13. September 2018

ITS1
Organisational it security

Security: Confidentiality, Integrity, Availability
Privacy by Design
Privacy Impact Assessment

Keld Bødker

Informatics
Computer Science

Roskilde University

Roskilde University
Keld Bødker
keldb@ruc.dk

Specific learning goals:

- Know security goals like Confidentiality, Integrity and Availability
- Know Privacy By Design, and the methods and techniques to achieve Privacy By Design
- Be able to plan a Privacy Impact Assessment for a mid-size software project
- Be able to conduct a Privacy Impact Assessment for a small software project

IT Security

1. What is the problem?

2. Who has the problem

3. Why is it a problem?

4. What to do with the problem?

Reflection

- Take a moment to reflect:
  - What do you understand to be ”security”
  - Note down 3-5 essential characteristics

Security

Definition

- The set of ***processes*** and ***technologies*** that the ***owners*** use to ***control*** which ***actors*** can ***access*** which ***resources***.

Rozanski&Woods, p.440

- Actors (principals) =
  people or software processes
- Resources = the (sensitive) parts of the system

- Computer security is the protection of the assets in computer systems (Pfleeger et al. Security in Computing. (Fifth Edition), p. 2)

Security differs

- Case by case

- No such thing as ***absolute secure or not,*** rather:
- Security is ***risk management***
  i.e. balancing security risks against cost of guarding against them or coping with the incident afterwards

  =>Trade offs

Solutions to security challenges

- Apply Recognized Security Principles

But what are

Recognized Security Principles

Recognized Security Principles

1. Grant least privilege
2. Secure the weakest link
3. Defend in depth
4. Separate privileges
5. "KISS"- keep security designs simple
6. Don't rely on obscurity
7. Use secure defaults
8. Fail securely
9. Assume externals are untrusted
10. Audit sensitive events

Rozanski&Woods, Ch. 25

Remember the “evil attacker”

Essential ingredients:

- An attack method, including
  - Knowledge, tools, education,…
- An opportunity, including
  - Time and access
- A motive,
  - A reason to attack this system

A Security Requirements Method

SQUARE

- Security Quality Requirements Engineering
- Nine-step process
- It’s not a new requirements engineering process!
- Can be used with existing requirements engineering process

SQUARE-Lite

- Five-step process (selected from the nine)

SQUARE

Who is involved?

- stakeholders of the project
- requirement engineers with security expertise

In SQUARE, security requirements are

- treated at the same time as the system's functional requirements, AND
- specified in the early stages
- specified in similar ways as software requirements engineering and practices
- determined through a process of nine discrete steps
- Quality attributes

SQUARE/SQUARE-Lite (5 out of 9 steps)

1. Agree on definitions.

2. Identify assets and security goals.

3. Develop artifacts.

4. Perform risk assessment.

5. Select an elicitation technique.

6. Elicit security requirements.

7. Categorize requirements.

8. Prioritize requirements.

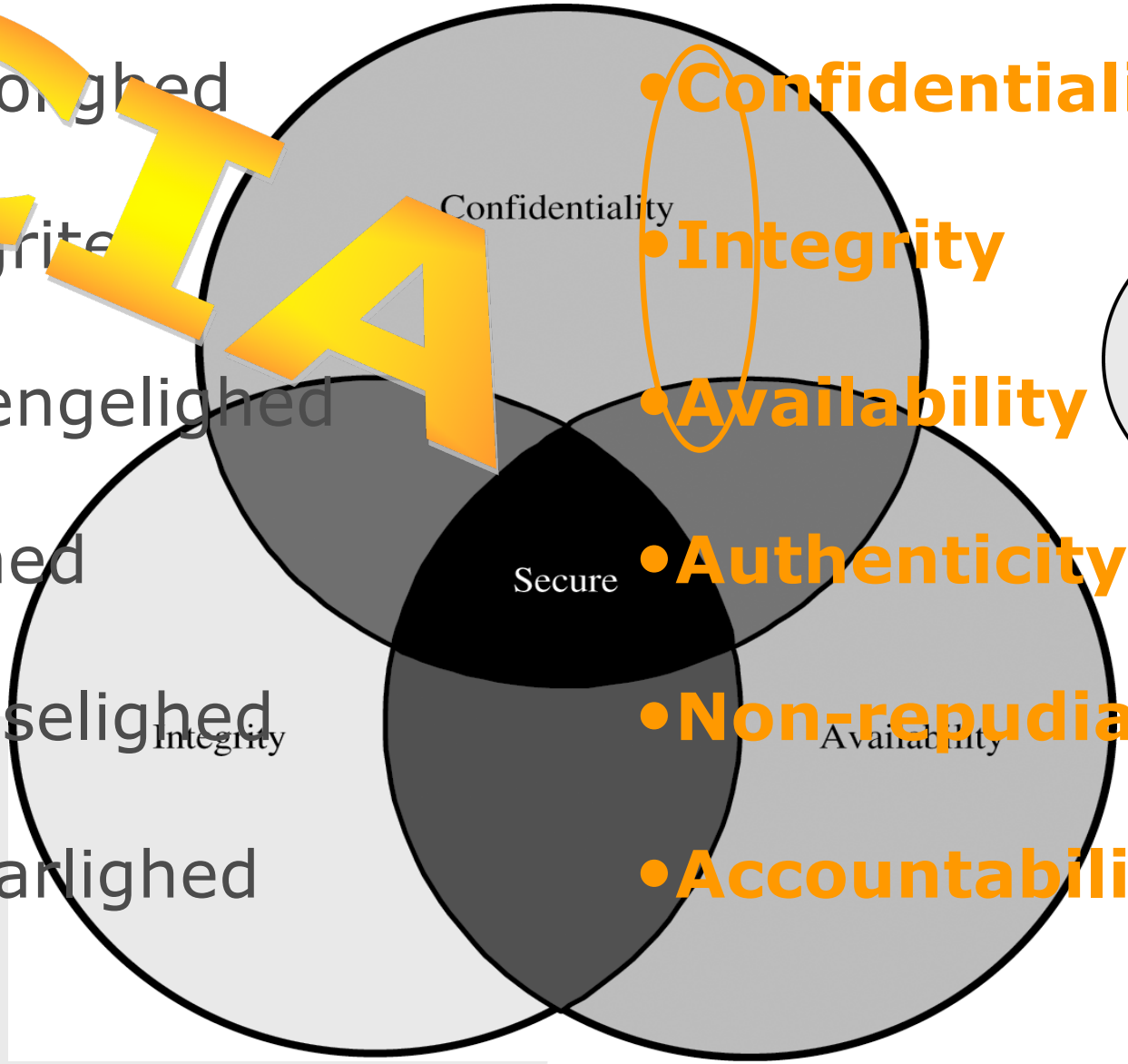
9. Inspect requirements.

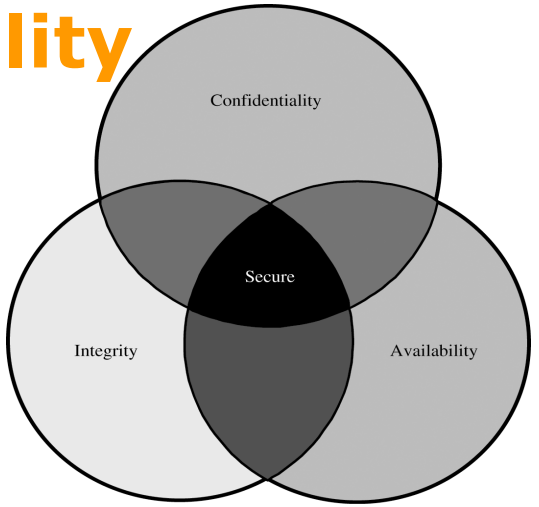
Key Security Goals

- Fortrolighed
- Integritet
- Tilgængelighed
- Ægthed
- Uafviselighed
- Ansvarlighed

CIA

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation
- Accountability





Exercise

- Security challenges with the CUTNMOVE case?

- You are assigned to the CUTNMOVE project.
- Jacob Nielsen (the owner) has said he ”wants to streamline the business”
  - Online booking
  - Receptionist making the rooster based on barber input

IT Security

We return to IT security in the ITS 2+3 lectures

For now

let's look at

Privacy in IT architecture

1. What is the problem?

2. Who has the problem

3. Why is it a problem?

4. What to do with the problem?

A Privacy Definition

- Privacy: *The right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others*
- Threats to Privacy: Government and business
  - Regime spying on citizens
  - Employee surveillance
  - Use/abuse of transaction information (or citizen records)

Fair Information Practices

- OECD (Organization of Economic Cooperation and Development) in 1980 developed the standard eight-point list of privacy principles.
  - **Limited Collection Principle**
  - **Quality Principle**
  - **Purpose Principle**
  - **Use Limitation Principle**
  - **Security Principle**
  - **Openness Principle**
  - **Participation Principle**
  - **Accountability Principle**

Comparing Privacy across oceans

- U.S. has not adopted OECD principles
- China does not protect privacy
- European Union has European Data Protection Directive (OECD principles),
  - and from May 2018 "General Data Protection Regulations" – GDPR
- EU Directive requires data on EU citizens to be protected at same standard even when it leaves their country

GDPR - "The right to be forgotten"

- GDPR - the new EU Data Regulation to supersede the Data Protection Directive
- Vivian Reading, former EU commissioner: "The right to be forgotten"
- personal data – all types of data that can be linked to an individual
- "sensitive" personal data – health, political, religion, sexual, economic,
- Control of "own data"
- Informed consent
- More on https://www.eugdpr.org (and in BUITA 8)

How to protect privacy?

Designers shall use:

- PbD
  Privacy by Design

- PIA
  Privacy Impact Assesment

- PET
  Privacy Enhancing Technology

PET – Privacy Enhancing Technology

The purpose of PET is to obtain:

- **Unobservability** – making private information invisible or unavailable to others
- **Unlinkability** – preventing others from linking different pieces of observed information together
- **Anonymity** – preventing others from connecting observed information with a specific person

PET – Privacy Enhancing Technology

- Data minimization
- Unlinkability
- Informed consent
- Virtual identities
- Anonymous credentials
- Transaction logs

Example of Challenge to Privacy:

Data mining – big data

- Privacy leakage problem

1. solution:

- Remove all identification data

2. Solution:

- Anonymize (e.g. use pseudonyms)

But:

Can de-identified data be re-identified?

PRIVACY

Credit card study blows holes in anonymity

Attack suggests need for new data safeguards

By John Bohannon

For social scientists, the age of big data carries big promises: a chance to mine demographic, financial, medical, and other vast data sets in fine detail to learn how we lead our lives. For privacy advocates, however, the prospect is alarming. They worry that the people represented in such data may not stay anonymous for long. A study of credit card data in this week's issue of *Science* (p. 536) bears out those fears, showing that it takes only a tiny amount of personal information to de-anonymize people.

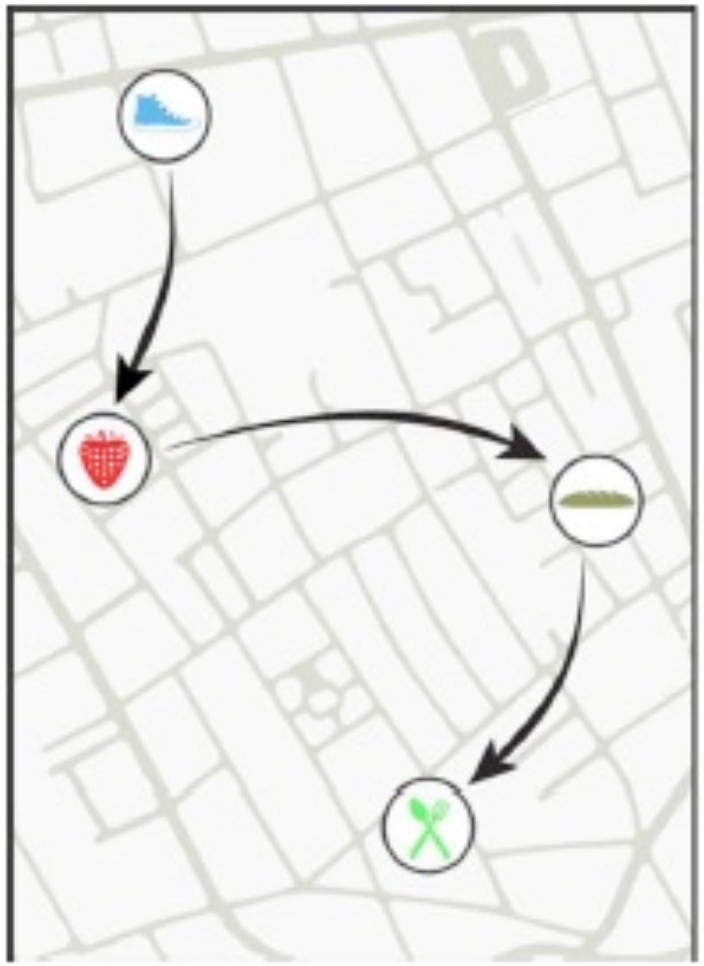
The result, coming on top of earlier demonstrations that personal identities are easy to pry from anonymized data sets, indicates that such troves need new safeguards. "In light of the results, data custodians should carefully limit access

One correlation attack became famous last year when the New York City Taxi and Limousine Commission released a data set of the times, routes, and cab fares for 173 million rides. Passenger names were not included. But armed with time-stamped photos of celebrities getting in and out of taxis—there are websites devoted to celebrity spotting—bloggers, after deciphering taxi driver medallion numbers, easily figured out the amount spent on those occasions—the equivalent of a few receipts from someone's trash—made it possible to de-anonymize nearly everyone and trace their entire transaction history with just three pieces of information per person. The findings echo the results of a 2013 *Scientific Reports* study in which de Montjoye and colleagues started with a trove of mobile phone metadata on subscribers' movements and showed that knowing a person's location on four occasions was enough to identify them.

One way to protect against correlation attacks is to blur the data by binning certain variables. For example, rather than revealing the exact day or price of a transaction, the public version of the data set might reveal only the week in which it occurred or a price range within which it fell. Binning did not thwart de Montjoye's correlation attack; instead, it only increased the amount of information needed to de-anonymize each person to the equivalent of a dozen receipts.

These studies needn't be the death knell for social science research using big data. "We need to bring the computation to the data, not the other way around," de Montjoye says. Big data with sensitive information could live "in the cloud," protected by gatekeeper software, he says. The gatekeeper

Anonymous data about 1.1 mill people shopping in 10.000 shops during 3 month



shop	user_id	time
	7abc1a23	09/23
	7abc1a23	09/23
	3092fc10	09/23
	7abc1a23	09/23
	4c7af72a	09/23
	89c0829c	09/24
	7abc1a23	09/24

- Add the equivalent of a photo with timestamp, eg. name and data
- In 9 out of 10 cases we can link to the right user_id, if the person did four purchases
- Add prices to the purchases in our dataset, and we have 95% hits.

Unique in the shopping mall: On the reidentifiability of credit card metadata

Yves-Alexandre de Montjoye,[1]* Laura Radaelli,[2] Vivek Kumar Singh,[1,3] Alex "Sandy" Pentland[1]

Large-scale data sets of human behavior have the potential to fundamentally transform the way we fight diseases, design cities, or perform research. Metadata, however, contain sensitive information. Understanding the privacy of these data sets is key to their broad use and, ultimately, their impact. We study 3 months of credit card records for 1.1 million people and show that four spatiotemporal points are enough to uniquely reidentify 90% of individuals. We show that knowing the price of a transaction increases the risk of reidentification by 22%, on average. Finally, we show that even data sets that provide coarse information at any or all of the dimensions provide little anonymity and that women are more reidentifiable than men in credit card metadata.

Large-scale data sets of human behavior have the potential to fundamentally transform the way we fight diseases, design cities, or perform research. Ubiquitous technologies

scale behavioral data sets to the invention of the microscope (*1*). New fields such as computational social science (*2*–*4*) rely on metadata to address crucial questions such as fighting malaria, study-

So …

- What are the lessons learned from this example?

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

PbD – Privacy by Design – 7 principles

1. ***Proactive*** **not Reactive;** ***Preventative*** **not Remedial**
2. **Privacy as the** ***Default Setting***
3. **Privacy** ***Embedded*** **into Design**
4. **Full Functionality –** ***Positive-Sum*****, not Zero-Sum**
5. **End-to-End Security –** ***Full Lifecycle Protection***
6. ***Visibility*** **and** ***Transparency*** **– Keep it** ***Open***
7. ***Respect*** **for User Privacy – Keep it** ***User-Centric***

1. Proactive not Reactive; Preventative not Remedial

- The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures.
- It anticipates and prevents privacy-invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.
- In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the Default Setting

- We can all be certain of one thing – the default rules!
- Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice.
- If an individual does nothing, their privacy still remains intact.
- No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. Privacy Embedded into Design

- Privacy is embedded into the design and architecture of IT systems and business practices.
- It is not bolted on as an add-on, after the fact.
- The result is that it becomes an essential component of the core functionality being delivered.
- Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum

- Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.
- Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security – Full Lifecycle Protection

- Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish.
- This ensures that at the end of the process, all data are securely destroyed, in a timely fashion.
- Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency – Keep it Open

- Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact operating according to the stated promises and objectives, subject to independent verification.
- Its component parts and operations remain visible and transparent, to users and providers alike.
- Remember – "trust but verify."

7. Respect for User Privacy – Keep it User-Centric

- Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by
  - offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.
  - Keep it user-centric.

PIA – Privacy Impact Assesment

Key Points

- A PIA is a process which assists organizations in identifying and minimizing the privacy risks of new projects or policies.
- Conducting a PIA involves working with people within the organization, with partner organizations and with the people affected to identify and reduce privacy risks.
- The PIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Conducting a PIA should benefit organizations by producing better policies and systems and improving the relationship between organizations and individuals.

Why PIA ?

- Individuals can be reassured that the organizations that use their information have followed best practice
- Transparency enables individuals to better understand how and why their information is being used
- Organizations will improve how they use information which impacts on individual privacy. Thus reduce the likelihood of the organization failing to meet its legal obligations
- Build trust

The PIA process - overview

1. Identify the need for a PIA
2. Describe the information flows
3. Identify the privacy and related risks
4. Identify and evaluate the privacy solutions
5. Sign off and record the PIA outcomes
6. Integrate the outcomes into the project plan
7. Consult with internal and external stakeholders

1. Identifying the need for a PIA

- The need for a PIA can be identified as part of an organization's usual project management process or by using the screening questions
  - Explain what the project aims to achieve, what the benefits will be to the organization, to individuals and to other parties
  - link to other relevant documents, eg. a project proposal
  - Answering the screening questions

Screening questions-Privacy impact assessment

Is a PIA necessary for your project?

Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?

Screening questions-Privacy impact assessment

- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

Screening questions-Privacy impact assessment

- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

PIA step 1

- Screen CUTNMOVE – using the 8 PIA screening questions.

2. Describing the information flows

- Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information

The information flows

- The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.
- You should also say how many individuals are likely to be affected by the project.

- What are the information flows in the system you are designing in your project?

3. Identifying the privacy and related risks

- Some will be risks to individuals – for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.
- Some risks will be to the organization - for example damage to reputation, or the financial costs or a data breach.
- Legal compliance risks include the GDPR, and the Human Rights Act.

The privacy and related risks

- Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.
- Annex three can be used to help identify the DPA related compliance risks

Privacy issue	Risk to individuals	Compliance risk	Associated organization / corporate risk

4. Identifying and evaluating privacy solutions

- Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.
- Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

Privacy solutions

- Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the Risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

5. Signing off and recording the PIA outcomes

- Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.
- A PIA report should summarize the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.
- Publishing a PIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

Sign off and record the PIA outcomes

- Who has approved the privacy risks involved in the project?
- What solutions need to be implemented?

Risk	Approved solution	Approved by

6. Integrating the PIA outcomes back into the project plan

- The PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.
- A PIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.
- Record what you can learn from the PIA for future projects.

Integrate the PIA outcomes back into the project plan

- Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork?
- Who is responsible for implementing the solutions that have been approved?
- Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

7. Consult with internal and external stakeholders

- Consultation is an important part of a PIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise.
- Consultation can take place at any point in the PIA process.
- Internal consultation will usually be with a range of internal stakeholders to ensure that all relevant perspectives are taken into account.
- External consultation provides the opportunity to get input from the people who will ultimately be affected by the project and to benefit from wider expertise.

Consultation requirements

- Explain what practical steps you will take to ensure that you identify and address privacy risks.
- Who should be consulted, internally and externally?
- How will you carry out the consultation? You should link this to the relevant stages of your project management process.
- Consultation can be used at any stage of the PIA process.

End of BUITA 4 lecture

Specific learning goals:

- Know security goals like Confidentiality, Integrity and Availability
- Know Privacy By Design, and the methods and techniques to achieve Privacy By Design
- Be able to plan a Privacy Impact Assessment for a mid-size software project
- Be able to conduct a Privacy Impact Assessment for a small software project