Information Security for the Business Analyst

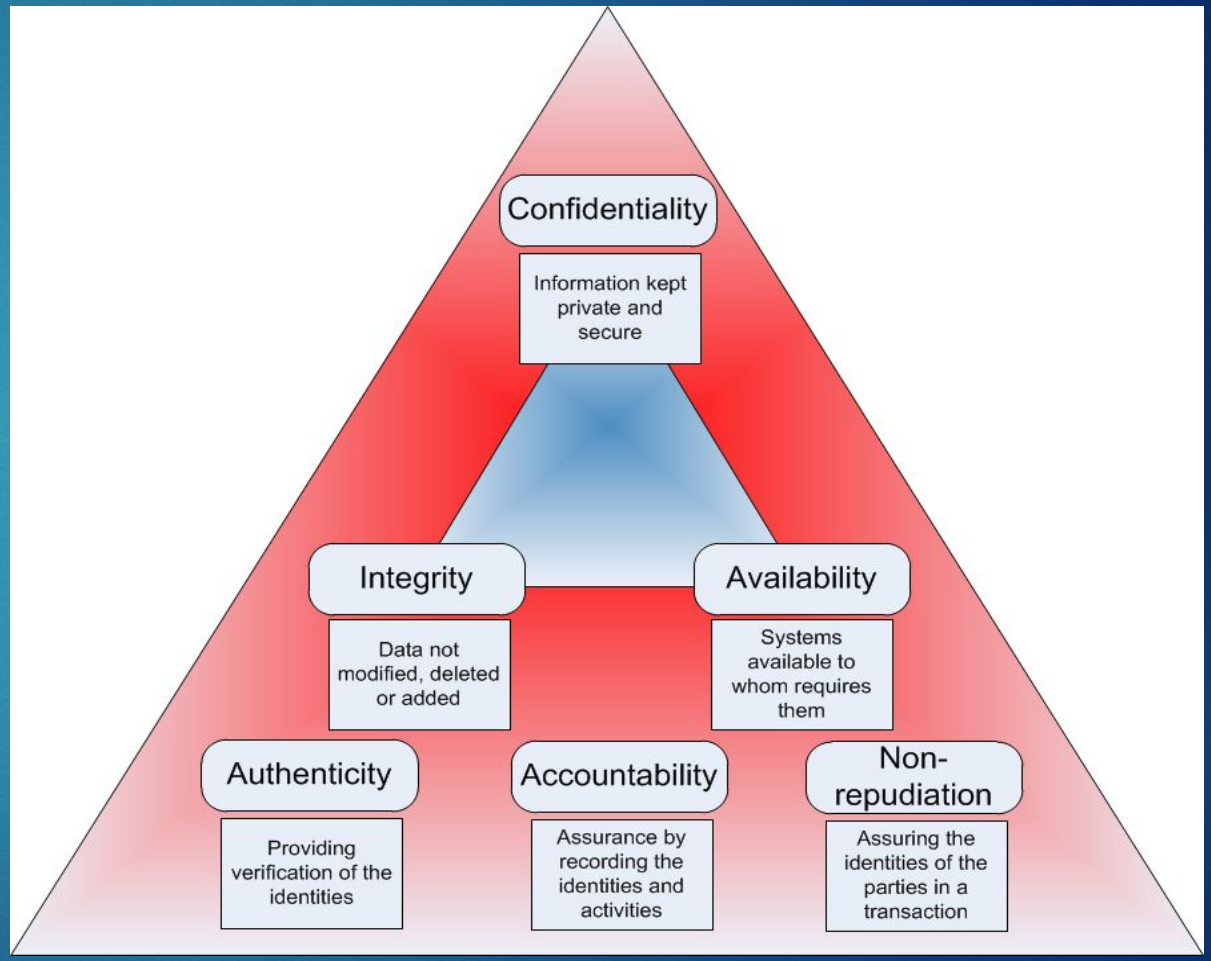
HOW CAN YOU MAKE A DIFFERENCE?

CIA – the Fundamentals

- No, I don't mean *that* calibre of security. (for most of us, anyway)
- We're talking about Confidentiality, Integrity, and Availability
- You also have the inverse, from the "dark side": DAD, or Dislcosure, Alteration, and Denial (of service).

The User Angle

- This is comprised of: Authenticity, Accountability, and Non-repudiation
- Each is centred around the fundamentals of IDENTITY (User ID)
- They are all intertwined with CIA



Functional & Non-Functional aspects of security

Functional aspects

- Provide authorization based on roles in a given context
- Provide status messaging (error, confirmation, warning) based on security related actions.

Non-functional aspects

- Acceptable hours of operation, distinctions like peak or off-peak hours
- Audit logging, i.e. for non-repudiation, also known as system *accounting*
- Availability thresholds (this may be linked to an SLA or SLO)

Solutions vs. Requirements

Don't say…

- Asymmetric encryption
- A Host-based Intrusion Detection System (HIDS)
- Retina scan and token ID card

Instead say:

- The system shall ensure non-repudiation of the users involved.
- The system shall be able to detect unauthorized users attempting to access endpoints.
- The system shall enforce 2-factor authentication.

Where does the BABOK come in?

- 7.4: Requirements Architecture:
  - A possible viewpoint is that of audit and security.
  - This may have different model notations and techniques than other views.
- 10.1: Techniques: Acceptance and Evaluation Criteria
  - **Security** may be an evaluation criteria.
  - These can be used to: Approve requirements (5.5), Define future state (6.2), and are used in the majority of Requirements Analysis & Design Definition (KA 7) and Solution Evaluation (KA 8)
- 10.15: Data Modelling
  - Such as, only one approver for many types of access requests

BABOK continued…

- 10.30: Non-functional requirements analysis (NFA)
  - Security must be considered in the context of an organization (unit)
  - Be mindful of inherent trade-offs with other NFAs, such as performance or usability
- 10.39: Roles and permissions matrix
  - Functions or roles are in the columns; activities or tasks are in the rows.
  - We'll see one of those on the next slide
- 10.47: Use Cases
  - You may have to satisfy post-conditions that security, or data integrity, is upheld.
- 10.49: Vendors:
  - Need I say more? (tighten up those RFIs, people!)

Functional Roles Matrix (FURM)

FURM	Role	Client Rep	Adjuster	Manager	Reg'l Coordr.
Activity					
Maintain Contracts		R, S, W	R, S, W, U	R, A, D	R, S, W, U
Modify Account			X	X	
Assign Work				X	X
Create User					X
Maintain Report		R, W, U	R, W, U	R, W, A, D	R

- For specific activities, you put an 'X' in the box of the acceptable role.
- For more general activities ("*Maintain* entity"), use a *distinct letter* e.g.:
  - R = Read, S = Search, W = Write, U = Update, A = Approve, D = Decline
- Typically, these letters appear in order of least rights to higher rights.

Seg. Of Duties (SoD)

- Basic Principle: not allowing users to perform two different duties which may be in conflict. Such as:
  - The right to create expenses, and approve them;
  - The right to cut cheques in the system, and change the recipient info
  - The right to conduct business duties, and IT functions.
- Supporting SoD, you have:
  - GRC, or *Governance, Risk & Compliance*; at the strategic-tactical level, this is the framework for the ongoing evaluation of risk vis-à-vis SoD
  - CCM, or *Continuous Controls Monitoring*; this is the ongoing checks for permissions that may be in conflict (at the tactical-operational level)

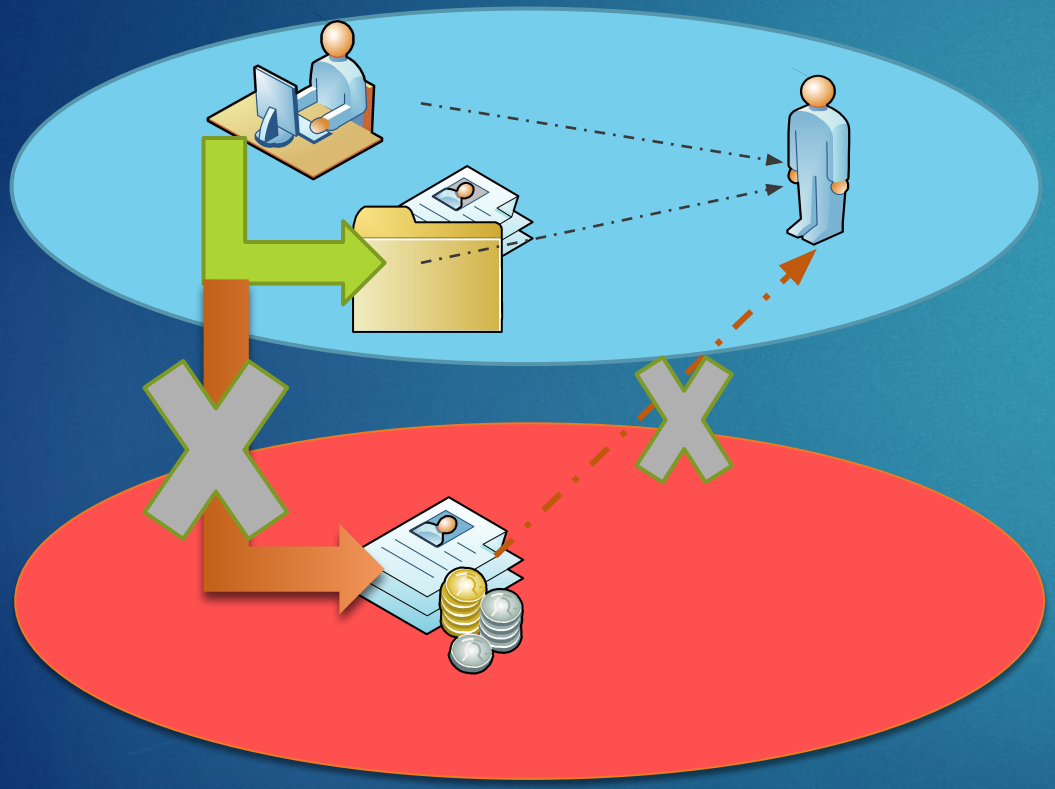
What are some SoD examples?

- Expense entering & Expense approvals
- Development & Administration (or Operations)
- Asset Custody & Asset Inventory
- Payments (or paycheques) and Bank Reconciliation
- Vendor Maintenance & Posting Invoices
- Master Data & Transactional abilities (like creating a fake customer, then…)
- Other…?

Process Cycle and SoD: the time dimension

- Or rather, the timing of function role changes as a business process is still in progress.
- Let's say that a basic user gets a lateral job change from procurement to accounts payable.
- Then the user's history should preclude them from making payments on accounts that they previously purchased from.
- Or, let's say that a line worker got promoted to supervisor – they should be barred from approving any of their previous work.

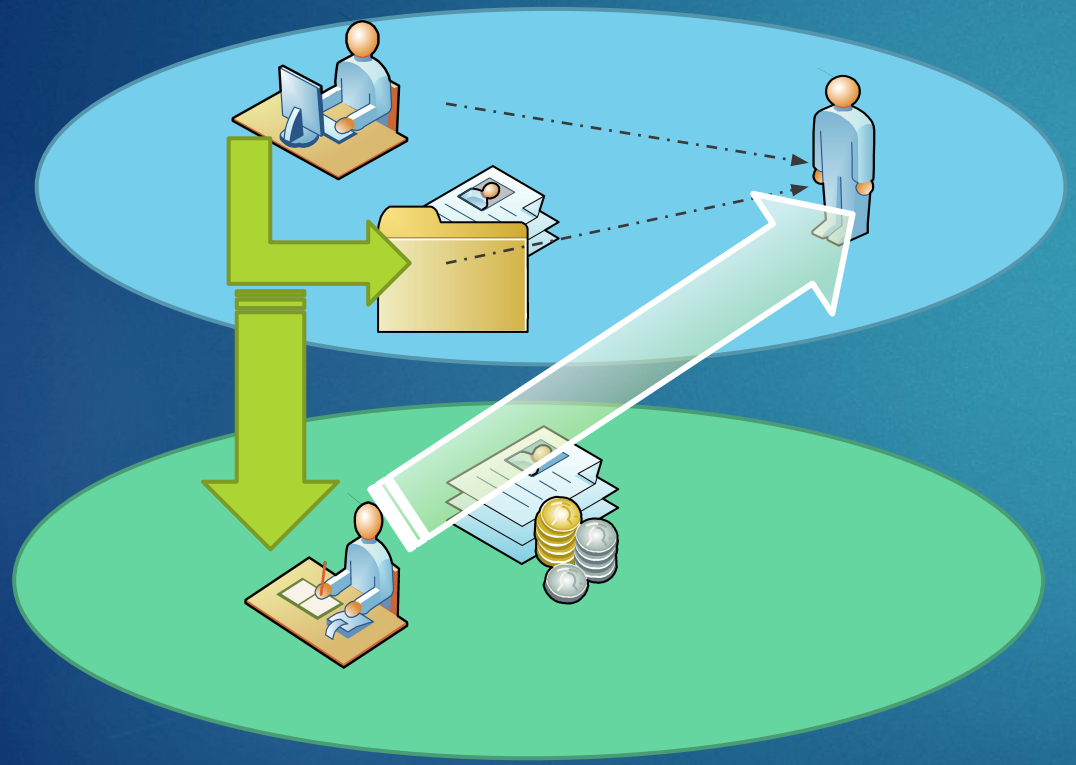
Sample Scenario



So, Jim in HR approves the hire of David Jones. So far so good right?

Ahh…but what you *didn't* know was that Dave is a good buddy of Jim's, so Jim inputs Dave's compensation as $10K above the salary band limit.

What could have been done differently (on scenario)



OK, now it's legitimate. Jim passed it on to someone in payroll who created acceptable compensation in Dave's new employee file.

Because Jim didn't have the role to create payroll records!

The “Super User” role – Beware!!

- This should be used for only a select number of individuals who are ONLY engaged in Admin functions.
- It is common for a web portal, using an Identity Manager tool.
- It can be a tricky concept, because in theory you can use any role you possess – not just assign those roles.
- As part of checks and balances, it is imperative to maintain an audit log to record all SU actions.

BI/Reporting Requirements for Info Security

- This will usually consist of dimensional elements, such as:
  - Org Unit
  - Problem Type / Access Type
  - Status of request / of user
- Proactive warning measures may be:
  - Irregular level of rejected requests in a given period of time
  - Rapid changes of assigned duties in a short time frame
  - Several unsuccessful access attempts from same address

This concludes the presentation…

ARE YOU CURIOUS TO KNOW MORE?