Implementing cloud solutions securely: How to get risk and compliance out of the way

Lenka Fibikova

Cloud solutions in the corporate environment

Why do we like them?

- Fast deployment
- High availability of the service and data
- Accessing the service from everywhere
- Avoiding fights for the limited IT resources in the organization

Why should they worry us?

- Who has access to the service and to the company data?
- Where is the company data?
- Do we comply with legal and regulatory requirements?
- Is the provider capable to respond to the company's need on the long term?
- Will we be able to change the provider if no more satisfied, and how?
- Are we able to integrate the new solution with other corporate solutions?

Cloud solutions and shadow IT

Shadow IT: IT systems and solutions built and used in an organization without being approved or supported by the organization's IT department

What did use to worry us?

- Servers placed in the office premises (physical security)
- No hardening, no patching, no updates, no malware protection (IT security)
- Often an own modem connection to the company's infrastructure (IT security)
- No backup, no redundant HW, no redundant power supply (IT service continuity)

Mostly IT problems

What does worry us today?

- Unclear access to the data and the service (access control)
- Unknown location of the company data (data security)
- Local legal and/or regulatory requirements (compliance)
- Further development of the solution and/or exit from the provider (service)
- Integration with the corporate solutions

Mostly business problems

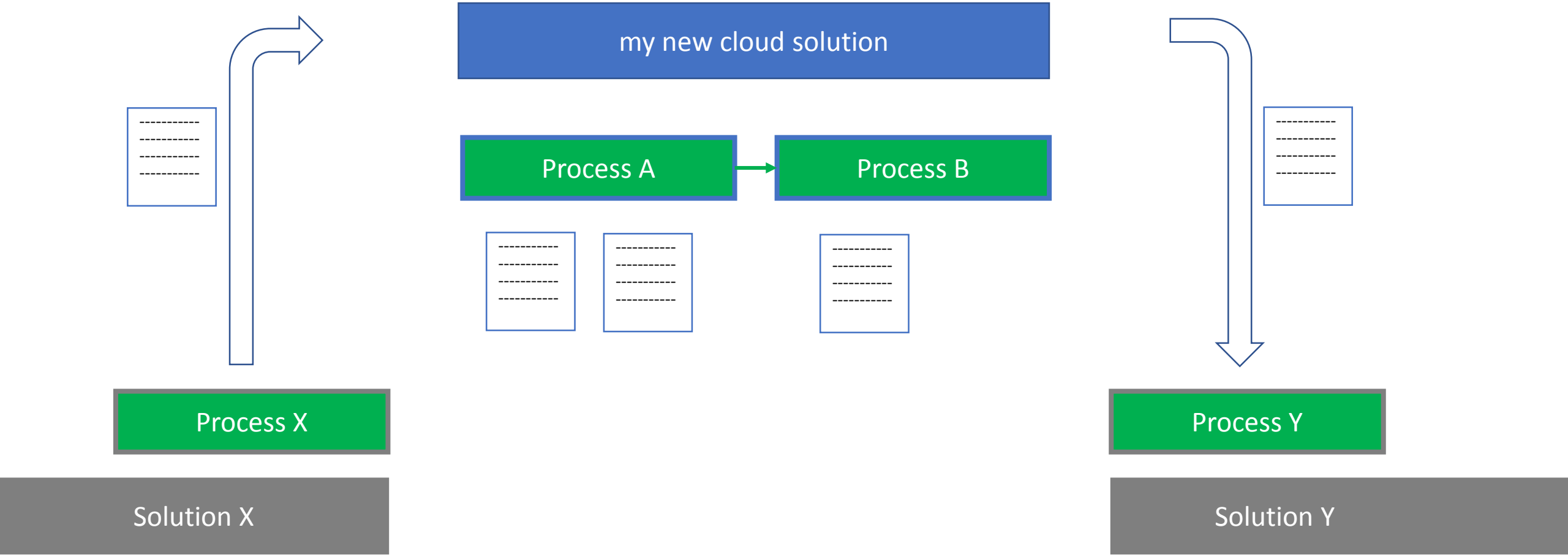
How to get risk and compliance out of the way?

Do the due diligence…

… and address the 5 worries

- Integration
- Compliance
- Data security
- Access Control
- Service

Integration



Compliance

What data will be stored in the cloud?

- Personal data → see your **Data Protection Officer**
- Financial data relevant for financial reporting → see your **Compliance**
- Credit card information → see your **Compliance**
- Company confidential data → see your **Information Security Officer**

Protecting data

- Data location
  - White-listing
  - Black-listing
- Data Ownership
  - Providing data to 3rd parties
- Data availability
  - Data feeds
  - Regular reports and data sheets
  - Overall data set extract
  - Archiving
- Data confidentiality
  - Encryption of data in transfer
  - Encryption of data at rest
  - Key management
- Data integrity
  - Input/output validation
  - Data reconciliation and edit checks
  - Handling interrupted operations

Access control

- Access to the service (1st line of defense)
  - All devices vs.
  - Only approved devices (company-owned and BYOD)
- Identity Management (2nd line of defense)
  - Own identities vs.
  - Single-sign-on
- Authentication (3rd line of defense)
  - Following best practices
  - Using 2-factor authentication admin
- Authorization (4th line of defense)
  - Role-based vs.
  - Individual entitlements
  - Need to know
  - Least privilege
  - Segregation of duties

Service: Service Provider

- IT security at the provider
  - ISO 27001 certifications
  - Annual external IT security audit report
  - Checklist with requirements and grade of fulfillment
- Compliance
  - External certification/audit confirming fulfillment of requirements
- Change management
  - Changes initiated by the provider
  - Changes initiated by the customer
  - Prioritization of customer changes
- Incident Management
  - Incidents at the service provider
  - Incidents within the organization
  - Support of law enforcement

Service: Customer’s side

- Right to audit
  - Scope
  - Time
  - Other conditions
- Business continuity (if the service is not available)
  - Criticality of the service
  - Data needed
  - Alternative ways of execution
- Exit strategy
  - Ownership of data
  - Data return (processes, formats, migration support)
  - Proper data deletion
  - Solution migration

Do you still want them to get out of your way?

As a service provider

- Do your homework
- Provide information and evidence about it
- Ask your customer whether they have internal requirements

As a deployer

- Ask a lot of questions
- Require evidence
- Know when and where to ask for help internally

As a compliance officer

- Provide necessary requirements as checklists
- Provide timely support

As an auditor

- Consider integrated audits

Thank you!