Improve IT Projects through Audits

Jörg Meyer

Zeewolde, August 2017
Improve IT Projects through Audits

Objective:

- At the end of this presentation you will know how audits can improve IT projects, what the challenges and typical observations are, how to prepare an audit, select the scope, select the team and conduct the audit.
Improve IT Projects through Audits

Agenda

- IT Projects / Start-up Businesses
- What to look out for
- Types of Controls
- How to do an audit
- Practical Examples and Recommendations
- Next Steps
What do IT projects and many start-up businesses have in common?

- Goal to develop and operate a Web-based platform
- 30 team members or less
- Distributed team and resources
- Few processes and controls
- Product sometimes not more than a demonstrator
- External services necessary to run operation
- Organization too small for regular audit
Improve IT Projects through Audits

**Agenda**

- IT Projects / Start-up Businesses
- What to look out for
- Types of Controls
- How to do an audit
- Practical Examples and Recommendations
- Next Steps

29. Januar 2017
Improve IT Projects through Audits

IT Projects / Start-up Businesses

- What can be looked at?
  - Development planning
    - A holistic view of the undertaking.
  - Server access controls
  - Customer data
  - Test data
  - Penetration Testing
  - Software libraries
  - Zero Day Exploits
  - DMZ Configuration
  - External Access
  - Data protection
    - Software versions
    - Free lancers
    - Acceptance testing
  - Service Provider
    - Source code repositories
    - Emergency plans
  - Ticketing systems
  - Coding habits

29. Januar 2017

SHA2017
IT Projects / Start-up Businesses

- What will typically **not** be looked at?
  - Platform content
  - Financial performance
  - Business model
  - Staff administration

- These are subjects of other types of audits.
Audit Scope Example
Improve IT Projects through Audits

Agenda

- IT Projects / Start-up Businesses
- What to look out for
- Types of Controls
- How to do an audit
- Practical Examples and Recommendations
- Next Steps

29. Januar 2017

SHA2017
What is Audit?

- **External Audit**
  - Statutory, annual audits
  - Focus on correctness of financial performance reporting
  - Mandatory audits required by industry or government

- **Internal Audits**
  - Processes and controls (existence and quality)
  - Effectiveness and application of processes and controls
The different types of controls

Preventive Controls
- Make sure that something unwanted doesn't happen.
- Example: user accounts and passwords
- Example: authorization levels

Detective Controls
- You can't prevent everything. Make sure things gets detected.
- Detect errors before damage happens or at least early.
- Example: log file reviews
Improve IT Projects through Audits

Agenda

- IT Projects / Start-up Businesses
- What to look out for
- Types of Controls
- How to do an audit
- Practical Examples and Recommendations
- Next Steps
Improve IT Projects through Audits

How to prepare and perform an audit

Preparation

- Define subjects to look at („Scope“)
- Define quality expectations („What is good?“)

Conduct

- Team members to be independent of audited project
- Separate observations from evaluations
- Verify understanding
Improve IT Projects through Audits

Agenda

- IT Projects / Start-up Businesses
- What to look out for
- Types of Controls
- How to do an audit
- Practical Examples and Recommendations
- Next Steps
Improve IT Projects through Audits

What can you find out there? (#1)

- Coordination and collaboration
  - “Agile” teams with ticketing portal, no other means of documentation.
  - Fluctuations in the team without proper on-boarding.
  - No „Definition of Done“. What does „good“ look like?
  - No accepted way to measure progress and completion.
  - Readiness to accept ready-made big modules when only a small part is needed. Loss of oversight and crazy dependencies.
  - Evaluate: Make vs. Buy vs. Make again, but better.

29. Januar 2017

SHA2017
What can you find out there? (#2)

- Coding and sources
  - Design decisions can be biased.
  - Sticking with outdated concepts or libraries for too long.
  - Diversified technology, too many different tools/languages. Thinned out knowledge/experience.
  - Git server (local, GitHub or BitBucket) with decentralized administration. Lots of unstructured repositories with little or no overview. Access to repos never coordinated or reviewed.
  - Some automated testing, but not enough.
What can you find out there? (#3)

- Operations
  - Test data is not sufficiently sanitized/randomized.
  - Servers not properly grouped and secured (DMZ), especially not when virtual and Cloud-based.
  - Too few admin accounts on production machines.
  - People sharing too few accounts and passwords, especially external team members.
  - Traceability/accountability is less than what would be necessary.
  - No emergency procedures or never tested.
Improve IT Projects through Audits

Agenda

- IT Projects / Start-up Businesses
- What to look out for
- Types of Controls
- How to do an audit
- Practical Examples and Recommendations
- Next Steps
What to check and do next? (#1)

- Development
  - Document design decisions, challenge decisions from time to time.
  - Define toolset, ascertain enough experience with tools.
  - Define quality expectations. What does „good“ look like? What gets reviewed? How much testing is required?
  - Enough different user accounts, enough good passwords.
What to check and do next? (#2)

- **Operations**
  - Structure services onto machines. Segregate security zones.
  - Review test documentation, traceability and accountability.
Improve IT Projects through Audits

What to check and do next? (#3)

Report
- Write an audit report.
- Document what was looked at and what not.
- Document findings and recommendations.
- Negotiate improvements with audited project.
- Review after selected intervals to evaluate progress.
Improve IT Projects through Audits

Professional Organizations

- Global Institute of Internal Auditors (IIA)
- European Confederation of Institutes of Internal Auditing (ECIIA)
- Instituut van Internal Auditors Nederland (IIA NL)
- Deutsches Institut für Interne Revision e.V. (DIIR)

Jörg Meyer, joerg.meyer@jogisoft.de