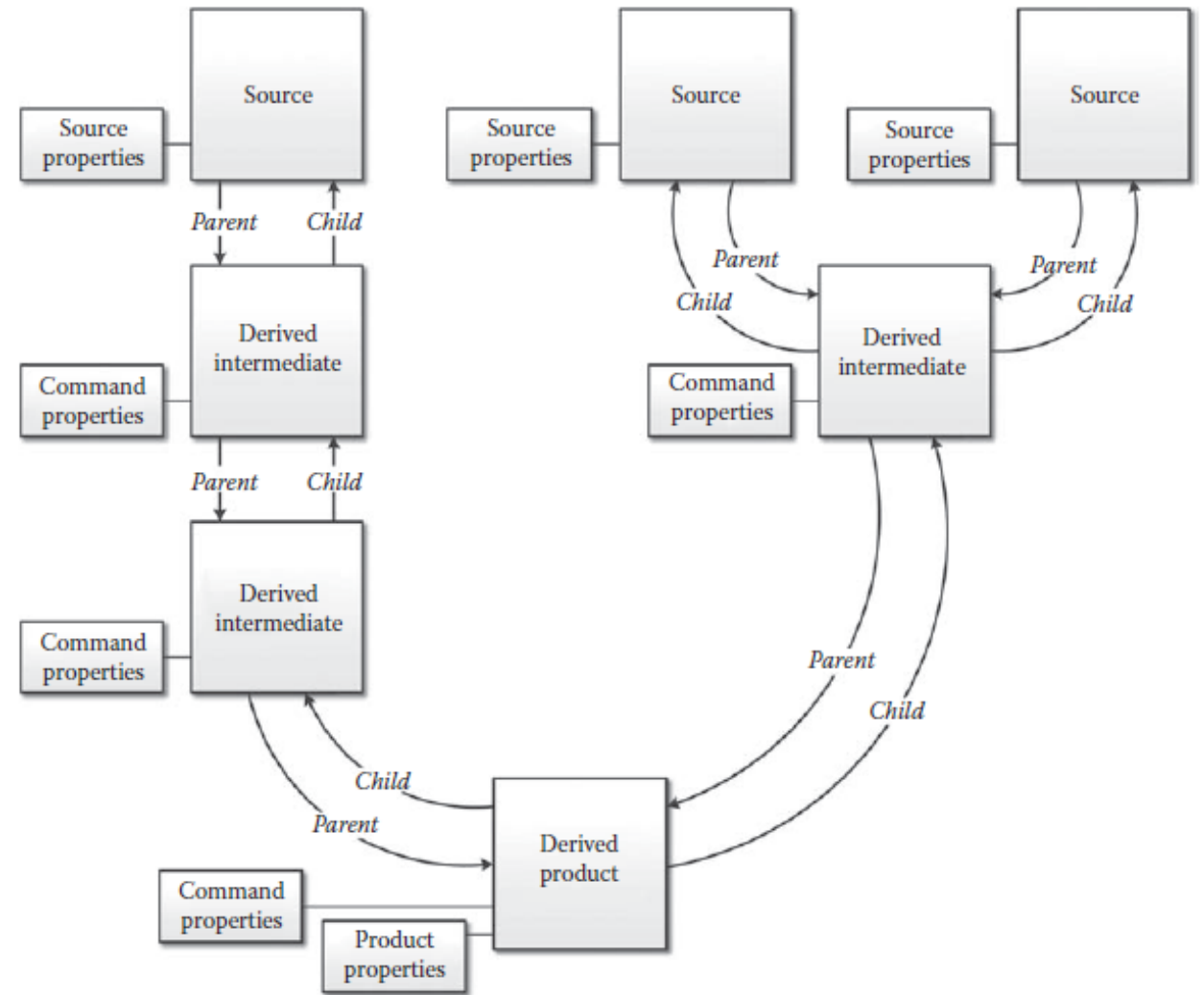
Products are derived datasets provided additional frame(s) for metadata detailing the **processing goal the dataset was intended to meet, intended users/audience of the dataset, when it was released, etc.**



Ancestors function was adapted to report metadata attributes of sources and intermediates to derive a target dataset

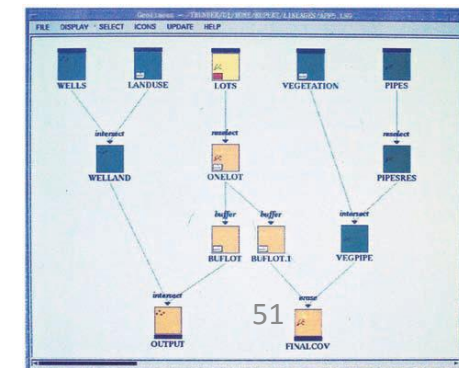
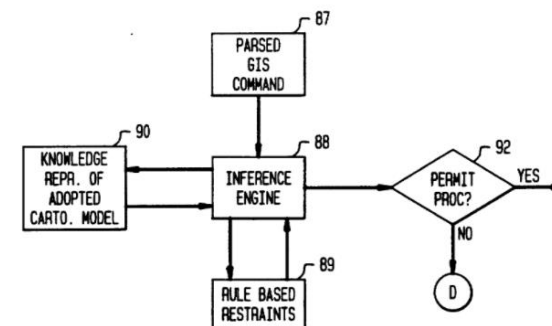
Ancestors function was integrated with a rule-based processor that checked inputs of each command, identified related sources, and evaluated their metadata to **detect, warn and block commands that would otherwise process restricted data or combine datasets of incompatible properties**

Descendants function was modified to automatically generate and run processing commands to **propagate edits** and new source materials **to update dependent intermediates and products**

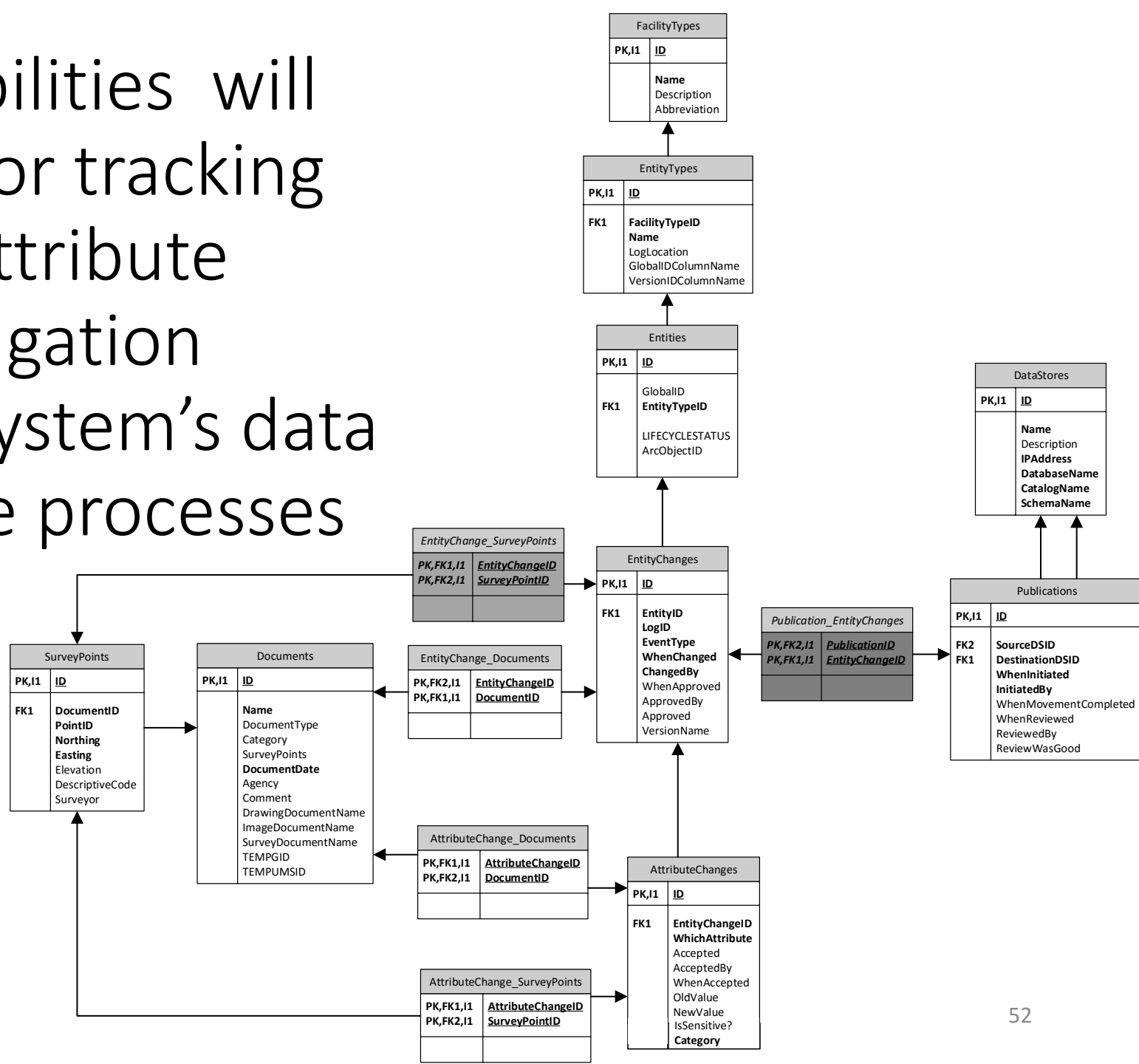


Data lineage metadata can be used to help information systems meet a number of key data privacy by design requirements, including:

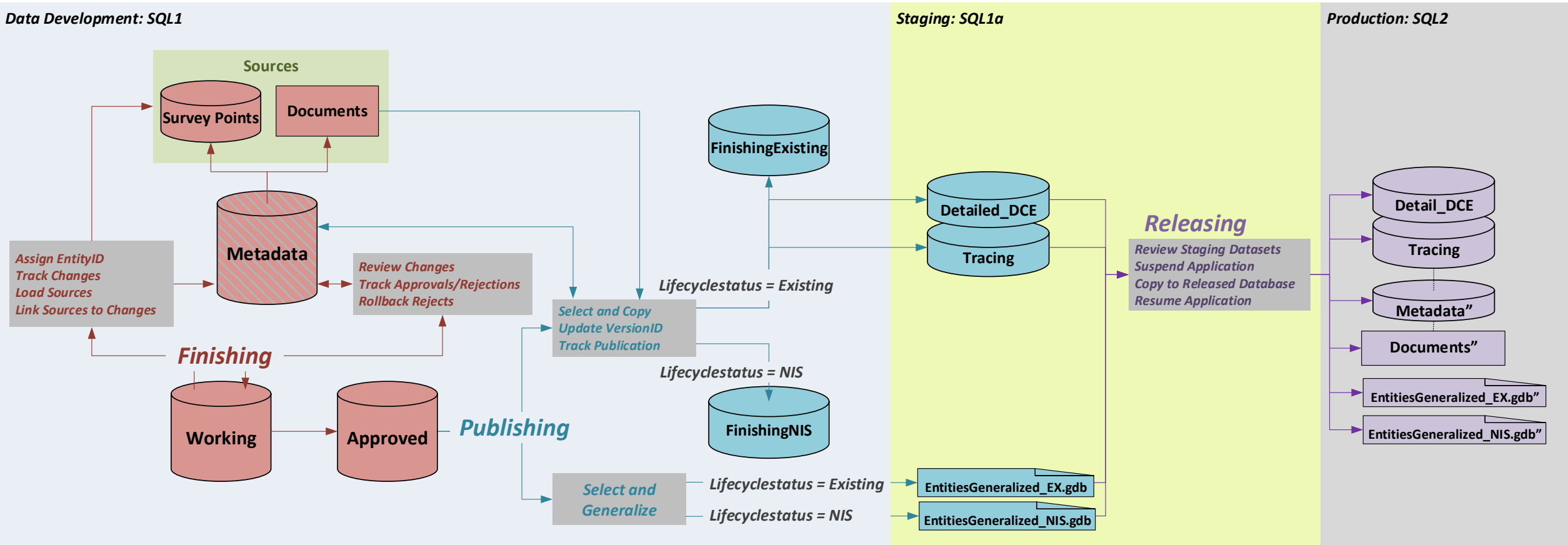
- Enabling data subjects access, review and rectify their personal data?
- Enable data subjects to withdraw given consent with effect for the future by:
 - a. Blocking access to their personal data?
 - b. Constraining processing and usage of their personal data?
 - c. Erasing their personal data?
- Blocking and restricting personal data obtained for one purpose from being processed for other purposes not compatible with the original purpose



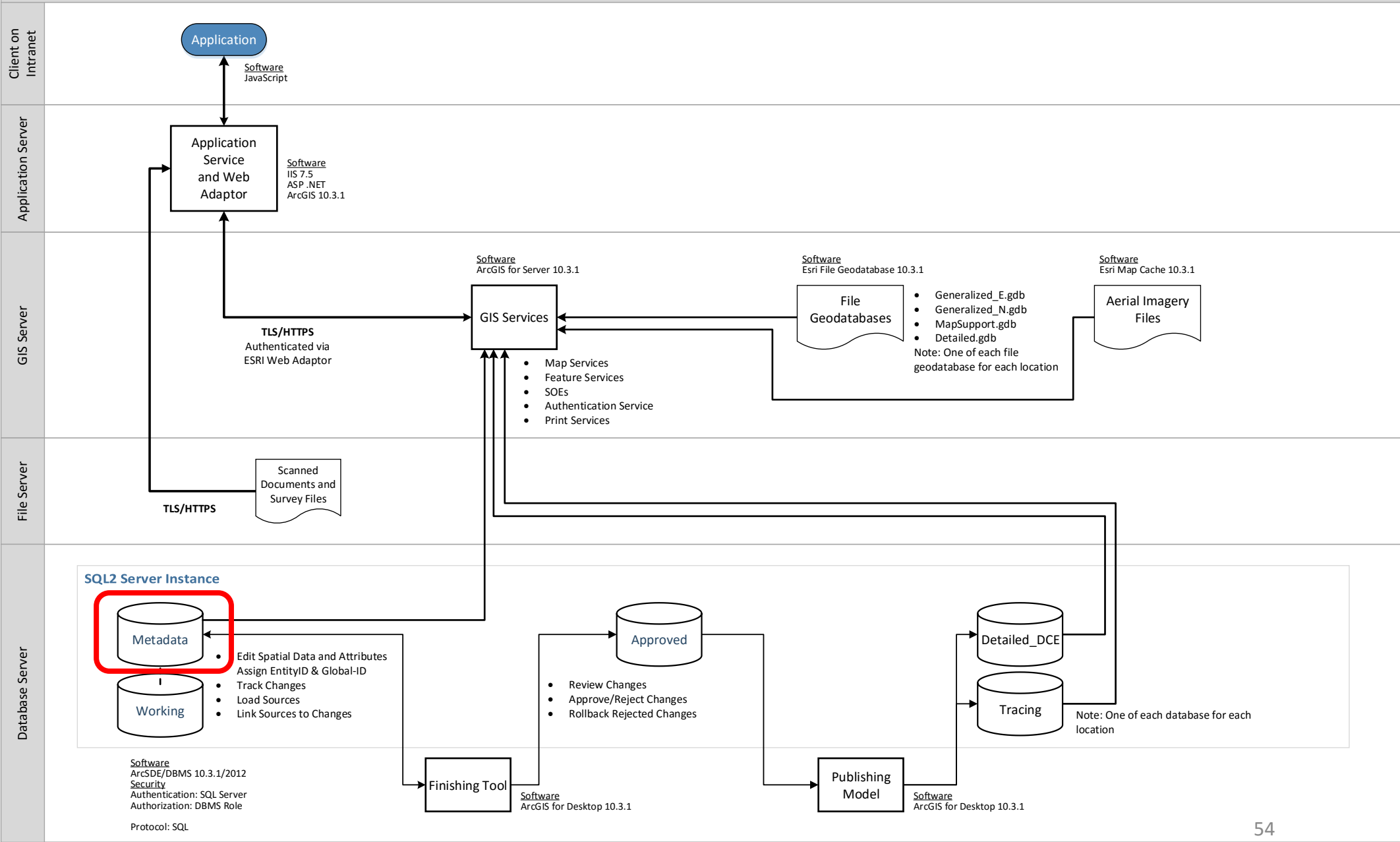
Other metadata capabilities will also provide support for tracking changes to sensitive attribute values and their propagation through information system's data store as part of update processes



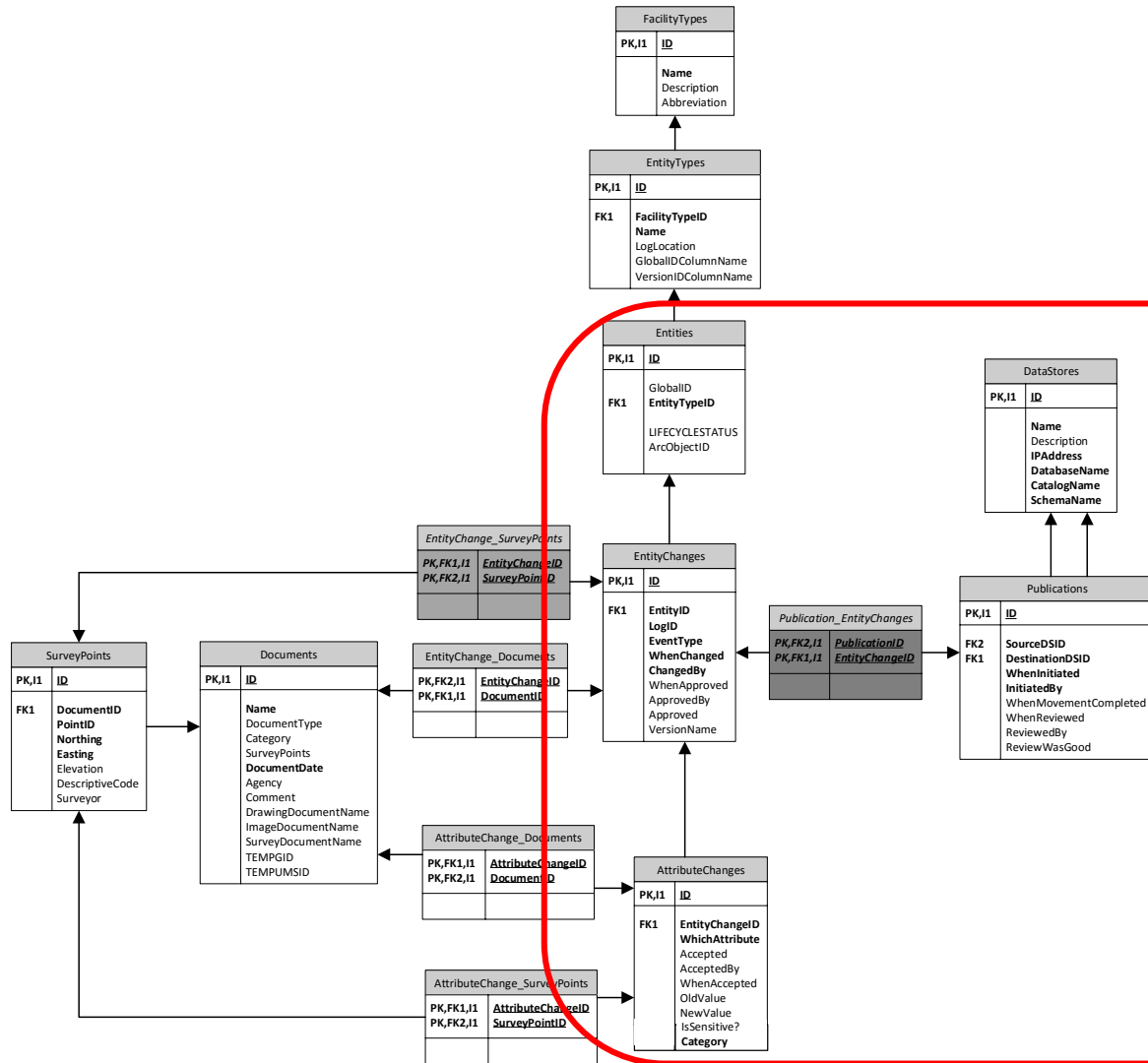
Example: Data update propagation documentation



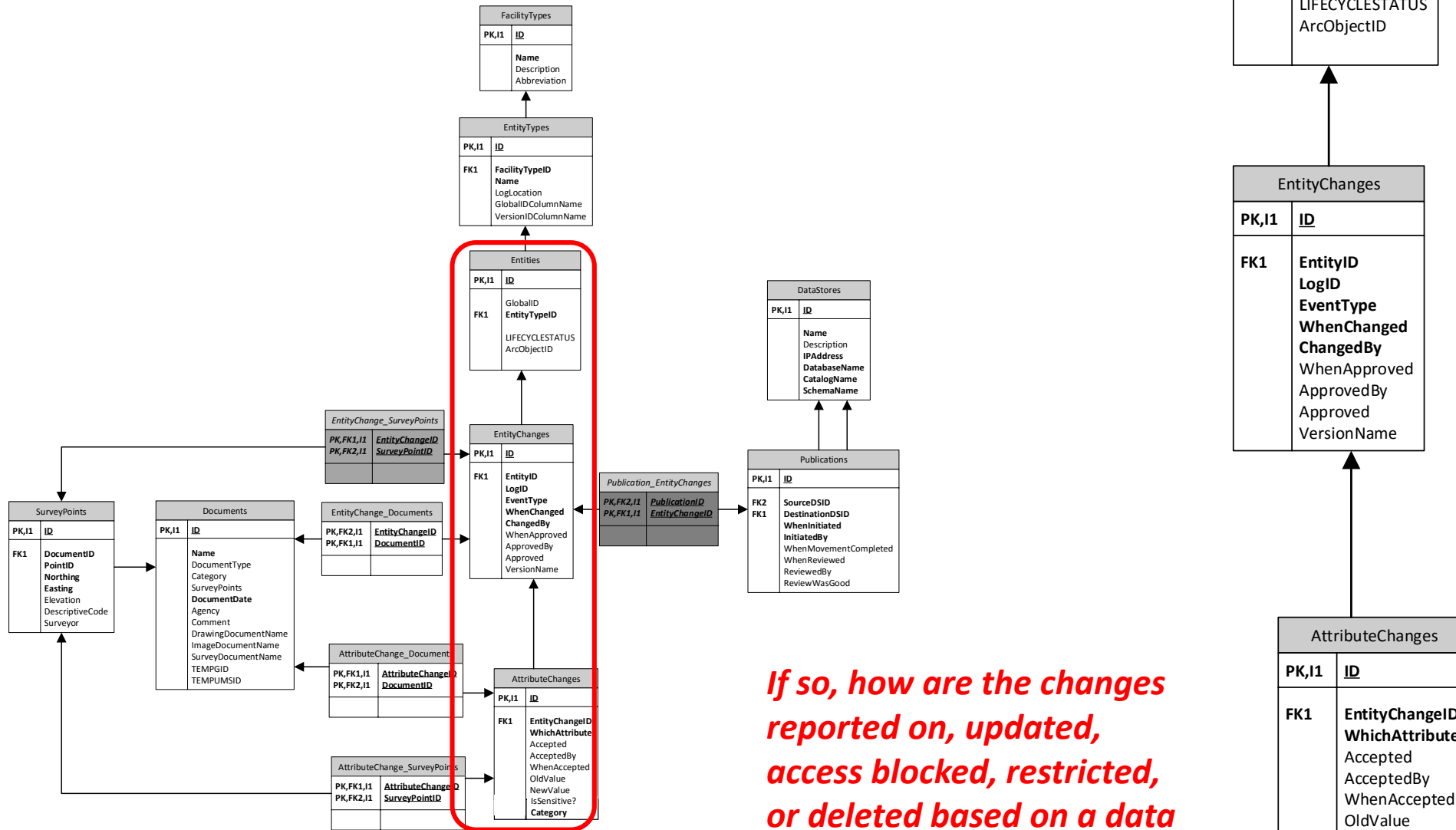
Production System Diagram



Possible metadata support for data privacy by design



Assessment questions



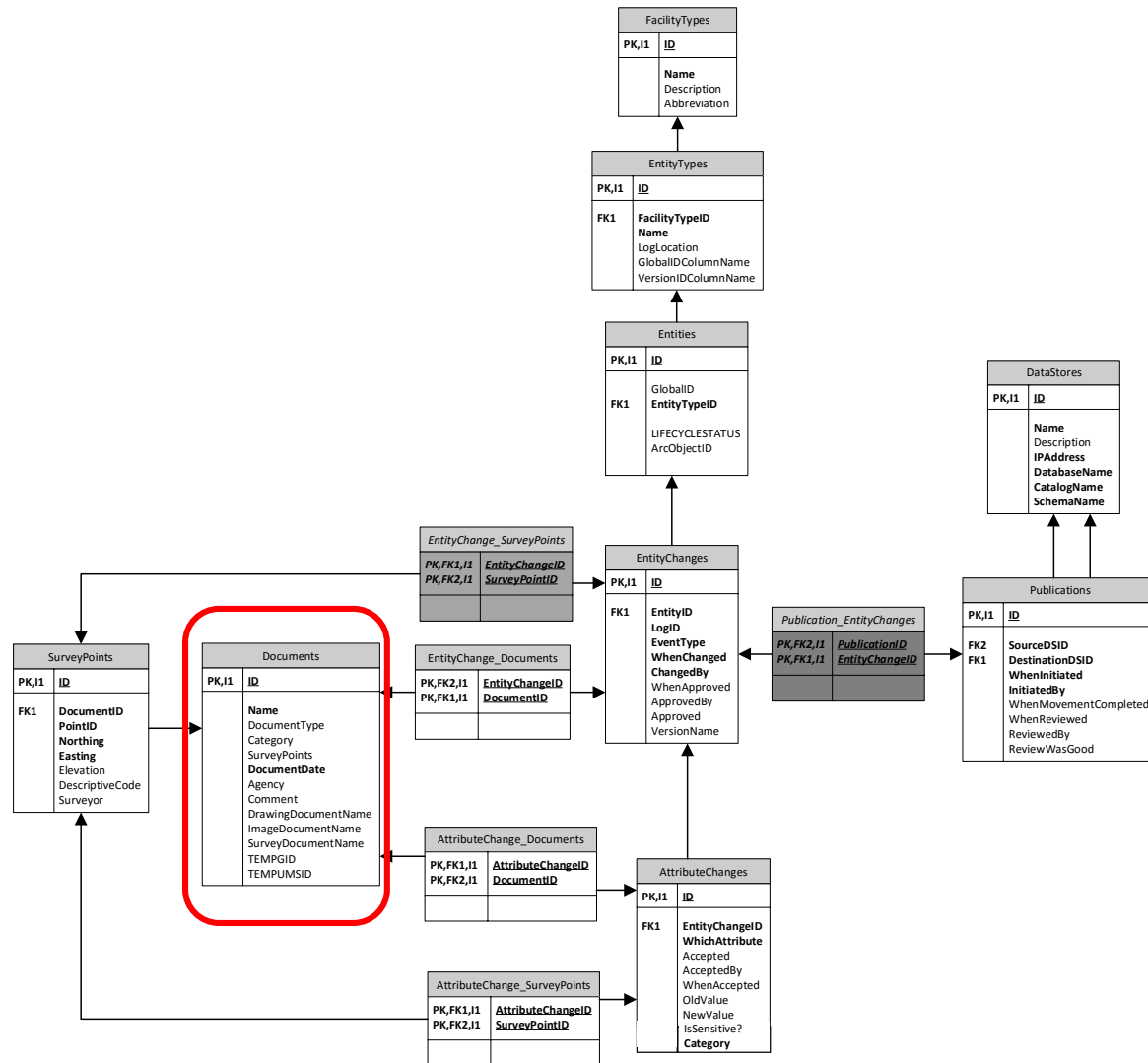
Which entities (if any) are data subject entities?

Do changes pertain to a data subject's personal data records?

If so, how are the changes reported on, updated, access blocked, restricted, or deleted based on a data subject's request?

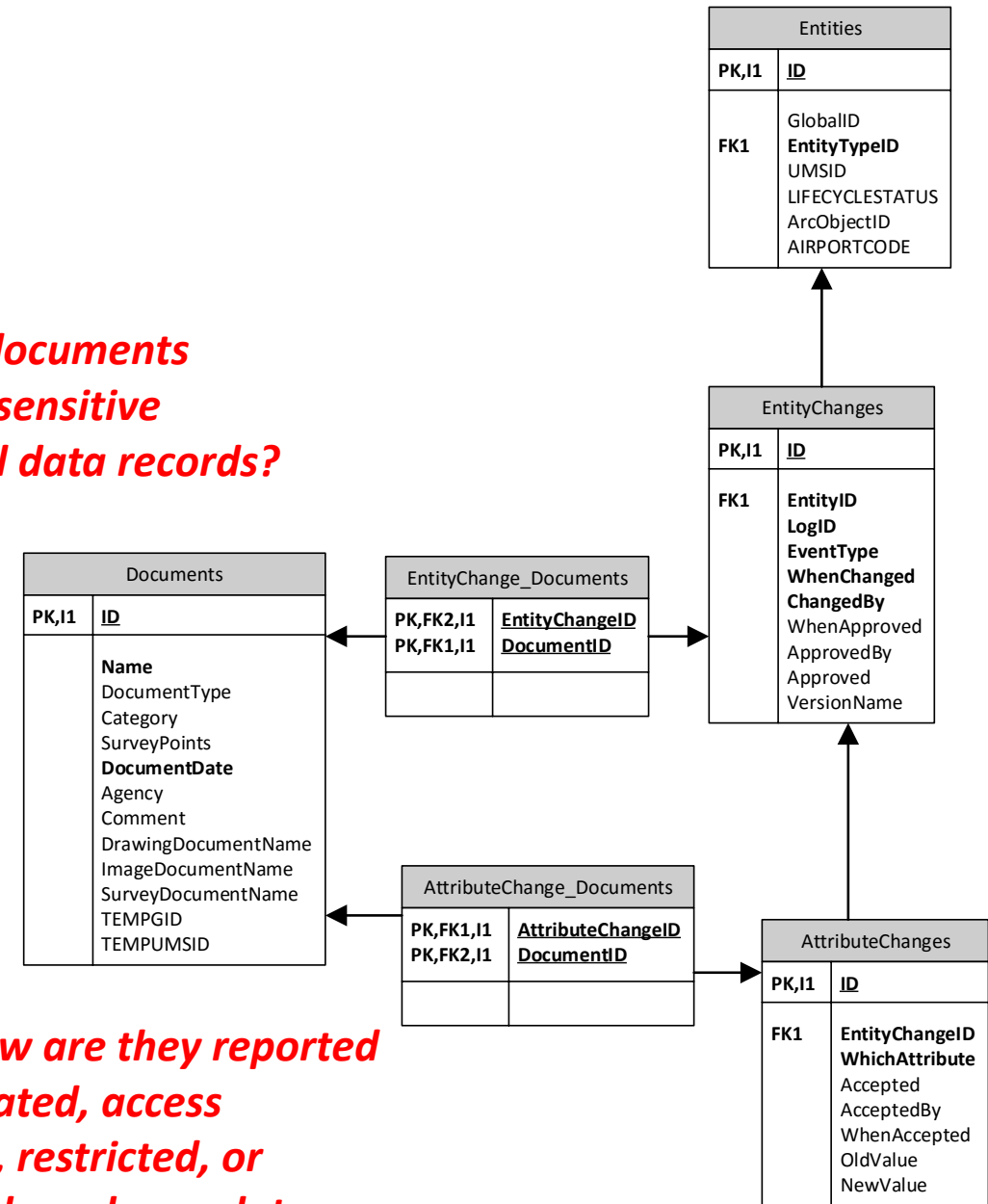
Do the changes pertain to a data subject's personal data attribute values? If so, which ones?

GDPR assessment questions



Do the documents contain sensitive personal data records?

If so, how are they reported on, updated, access blocked, restricted, or deleted based on a data subject's request?



Agenda

- Emerging issues in Application Security
 - ✓ GDPR Background
 - ✓ Principles for Privacy by Design
 - ✓ Key requirements
 - ✓ Approaches to meeting requirements
 - ✓ Assessing information system documentation
 - ✓ Data lineage (“provenance”) metadata
 - ✓ Assessing a metadata approach
- A few other frameworks for application security assessment
- Some best practices for secure application development
- Test areas for auditing applications

A few other General Frameworks for Application Security Assessment:

- **PPTM - People, Processes, Tools, and Measures**
- **STRIDE - Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege**
- **PDIO – Planning, Design, Implementation, and Operations**

PPTM - People, Processes, Tools, and Measures

- A brainstorming framework for examining security of an application from the macro-level
- **People** – describes every aspect of the application that deals with a human
 - Make sure the right people are involved in planning, design, implementation or operations, and the right stakeholders are involved
 - E.g. If the application involves end users, ensure:
 - The application has controls around providing and removing access
 - End users have been involved with the planning and design of components they will (to ensure usability)
- **Process** – Describes every aspect of the application that is involved in a policy, procedure, method, or course of action
 - Review the interaction of the application with interfacing systems and verify compliance with security models
 - E.g. Ensure that firewalls are in place to protect the application from external applications, users, business partners, ...
 - Policies and procedures should be written to support how the application is intended to be used
 - Adequate documentation should exist to support technicians who need to maintain the application
- **Tools** – Describe every aspect of the application that deals with concrete technology or product.
 - Ensure appropriate hardware and environment exist to support the application
 - Ensure the application interfaces with recommended technologies appropriate for your intended policies and procedures
 - Verify that the application and infrastructure are tested and audited appropriately
- **Measures** – Describe every aspect of the application that is quantifiable conceptually, such as the business purpose or application performance
 - E.g. verify that the application meets well-documented and well-thought out acceptance criteria
 - E.g. if the application is intended to solve a quantifiable business problem verify that it does indeed solve the problem
 - Verify that the logs are meaningful and that you can measure the performance of the application

STRIDE: Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege

- A methodology used for identifying known threats
- A simplified threat-risk model – easy to remember and apply to develop steps that address how each of the risks are mitigated
- **Spoofing Identity**
 - Is a key risk for applications with many users and a single execution context at the application and database tiers
 - Users should not be able to become any other user or assume the attributes of another user
- **Tampering with Data**
 - Data should be stored in a secure location, with access appropriately controlled
 - The application should carefully check data received from the user and validate that it is “sane” (i.e. relevant and valid) and applicable before storing or using it
 - Data entered in the client (e.g. browser) should be checked and validated on the server and not in the client where the validation checks might be tampered with
 - Application should not send and calculate data in the client where the user can manipulate the data, but in the server-side code
- **Repudiation**
 - Determine if the application requires nonrepudiation controls, such as web access logs, audit trails at each tier, or the same user context from top to bottom
 - Users may dispute transactions if there is insufficient auditing or record-keeping of their activity
- **Denial of Service**
 - Application designers should be aware that their applications are at risk of denial of service attacks
 - Use of expensive resources (e.g. large files, heavy-duty searches, long queries) should be reserved for authenticated and authorized users and should not be available to anonymous users.
 - Every facet of the application should be engineered to perform as little work as possible, to use fast and few database queries, and to avoid exposing large files or unique links per user to per user to prevent simple denial-of-service attacks
- **Elevation of Privilege**
 - If an application provides distinct user and administrative roles, ensure that the user cannot elevate his or her role to a more highly privileged one
 - All actions should be controlled through an authorization matrix to ensure that only the permitted roles can access privileged functionality. It is not sufficient, for example, to not display privileged-role links

PDIO – Planning, Design, Implementation, and Operations

- Comes from CISCO Systems
- Considers potential challenges at each stage of an application development project
- E.g. A problem might result if system administrators are planning the design of a network solution without the involvement of a senior networking engineer

Agenda

- ✓ Emerging issues in Application Security
 - ✓ GDPR Background
 - ✓ Principles for Privacy by Design
 - ✓ Key requirements
 - ✓ Approaches to meeting requirements
 - ✓ Assessing information system documentation
 - ✓ Data lineage (“provenance”) metadata
 - ✓ Assessing a metadata approach
- ✓ A few other frameworks for application security assessment
- Some best practices for secure application development
- Test areas for auditing applications

Some best practices for secure application development

Can help you quickly spot common weaknesses and poor controls

1. Defense-in-Depth
2. Positive Security Model
3. Fail Safely
4. Run with Least Privilege
5. Avoid Security by Obscurity
6. Keep Security Simple
7. Detect Intrusions and Keep Logs
8. Never Trust External Infrastructure and Services
9. Establish Secure Defaults
10. Use Open Standards

Defense In Depth

Layered approaches provide more security over the long term than one complicated mass of security architecture

- Access Control Lists (ACLs), for example, on the networking routers and firewall equipment to allow only necessary traffic to reach the application
 - *Quickly eliminating access to services, ports, and protocols significantly lowers the overall risk of compromise to the system on which the application is running*

Positive Security Model

- Positive security models use “whitelist” to allow only what is on the list, excluding everything else by default
 - “Deny by default”
 - A challenge for antivirus programs
- In contrast with negative (blacklist) security models that allow everything by default, eliminating only the items known to be bad
 - Problems:
 - Blacklist must be kept up to date
 - Even if blacklist is updated, an unknown vulnerability can still exist
 - Attack surface is much larger than with a positive security model

Fail Safely

- An application failure can be dealt with in one of 3 ways:
 - Allow
 - Block
 - Error
- In general, application errors should all fail in the same way:
 - Disallow the operation (as viewed by the user) and provide no or minimal information on the failure
 - Do not provide the end user with additional information that may help in compromising the system
 - Put the error information in the logs, but do not provide to the user to use in compromising the system

Run with Least Privilege

- Principle of Least Privilege mandates that accounts have the least amount of privilege possible to perform their activity
- This includes:
 - User rights
 - Resource permissions such as CPU limits, memory capacity, network bandwidth, file system permissions, and database permissions

Avoid Security by Obscurity

- Obfuscating data (hiding it) instead of encrypting it is a very weak security mechanism
 - If a human can figure out how to hide the data a human can learn how to recover the data
- Never obfuscate critical data that can be encrypted or never stored in the first place

Keep Security Simple

- Simple security mechanisms are easy to verify and easy to implement correctly
- Avoid complex security mechanisms if possible
 - *“The quickest method to break a cryptographic algorithm is to go around it”*
- Do not confuse complexity with layers: Layers are good; complexity isn't

Detect Intrusions and Keep Logs

- Applications should have built-in logging that is protected and easily read
- Logs help you troubleshoot issues, and just as important – help you to track down when or how an application might have been compromised

Never Trust External Infrastructure and Services

- Many organizations use the processing capabilities of third-party partners that more than likely have differing security policies and postures than your organization
- It is unlikely that you can influence or control an external third party
- Implicitly trusting externally run systems is dangerous!

Establish Secure Defaults

- New applications should arrive or be presented to users with the most secure default settings possible that still allow business to function
- This may require training end users or communications messages
- End result is a significantly reduced attack surface
 - *Especially when application is pushed out across a large population*

Use Open Standards

- Open security standards provide increased portability and interoperability
- IT infrastructure is often a heterogeneous mix of platforms, open standards helps ensure compatibility between systems as the application grows
- Open standards are often well known and scrutinized by peers in the security industry to ensure they remain secure

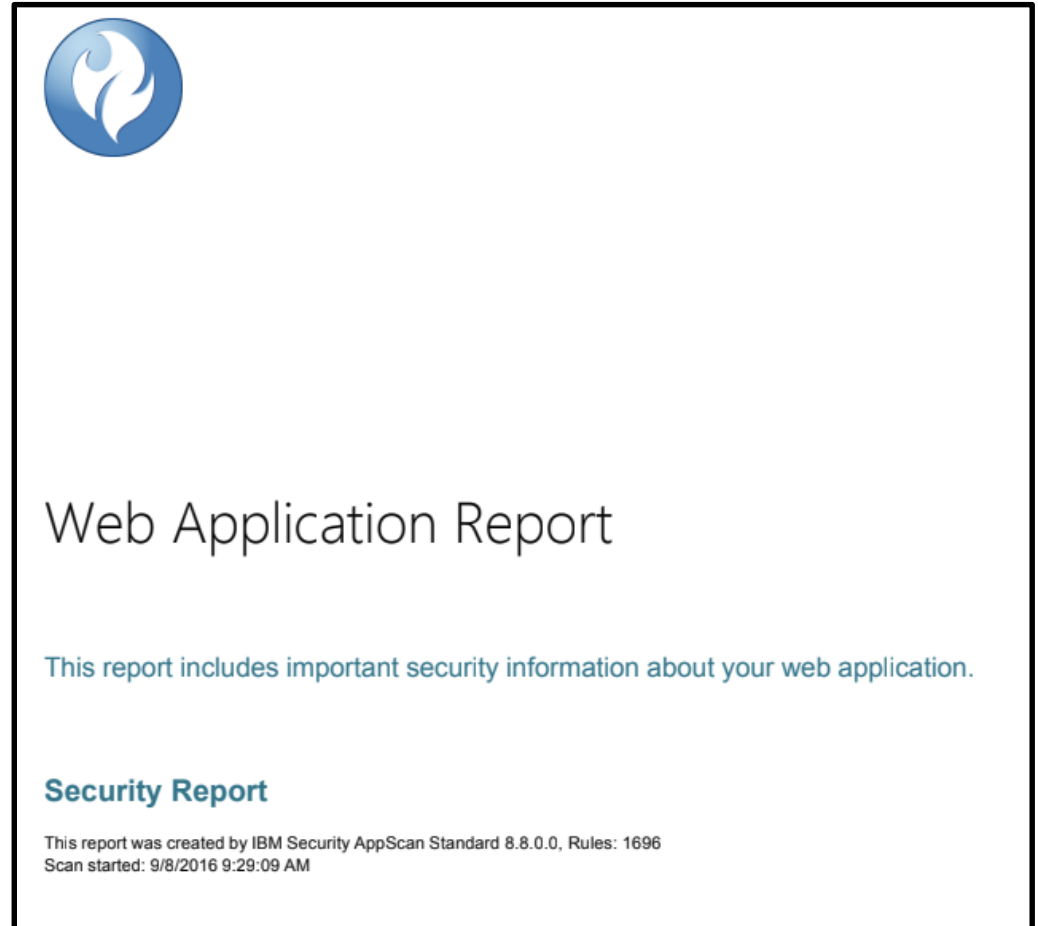
Agenda

- ✓ Emerging issues in Application Security
 - ✓ GDPR Background
 - ✓ Principles for Privacy by Design
 - ✓ Key requirements
 - ✓ Approaches to meeting requirements
 - ✓ Assessing information system documentation
 - ✓ Data lineage (“provenance”) metadata
 - ✓ Assessing a metadata approach
- ✓ A few other frameworks for application security assessment
- ✓ Some best practices for secure application development
- Test areas for auditing applications

Automated application security testing tools

Magic Quadrant

Figure 1. Magic Quadrant for Application Security Testing



Introduction

This report contains the results of a web application security scan performed by IBM Security AppScan Standard.

High severity issues:	79
Medium severity issues:	198
Total security issues included in the report:	277
Total security issues discovered in the scan:	308

Issues Sorted by Issue Type

- Authentication Bypass Using SQL Injection **2**
- Blind SQL Injection **4**
- Cross-Site Request Forgery **24**
- Cross-Site Scripting **3**
- HTTP PUT Method Site Defacement **20**
- Inadequate Account Lockout **1**
- Microsoft FrontPage Extensions Site Defacement **3**
- Missing Secure Attribute in Encrypted Session (SSL) Cookie **1**
- Phishing Through URL Redirection **1**
- WebDAV MKCOL Method Site Defacement **20**
- Alternate Version of File Detected **50**
- Cacheable SSL Page Found **26**
- Hidden Directory Detected **7**
- Microsoft FrontPage Configuration Information Leakage **1**
- Microsoft FrontPage Server Extensions Vital Information Leakage **2**
- Microsoft IIS Missing Host Header Information Leakage **1**
- Query Parameter in SSL Request **66**
- Temporary File Download **32**
- Unencrypted __VIEWSTATE Parameter **11**
- Web Application Source Code Disclosure Pattern Found **2**

Issue 1 of 2

TOC

Authentication Bypass Using SQL Injection

Severity: High**URL:** <https://www.r.../login.aspx>**Entity:** UserName (Parameter)**Risk:** It may be possible to bypass the web application's authentication mechanism**Causes:** Sanitation of hazardous characters was not performed correctly on user input**Fix:** [Review possible solutions for hazardous character injection](#)

Reasoning: The test result seems to indicate a vulnerability because when four types of request were sent - a valid login, an invalid login, an SQL attack, and another invalid login - the responses to the two invalid logins were the same, while the response to the SQL attack seems similar the response to the valid login.

Issue 2 of 2

TOC

Authentication Bypass Using SQL Injection

Severity: High**URL:** <https://www.r.../login.aspx>**Entity:** Password (Parameter)**Risk:** It may be possible to bypass the web application's authentication mechanism**Causes:** Sanitation of hazardous characters was not performed correctly on user input**Fix:** [Review possible solutions for hazardous character injection](#)

Reasoning: The test result seems to indicate a vulnerability because when four types of request were sent - a valid login, an invalid login, an SQL attack, and another invalid login - the responses to the two invalid logins were the same, while the response to the SQL attack seems similar the response to the valid login.

IBM AppScan example

Advisories

- Authentication Bypass Using SQL Injection ←
- Blind SQL Injection
- Cross-Site Request Forgery
- Cross-Site Scripting
- HTTP PUT Method Site Defacement
- Inadequate Account Lockout
- Microsoft FrontPage Extensions Site Defacement
- Missing Secure Attribute in Encrypted Session (SSL) Cookie
- Phishing Through URL Redirection
- WebDAV MKCOL Method Site Defacement
- Alternate Version of File Detected
- Cacheable SSL Page Found
- Hidden Directory Detected
- Microsoft FrontPage Configuration Information Leakage
- Microsoft FrontPage Server Extensions Vital Information Leakage
- Microsoft IIS Missing Host Header Information Leakage
- Query Parameter in SSL Request
- Temporary File Download
- Unencrypted __VIEWSTATE Parameter
- Web Application Source Code Disclosure Pattern Found

Authentication Bypass Using SQL Injection

[TOC](#)

Test Type:

Application-level test

Threat Classification:

Insufficient Authentication

Causes:

Sanitation of hazardous characters was not performed correctly on user input

Security Risks:

It may be possible to bypass the web application's authentication mechanism

Affected Products:

CWE:

566

References:

"Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
SQL Injection Training Module

Technical Description:

The application uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted user in a way that bypasses the protection mechanism.

When security decisions such as authentication and authorization are made based on the values of user input, attackers can bypass the security of the software.

Suppose the query in question is:

```
SELECT COUNT(*) FROM accounts WHERE username='$user' AND password='$pass'
```

Where \$user and \$pass are user input (collected from the HTTP request which invoked the script that constructs the query - either from a GET request query parameters, or from a POST request body parameters). A regular usage of this query would be with values \$user=john, \$password=secret123. The query formed would be:

```
SELECT COUNT(*) FROM accounts WHERE username='john' AND password='secret123'
```

The expected query result is 0 if no such user+password pair exists in the database, and >0 if such pair exists (i.e. there is a user named 'john' in the database, whose password is 'secret123'). This would serve as a basic authentication mechanism for the application. But an attacker can bypass this mechanism by submitting the following values: \$user=john, \$password=' OR '1'='1'.

The resulting query is:

```
SELECT COUNT(*) FROM accounts WHERE username='john' AND password='' OR '1'='1'
```

This means that the query (in the SQL database) will return TRUE for the user 'john', since the expression 1=1 is always true. Therefore, the query will return a positive number, and thus the user (attacker) will be considered valid without having to know the password.

Technical Description:

The application uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted user in a way that bypasses the protection mechanism.

When security decisions such as authentication and authorization are made based on the values of user input, attackers can bypass the security of the software.

Suppose the query in question is:

```
SELECT COUNT(*) FROM accounts WHERE username='$user' AND password='$pass'
```

Where \$user and \$pass are user input (collected from the HTTP request which invoked the script that constructs the query - either from a GET request query parameters, or from a POST request body parameters). A regular usage of this query would be with values \$user=john, \$password=secret123. The query formed would be:

```
SELECT COUNT(*) FROM accounts WHERE username='john' AND password='secret123'
```

The expected query result is 0 if no such user+password pair exists in the database, and >0 if such pair exists (i.e. there is a user named 'john' in the database, whose password is 'secret123'). This would serve as a basic authentication mechanism for the application. But an attacker can bypass this mechanism by submitting the following values: \$user=john, \$password=' OR '1'='1'.

The resulting query is:

```
SELECT COUNT(*) FROM accounts WHERE username='john' AND password='' OR '1'='1'
```

This means that the query (in the SQL database) will return TRUE for the user 'john', since the expression 1=1 is always true. Therefore, the query will return a positive number, and thus the user (attacker) will be considered valid without having to know the password.

Application Security Assessment and Recommendations

Issue Types 21

Issue Type	Number of Issues
H Authentication Bypass Using HTTP Verb Tampering	3
H Cross-Site Request Forgery	23
H Cross-Site Scripting	2
H Microsoft FrontPage Extensions Site Defacement	3
H Missing Secure Attribute in Encrypted Session (SSL) Cookie	5
H RC4 cipher suites were detected	1
M Alternate Version of File Detected	45
M Body Parameters Accepted in Query	9
M Browser Exploit Against SSL/TLS (a.k.a. BEAST)	1
M Cacheable SSL Page Found	67
M Direct Access to Administration Pages	1
M Drupal "keys" Path Disclosure	1
M Insecure "OPTIONS" HTTP Method Enabled	1
M Microsoft FrontPage Server Extensions Vital Information Leakage	2
M Microsoft IIS Missing Host Header Information Leakage	1
M Missing "Content-Security-Policy" header	5
M Missing Cross-Frame Scripting Defence	4
M Query Parameter in SSL Request	185
M Temporary File Download	3
M Unencrypted __VIEWSTATE Parameter	20
M Web Application Source Code Disclosure Pattern Found	1

TOC Fix Recommendations 19

TOC

Remediation Task	Number of Issues
H Review possible solutions for hazardous character injection	2
M Add the 'Secure' attribute to all sensitive cookies	5
M Change server's supported ciphersuites	2
M Configure your server to allow only required HTTP methods	3
M Set proper permissions to the FrontPage extension files	3
M Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form	23
L Always use SSL and POST (body) parameters when sending sensitive information.	185
L Apply configuration changes according to Q218180	1
L Apply proper authorization to administration scripts	1
L Config your server to use the "Content-Security-Policy" header	5
L Config your server to use the "X-Frame-Options" header	4
L Contact the vendor of your product to see if a patch or a fix has been made available recently	1
L Disable WebDAV, or disallow unneeded HTTP methods	1
L Do not accept body parameters that are sent in the query string	9
L Modify FrontPage extension file permissions to avoid information leakage	2
L Modify your Web.Config file to encrypt the VIEWSTATE parameter	20
L Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	67
L Remove old versions of files from the virtual directory	48
L Remove source code files from your web-server and apply any relevant patches	1

Test Areas for Auditing Applications

1. Input Controls

- Review and evaluate controls built into system transactions for input data
- Determine the need for error/exception reports related to data integrity and evaluate whether this need has been filled

2. Interface Controls

- Review and evaluate the controls in place over data feeds to and from interfacing systems
- If the same data is kept in multiple databases and/or systems, ensure that periodic sync processes are executed to detect any inconsistencies in the data

3. Audit Trails

- Review and evaluate the audit trails present in the system and the controls over those audit trails
- Ensure that the system provides a means of tracing a transaction or piece of data from the beginning to the end of the process enabled by the system

Test Areas for Auditing Applications

4. Identity, Authentication, and Access Controls

- Ensure that the application provides a mechanism that authenticates users based, at a minimum, on a unique identifier for each user and appropriate authentication factors
- Review and evaluate the application's authorization mechanism to ensure that users are not allowed to access any sensitive transactions or data without first being authorized by the system's security mechanism
- Ensure that the system's security/authorization mechanism has an administrator function with appropriate controls and functionality
- Determine whether the security mechanism enables any applicable approval processes
- Review and evaluate processes for granting access to users, ensure that access is granted only when there is a legitimate business need
- Review processes for removing user access when it is no longer needed. Ensure that a mechanism or process is in place that suspends user access on termination from the company or on a change of jobs within the company
- Verify that the application has appropriate password controls. Also, determine whether default application account passwords have been changed
- Ensure that users are automatically logged off from the application after a certain period of inactivity
- Evaluate the use of encryption techniques to protect application data
- Evaluate application developer access to alter production data

Test Areas for Auditing Applications

5. Software Change Controls

- Ensure that the application software cannot be changed without going through a standard checkout/staging/testing/approval process after it is placed into production
- Evaluate controls regarding code checkout and versioning
- Evaluate controls regarding the testing of application code before it is placed into a production environment
- Evaluate controls regarding batch scheduling

6. Backup and Recovery

- Determine whether a Business Impact Analysis (BIA) has been performed on the application to establish backup and recovery needs
- Ensure that appropriate backup and recovery controls are in place
- Ensure appropriate recovery controls are in place

Test Areas for Auditing Applications

7. Data Retention and User Involvement

- Evaluate controls regarding the application's data retention
- Evaluate overall user involvement and support for the Application

8. Host Hardening...

Agenda

- ✓ Emerging issues in Application Security
 - ✓ GDPR Background
 - ✓ Principles for Privacy by Design
 - ✓ Key requirements
 - ✓ Approaches to meeting requirements
 - ✓ Assessing information system documentation
 - ✓ Data lineage (“provenance”) metadata
 - ✓ Assessing a metadata approach
- ✓ A few other frameworks for application security assessment
- ✓ Some best practices for secure application development
- ✓ Test areas for auditing applications