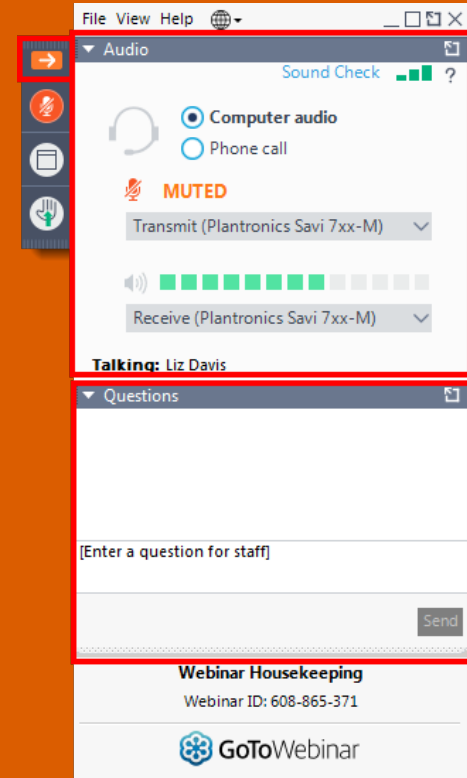


Welcome to the Webinar...we will begin shortly.

There are two methods for listening to this webinar, select **Audio** from the tool box on the right side of your screen, and:

- Select either **Computer audio** to use your computer's mic and speakers; or
- **Phone call** to use your telephone. Dial in with the phone number provided in your webinar confirmation e-mail or the number provided in the tool box, and enter your **Access Code** and **Audio PIN** when prompted.
- If no phone number is listed, you must use the **Computer audio** option.
- Please submit your questions and comments via the **Questions** panel during the presentation.
- This webinar is being recorded and will be posted to the Webinar Archives on IIBA's website within 5 business days.
<https://www.iiba.org/professional-development/knowledge-centre/webinars/webinar-archives/>
- All participants are muted during the webinar.

For demonstration purposes



The screenshot shows a software interface for a webinar. At the top, there is a menu bar with 'File', 'View', and 'Help'. Below it is a 'Audio' control panel. The 'Audio' panel has a 'Sound Check' indicator with a green bar and a question mark. There are two radio buttons: 'Computer audio' (selected) and 'Phone call'. Below these is a microphone icon and the word 'MUTED' in orange. There are two dropdown menus: 'Transmit (Plantronics Savi 7xx-M)' and 'Receive (Plantronics Savi 7xx-M)'. A volume slider is visible. Below the audio controls, it says 'Talking: Liz Davis'. There is a 'Questions' panel with a text input field containing '[Enter a question for staff]' and a 'Send' button. At the bottom, there is a footer with 'Webinar Housekeeping', 'Webinar ID: 608-865-371', and the 'GoToWebinar' logo.



"Mapping Business Processes to Compliance Procedures"

Hosted by: Liva Randrembason, IIBA

Presented and Sponsored by: Idera

Gain a Competitive Edge with IIBA Membership

Supports your connections, your development and your career growth



Online Library

- 300+ industry books and videos - a \$15,000 USD value.



Essential Resources

- *BABOK® Guide v3*
- Agile Extension to the *BABOK®*
- Member e-newsletters & BA Lens magazine
- Podcast



Thought Leadership

- The leading-edge insights that provides BAs the opportunity to evolve professionally and advance their careers.



IIBA Career Resources

- Career Centre
- Competency Model
- Special Interest Groups



Connections

- Join your local Chapter
- Volunteer
- Participate in online Community



Webinars

- Access to webinars on the latest topics

OUR DRIVER

“Unite a
community of
professionals to
create better
business
outcomes”

- IIBA Core Purpose



This webinar is brought to you by:

I D E R A

www.idera.com

 Premier
Sponsor

Supporting the Business Analysis Community

Today's Presenters



**Kim
Brushaber**

Senior Product
Manager for ER/Studio
Business Architect
IDERA

MAPPING BUSINESS PROCESSES TO COMPLIANCE PROCEDURES

Presented by Kim Brushaber, Senior Product Manager, IDERA



I D E R A[®]



*A jury consists of twelve persons chosen to decide
who has the better lawyer.
- Robert Frost*

BUSINESS JARGON VS TECHNICAL JARGON



OBJECTIVES FOR EACH GROUP

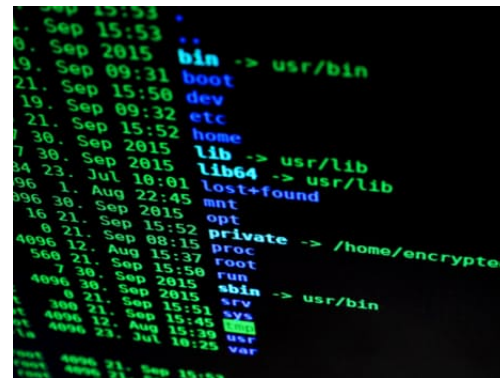
BUSINESS GROUP

- Reporting to Stakeholders
- Assessing ROI of releases
- Identifying PII Data
- Defining Business Processes



TECHNICAL GROUP

- Software implementations
- Database Security
- Encryption
- Data Masking



LEGAL GROUP

- Liability
- Addressing regulation concerns
- Legal bases covered
- Data Protection Policies

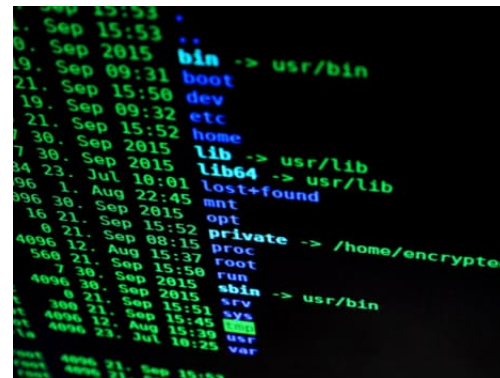
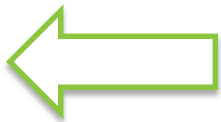


OBJECTIVES FOR EACH GROUP

BUSINESS GROUP

TECHNICAL GROUP

LEGAL GROUP



GETTING THE TEAMS TO WORK TOGETHER





*A lawyer is a person who writes a 10,000 word document and calls it a brief.
– Franz Kafka*

WHY ARE LEGAL TEAMS GETTING MORE INVOLVED?

PRIMARY AREAS OF FOCUS FOR GENERAL COUNSEL

When asked what are the primary areas of focus for the coming 12 months (selecting all that apply):

- 59% - Data privacy and security matters
- 49% - Employee compliance training
- 40% - Third-party oversight and management
- 36% - Changes in regulatory matters
- 34% - Bribery and corruption
- 19% - Internal investigations

<https://consero.com/august-2017-corporate-compliance-ethics-report/>



REGULATORY GUIDELINES (NOT ALL INCLUSIVE)

- Basel I, II and III (Banking)
- CGMP (Goods Manufacturing)
- CIS (Security)
- DISA/STIG (Security)
- FERPA (Family Rights)
- FISMA (Federal Agencies)
- GLBA (Finance)
- GDPR (Data Protection – EU)
- HIPAA (Healthcare)
- ISO (Security)
- NERC CIP (Electricity)
- PIPEDA (Data Protection – Canada)
- PCI DSS (Payment Cards)
- SOX (Accounting and Finance)



GUIDELINES MAY ASK YOU TO:

- Be transparent in how data is processed
- Collect only the information that is necessary
- Keep data accurate and up to date
- Keep data for a set amount of time
- Process information with adequate security measures in place
- Log, audit and monitor your operations and processing systems
- Detect and report on data breaches in a timely manner



GDRP AND THE DATA PROTECTION OFFICER (DPO)

GDPR Article 39 states that the DPO's responsibilities include (but are not limited to):

- Educating the company and employees on compliance requirements
- Training staff who are involved in data processing
- Conducting audits to ensure compliance and address any issues
- Liaison between the company and the GDPR Supervising Authority
- Monitoring the impact of data protection efforts
- Maintaining comprehensive records on all data processing activities
- Interfacing with users to inform them how their data is being used
- Creating and updating documentation on data protection policies
- Consulting on how to deal with privacy breaches



28K Data Protection Officers (DPOs) will be needed in the US and EU with as many as 75K needed around the Globe due to GDPR.

(<https://www.reuters.com/article/us-cyber-gdpr-dpo/rise-of-the-data-protection-officer-the-hottest-tech-ticket-in-town-idUSKCN1FY1MY>)

DATA SECURITY EXECUTIVE PERSPECTIVE



- **90% of CIOs** admit to wasting millions on inadequate cybersecurity
- **90% of CIOs** have already been attacked or expect to be attacked by bad guys hiding in their encryption
- **87% of CIOs** believe their security controls are failing to protect their businesses
- **85% of CIOs** expect criminal misuse of keys and certificates to get worse

https://www.venafi.com/assets/pdf/wp/Venafie_2016CIO_SurveyReport.pdf



*Almost **15 Billion** Records have been lost or stolen since 2013. Only **4%** were secure breaches where encryption was used and the stolen data was useless.*

BreachLevelIndex.com



Over 6.5 million data records are lost or stolen every day.

<http://breachlevelindex.com/>



IDERA®

US DATA BREACHES IN 2017

Category	# of Breaches (2017)	# of Records (2017)		
Banking/Credit/Financial	134	3,230,308		
Business	907	181,630,520		
Educational	128	1,418,455		
Government/Military	79	6,030,619		
Medical/Healthcare	384	5,302,846		
Total for all Categories	1632	197,612,748		

<https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/>

US DATA BREACHES IN 2017 AND 2018

Category	# of Breaches (2017)	# of Records (2017)	# of Breaches (2018)	# of Records (2018)
Banking/Credit/Financial	134	3,230,308	135	1,709,013
Business	907	181,630,520	571	415,233,143
Educational	128	1,418,455	76	1,408,670
Government/Military	79	6,030,619	99	18,236,710
Medical/Healthcare	384	5,302,846	363	9,927,798
Total for all Categories	1632	197,612,748	1244	446,515,334

<https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/>

US DATA BREACHES IN 2017 AND 2018

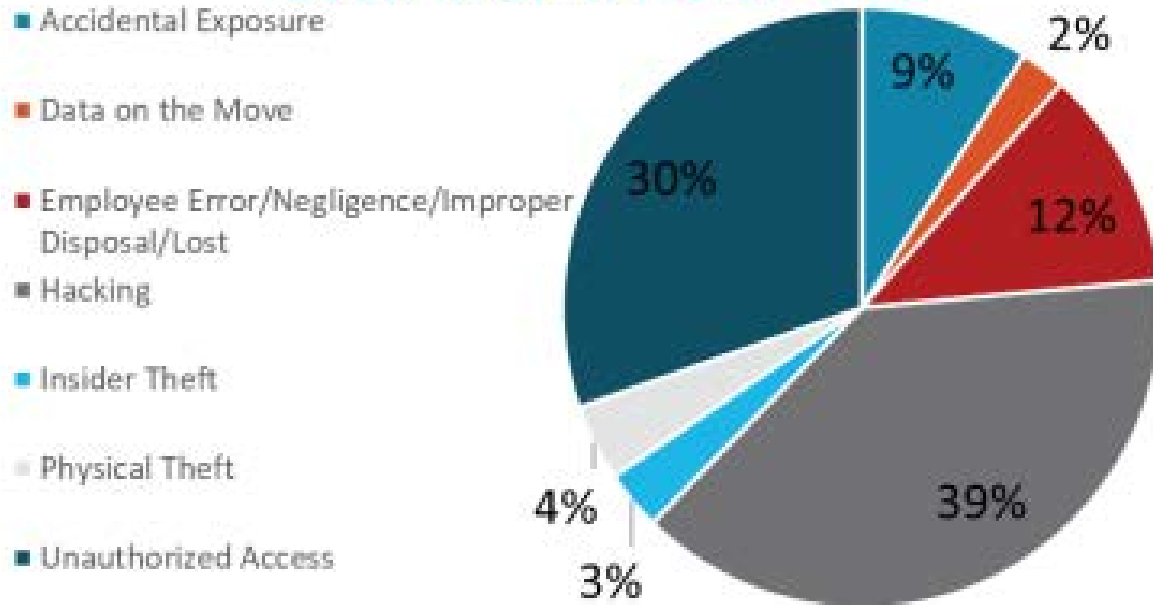
Category	# of Breaches (2017)	# of Records (2017)	# of Breaches (2018)	# of Records (2018)
Banking/Credit/Financial	134	3,230,308	135	1,709,013
Business	907	181,630,520	571	415,233,143
Educational	128	1,418,455	76	1,408,670
Government/Military	79	6,030,619	99	18,236,710
Medical/Healthcare	384	5,302,846	363	9,927,798
Total for all Categories	1632	197,612,748	1244	446,515,334

- Breaches are down 23%
- Exposed Records are up 126%

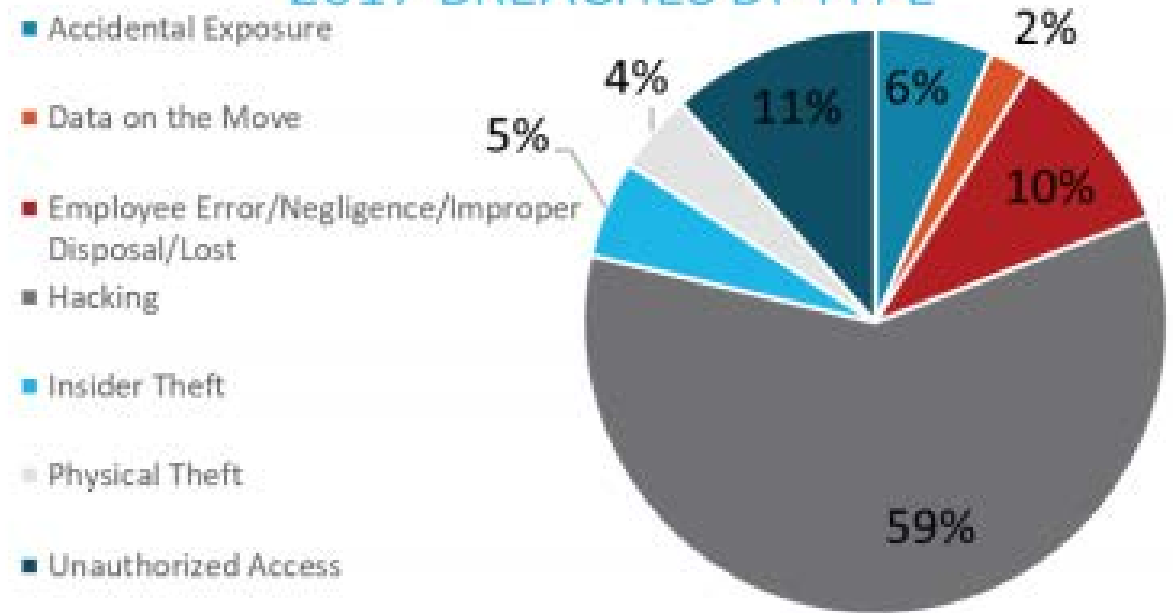
<https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/>

BREACHES BY TYPE

2018 BREACHES BY TYPE



2017 BREACHES BY TYPE



<https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/>



In the first 60 days of 2019, there have already been 29 major data breaches with over 1.2 billion records affected – averaging a breach every other day and 20 million records a day.

<https://www.identityforce.com/blog/2019-data-breaches>

SHOCKING, RIGHT??



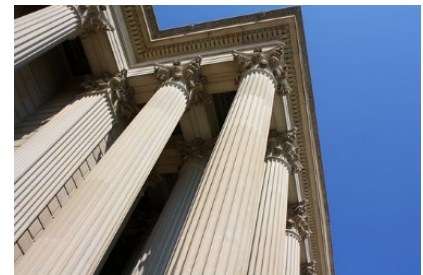
DATA BREACH LITIGATION



- Lawsuits are filed almost instantaneously upon announcement of a breach
- Legal defense costs between **\$500K** and **\$1M** are typical
- Regulatory fees and judgments can be extensive
 - Target paid **\$18.5M** after a 2013 breach affecting **41M** customers
- Legal defense works to determine the perceived “injury” and standard of harm of those affected by the breach (which still varies wildly)
 - Who was affected and what data was breached?
- Legal defense works on second level issues – class certification, causation, proof of damages

DATA IN A “LEGAL HOLD” OR “LITIGATION HOLD”

- Initiate a legal hold ASAP instructing stakeholders, key employees and data stewards not to delete or alter their data
- Interview data team to understand what data needs to be retained
- Interview data team to understand the events under investigation
- Make sure that relevant data is preserved (either left in place or archived)
- Confirm that processes will not interfere with the preserved data
- Create a process to handle the responsibilities of the hold (preparing information for the legal teams and managing the process)
- Tracking the hold through the process and releasing it upon completion



INTERNAL INVESTIGATIONS INVOLVING DATA

Amazon is currently investigating claims of employees leaking data for bribes

- Providing internal sales metrics
- Delivering reviewers' email addresses
- Deleting negative reviews
- Restoring banned accounts



<https://www.cnbc.com/2018/09/17/amazon-investigating-claims-of-employees-leaking-data-for-bribes.html>

LEGAL TEAMS NEED TO KNOW



- What processes affect data (especially PII data)?
- Which systems interact with the data?
- What happens to the data out of the company domain?
- Who has access to the data?
- What are the security policies and protocols?
- Are the processes being followed/audited?
- In the case of a “legal hold” what information is relevant?
- How do you track users accessing/modifying data they shouldn't be?



*People are getting smarter nowadays; they are letting lawyers, instead of their conscience, be their guide.
- Will Rogers*

HOW CAN YOU START TO ENGAGE YOUR LEGAL TEAM?

DATA IN PICTURES

Business



Technical



Legal

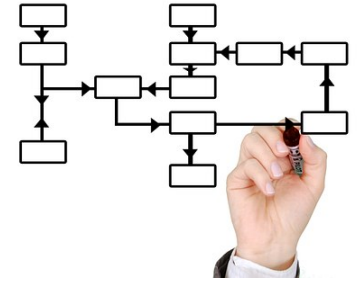


PICTURES AREN'T JUST WORTH 1000 WORDS

- They enhance the story
- They communicate a vision
- They can be language/jargon agnostic
- They clarify the points you are trying to make
- They bring everyone onto the same page

So why not use pictures instead of words when describing a business?

BUSINESS PROCESS DIAGRAMS



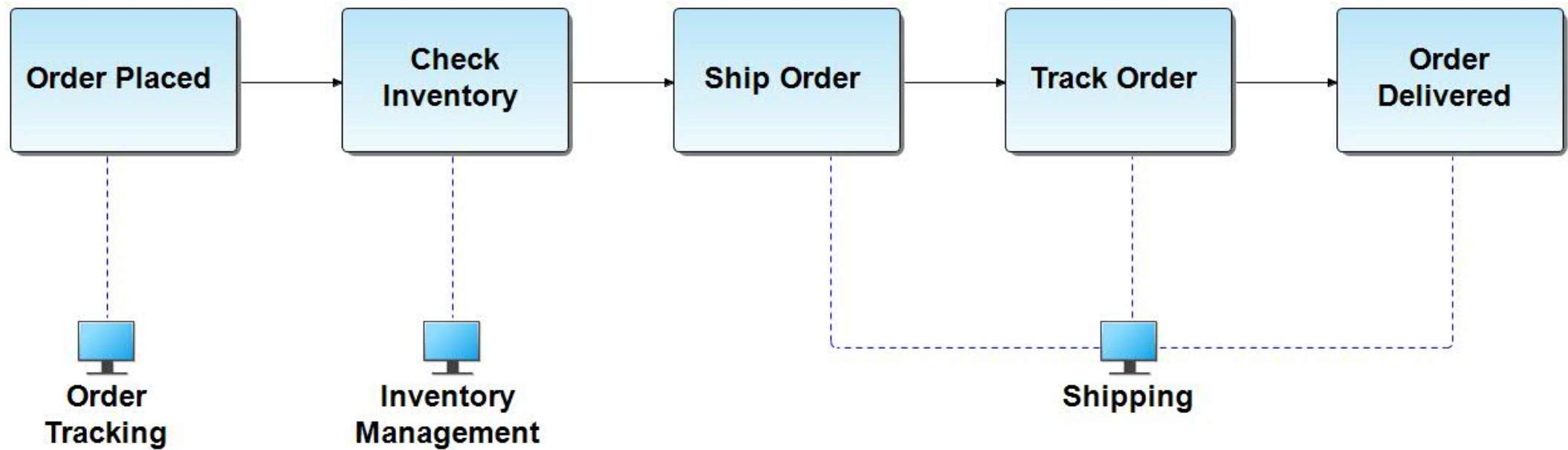
- Business Process Diagrams allow you to tell the story in a language that all 3 can understand
- Once you have started documenting a process, it's easy to discuss all of the aspects relating to that item
- Each group will see different gaps and holes in the process
- Processes can easily be refined to incorporate new input
- Processes can be used to educate others in the company
- Processes can be used to train new people when they join

SIMPLE ORDER PROCESS



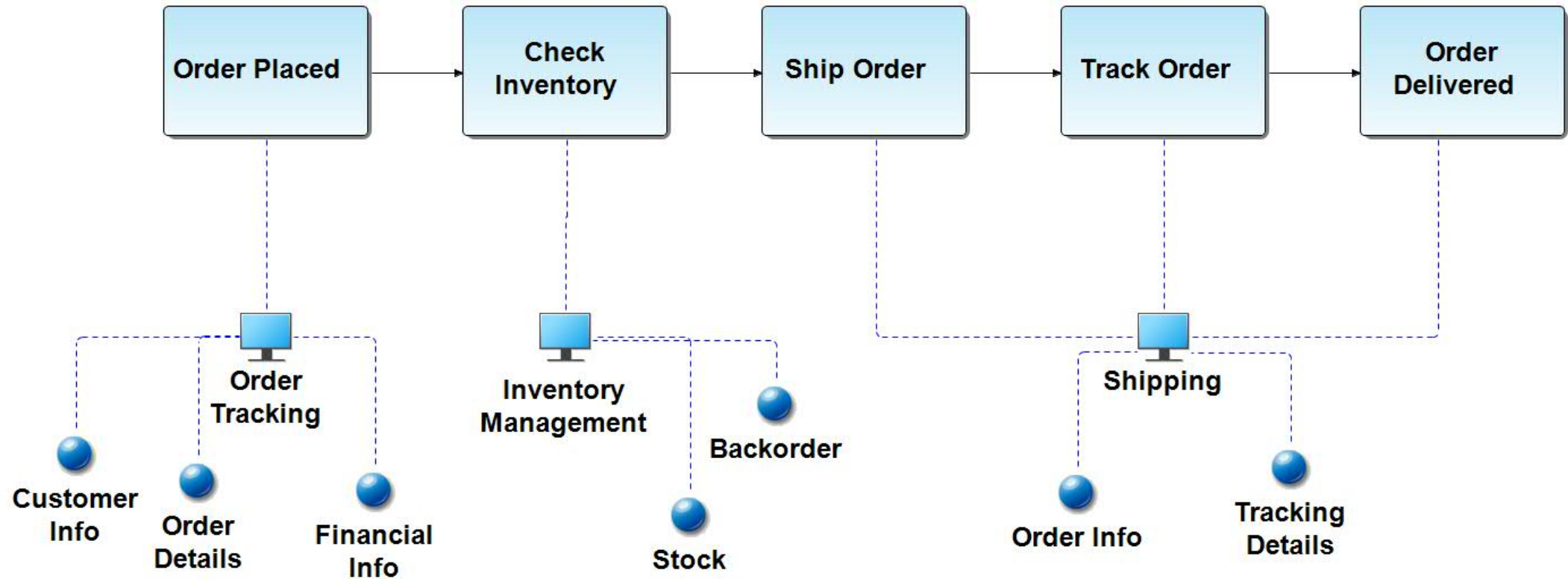
* Business Process Diagram created using ER/Studio Business Architect

BUSINESS APPLICATIONS



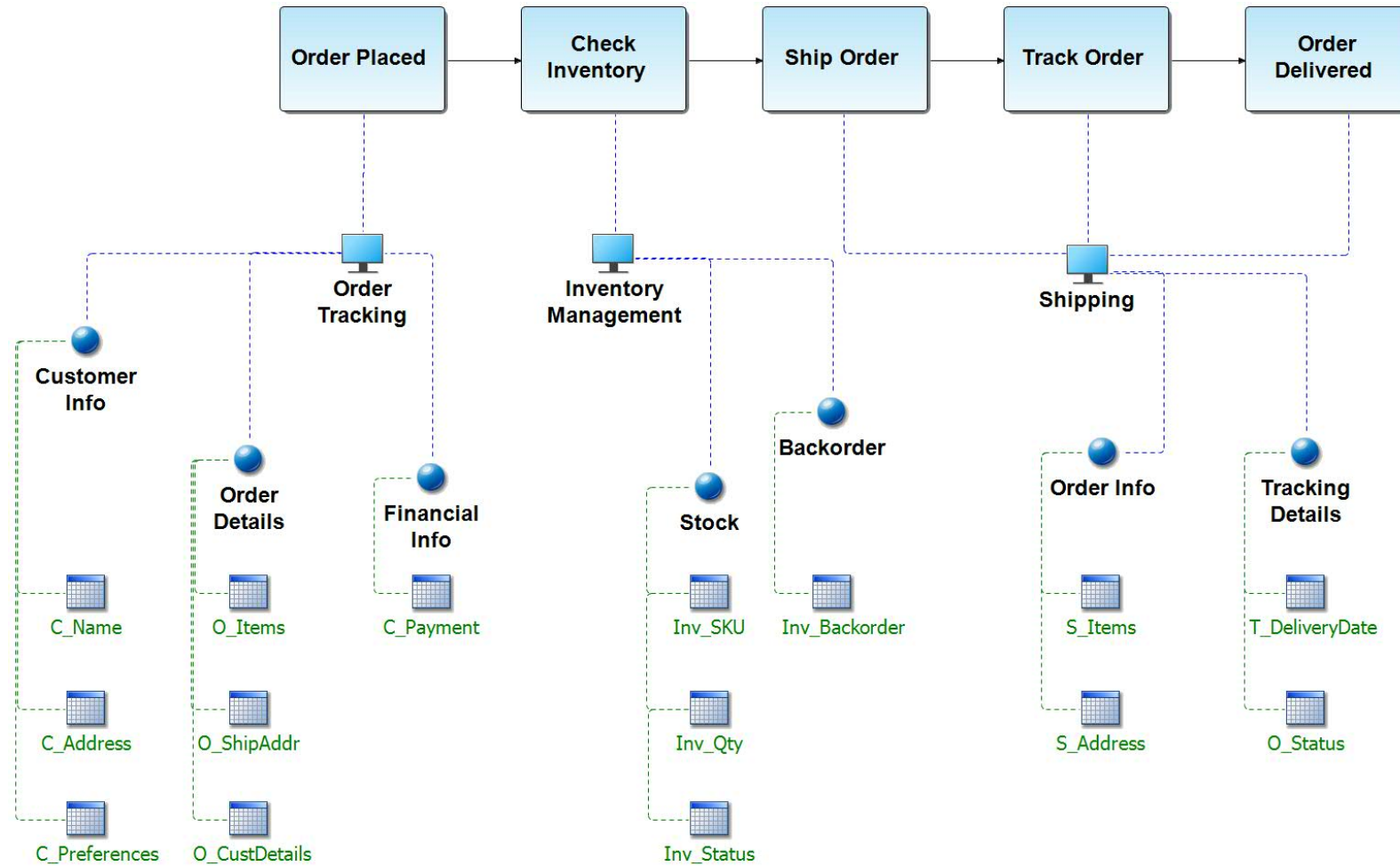
* Business Process Diagram created using ER/Studio Business Architect

BUSINESS ELEMENTS



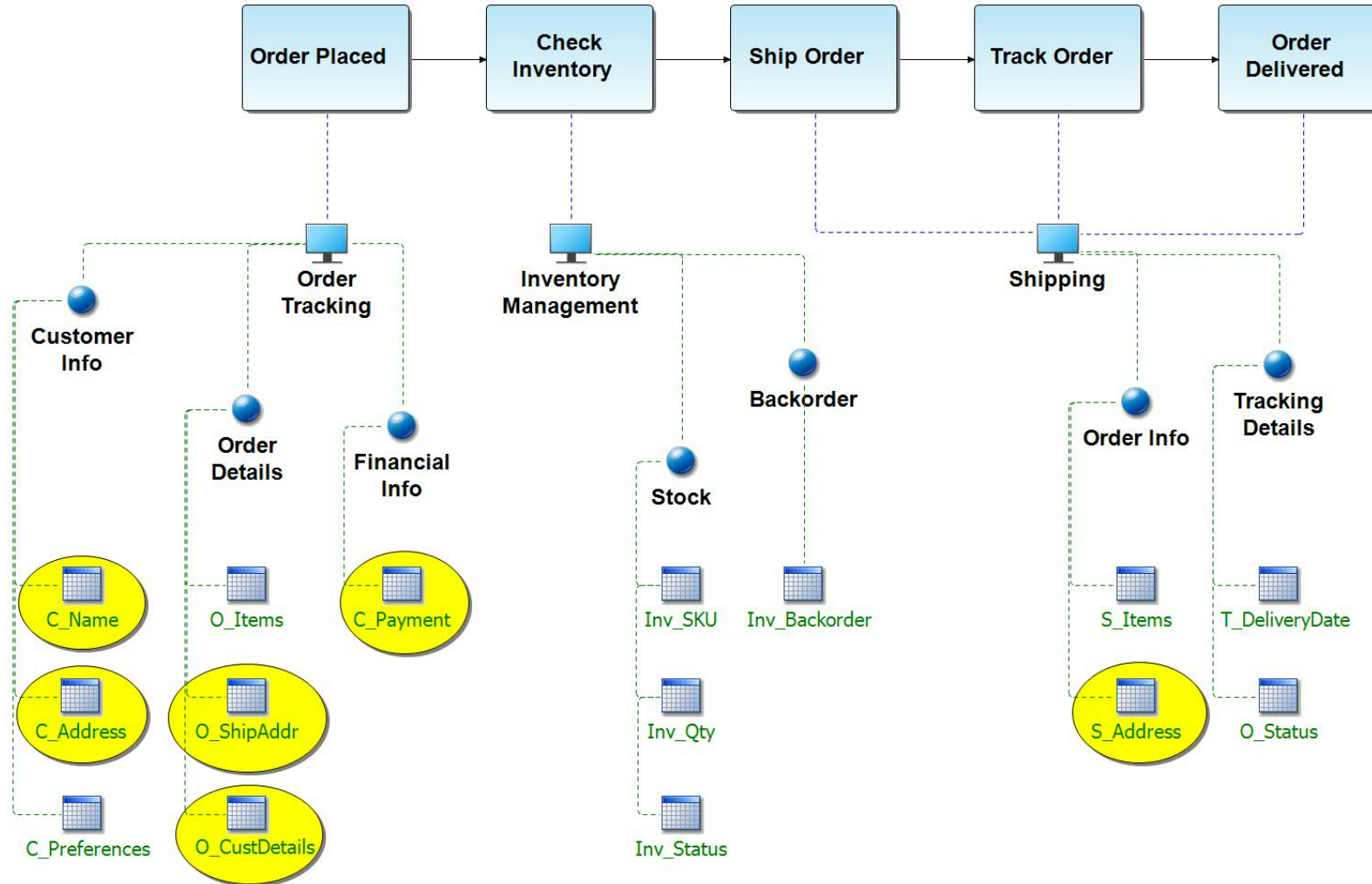
* Business Process Diagram created using ER/Studio Business Architect

TECHNICAL DETAILS



* Business Process Diagram created using ER/Studio Business Architect

LEGAL CONSIDERATIONS



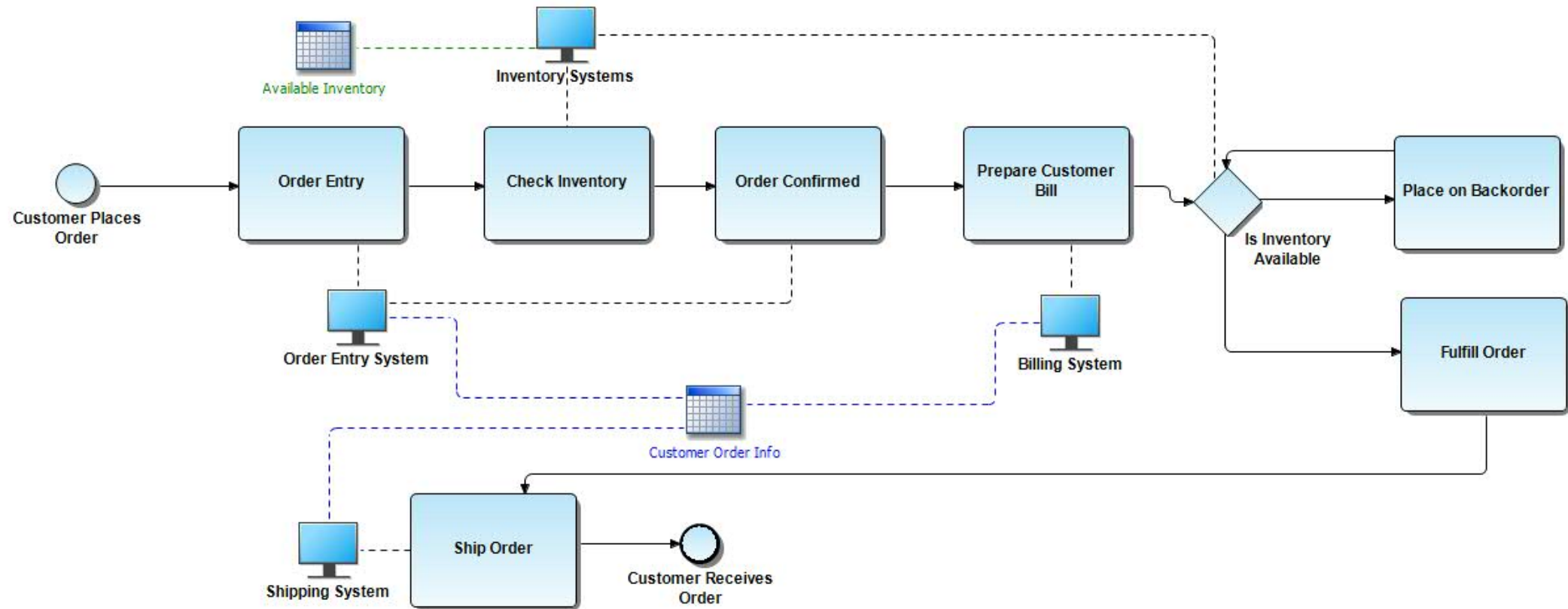
* Business Process Diagram created using ER/Studio Business Architect



Lawyers are seldom loved but often needed.
- Robert McKay

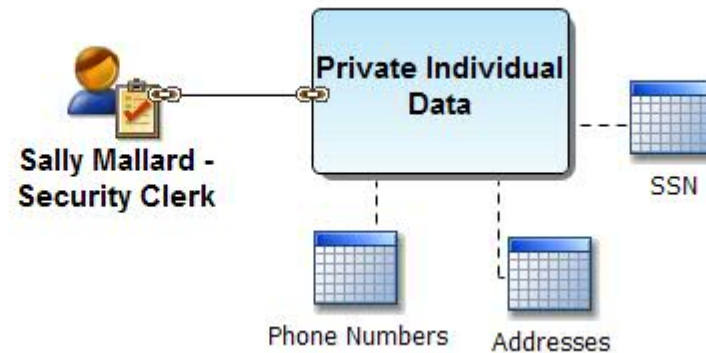
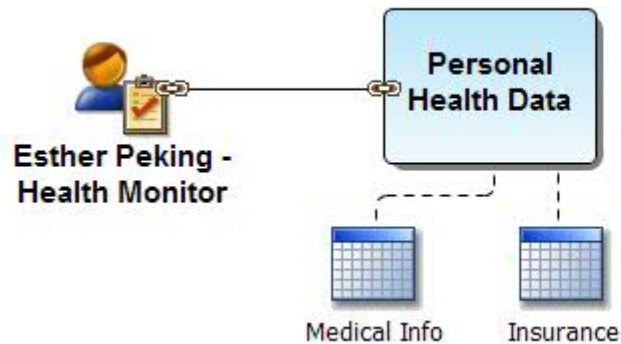
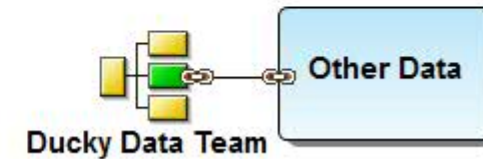
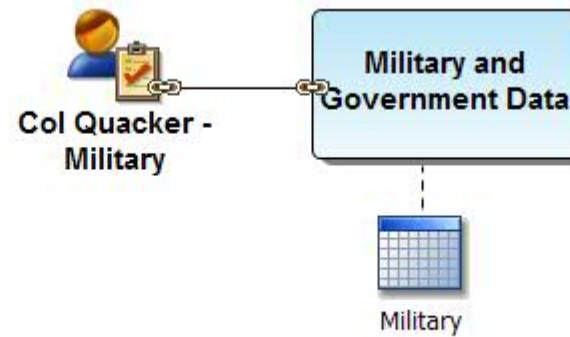
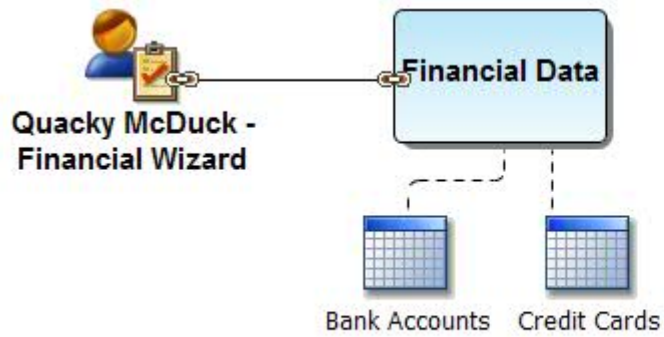
EXAMPLES OF BUSINESS PROCESS MODELS FOR EVERYONE

DETERMINE WHEN DATA SHOULD BE AVAILABLE



* Business Process Models created using IDERA's ER/Studio Business Architect

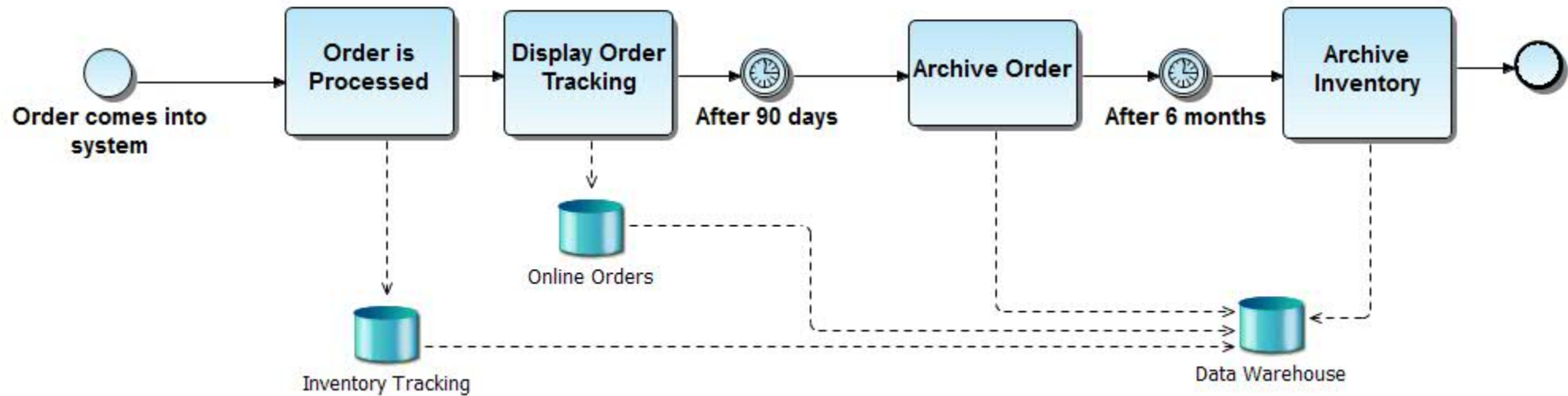
WHO HAS ACCESS TO THE DATA?



* Business Process Diagram created using ER/Studio Business Architect

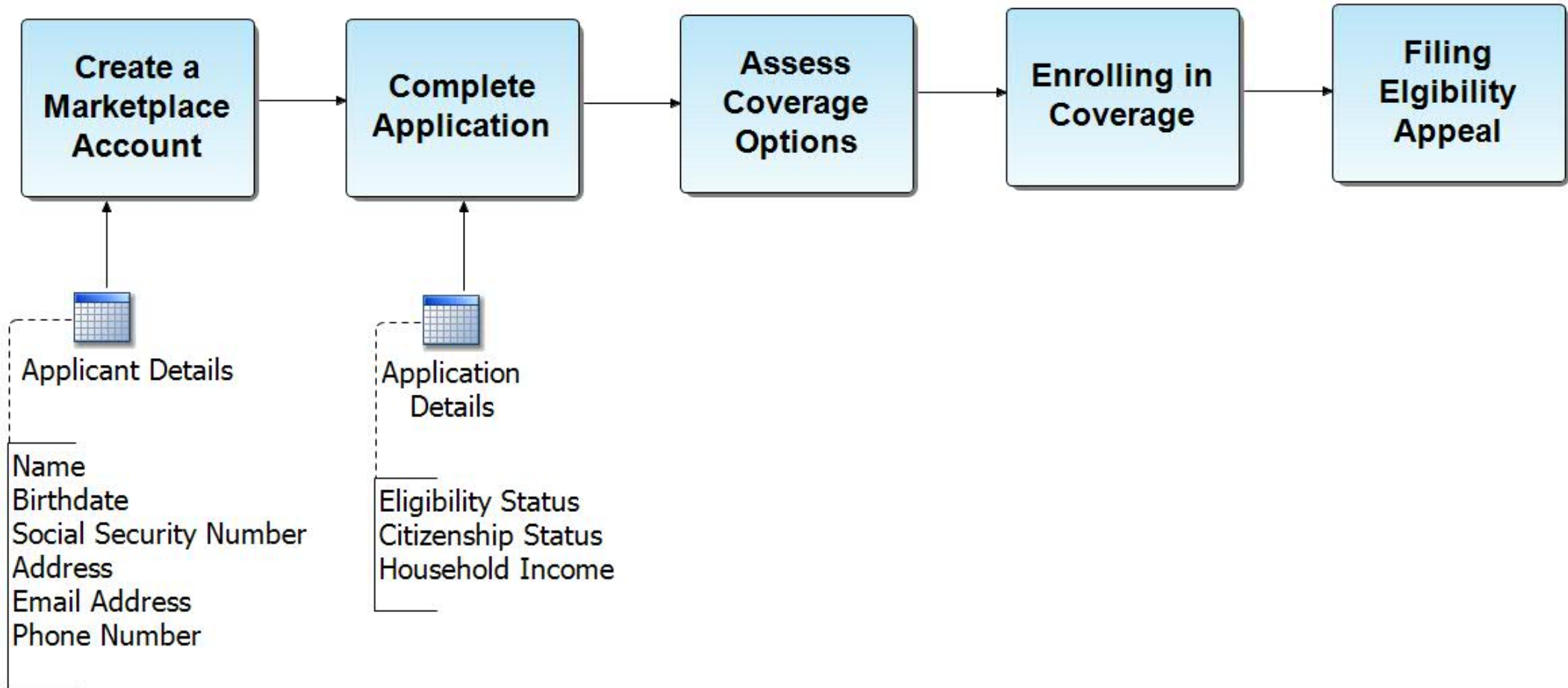
HOW DATA IS ARCHIVED

Archive Order Inventory



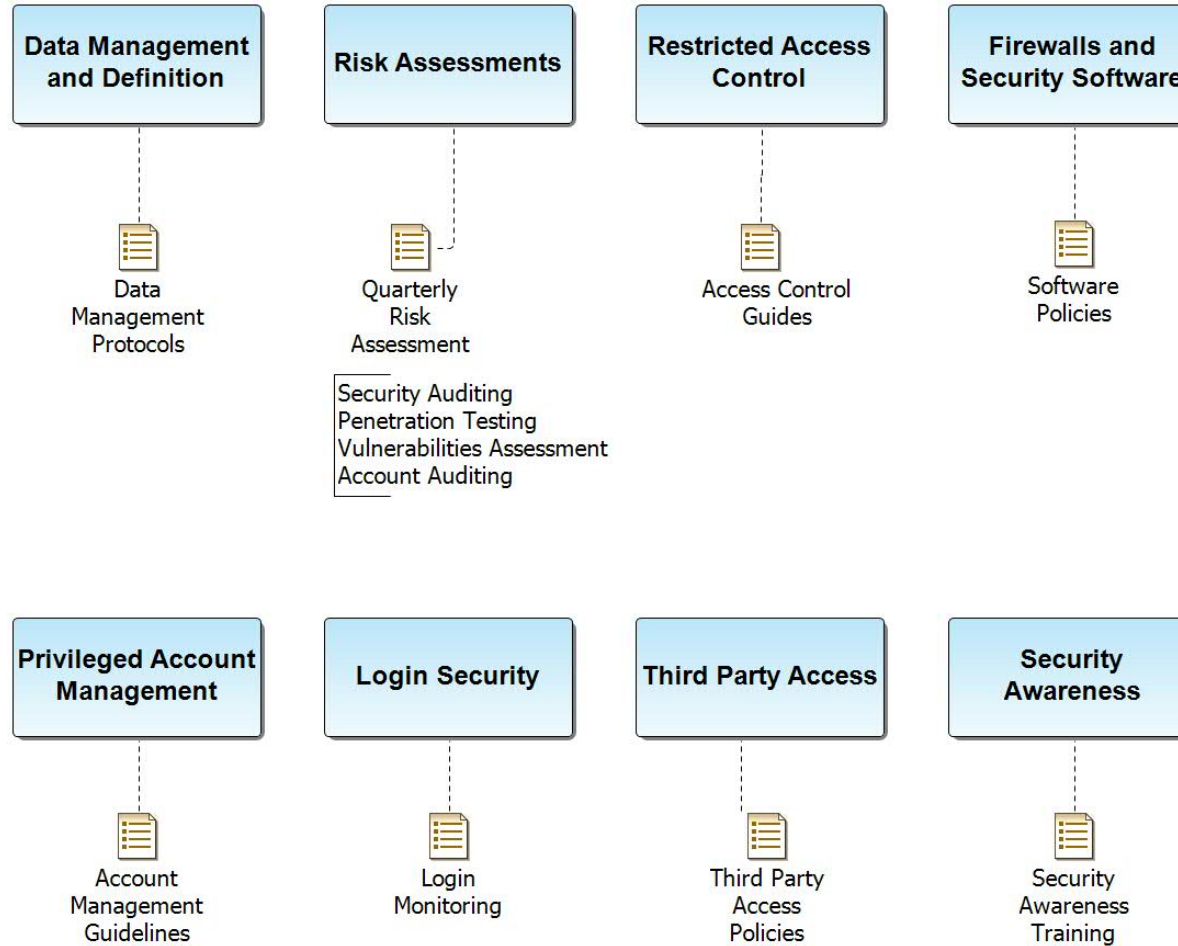
* Business Process Models created using IDERA's ER/Studio Business Architect

HANDLING PII DATA



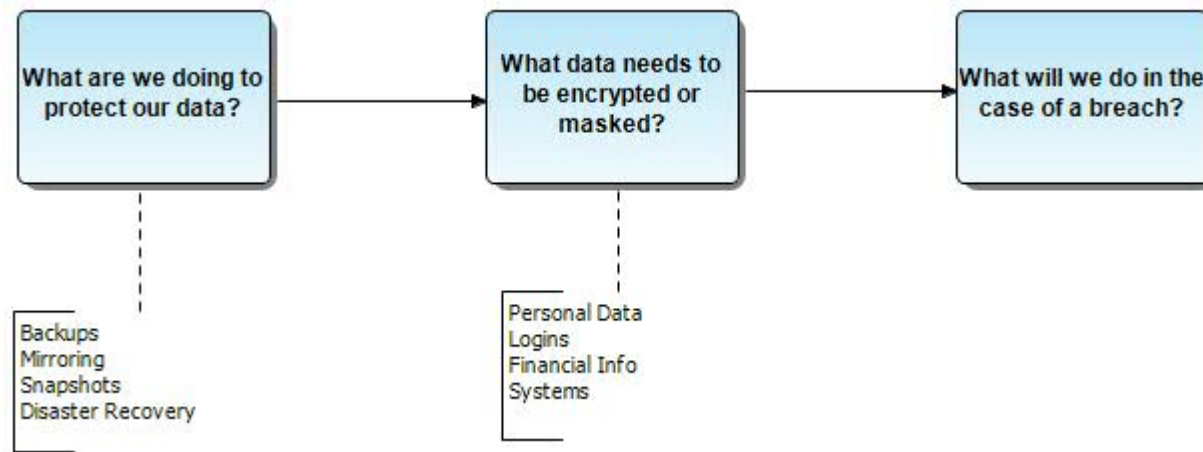
* Business Process Diagram created using ER/Studio Business Architect

ESTABLISHING SECURITY PROTOCOLS



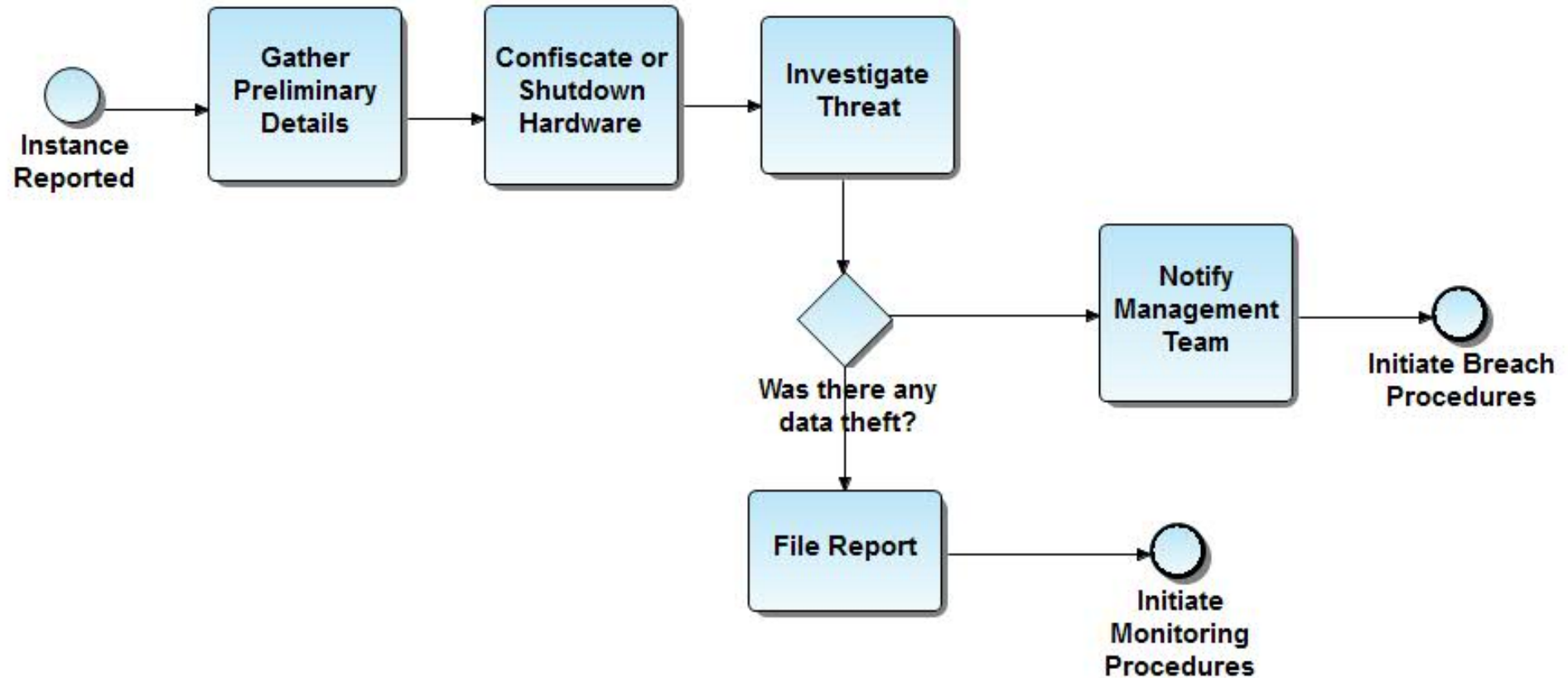
* Business Process Diagram created using ER/Studio Business Architect

DATA PROTECTION



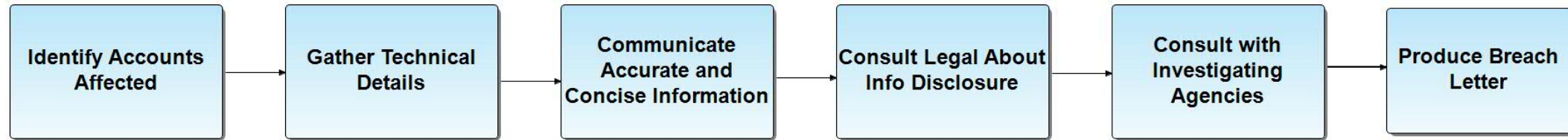
* Business Process Models created using IDERA's ER/Studio Business Architect

HOW TO RESPOND TO A BREACH



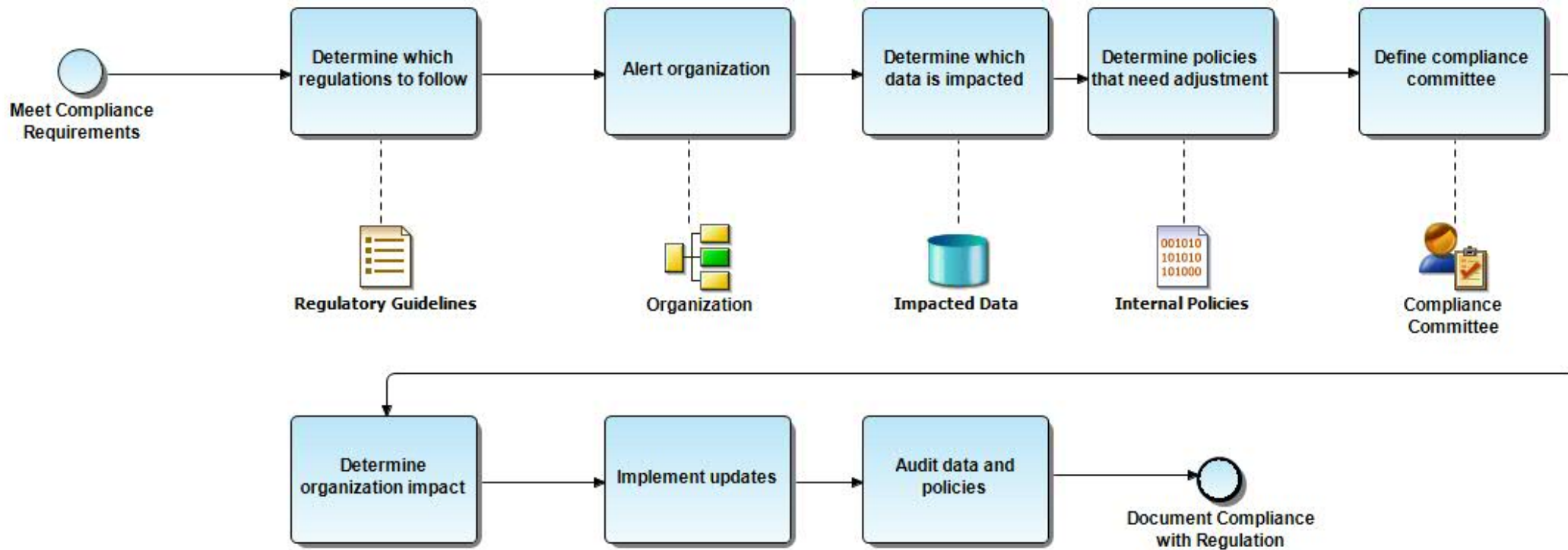
* Business Process Models created using IDERA's ER/Studio Business Architect

DATA BREACH NOTIFICATION



* Business Process Models created using IDERA's ER/Studio Business Architect

DATA COMPLIANCE



IN CONCLUSION

- Different parts of the organization need to work together like never before
- Data Protection Officers are mandatory for those adhering to GDPR
- Regulations, Data Breaches and Litigation Holds require the legal team to have more active participation with data and how it is processed
- As companies continue to acquire more data, the need will not diminish
- Business Processes are the pictures that bring everyone (business, technical, and legal) into alignment



RESOURCES

- Download a whitepaper: [Governing GDPR Challenges with Enterprise Data Architecture](#)
- Learn more about IDERA products:
 - Create business process models with [ER/Studio Business Architect](#)
 - Define your data architecture with [ER/Studio Enterprise Team Edition](#)
- See how they work:
 - Download a free trial of [ER/Studio Business Architect](#)
 - Request a live demonstration of [ER/Studio Enterprise Team Edition](#)

THANKS!

Any questions?

You can find me on Twitter via:

Kim Brushaber
@Brushaber_IDERA