🔍 Audit Fundamentals

Defining Scope, Requirements, IT Security & Information Gathering

Making audits less scary, one meme at a time 😅

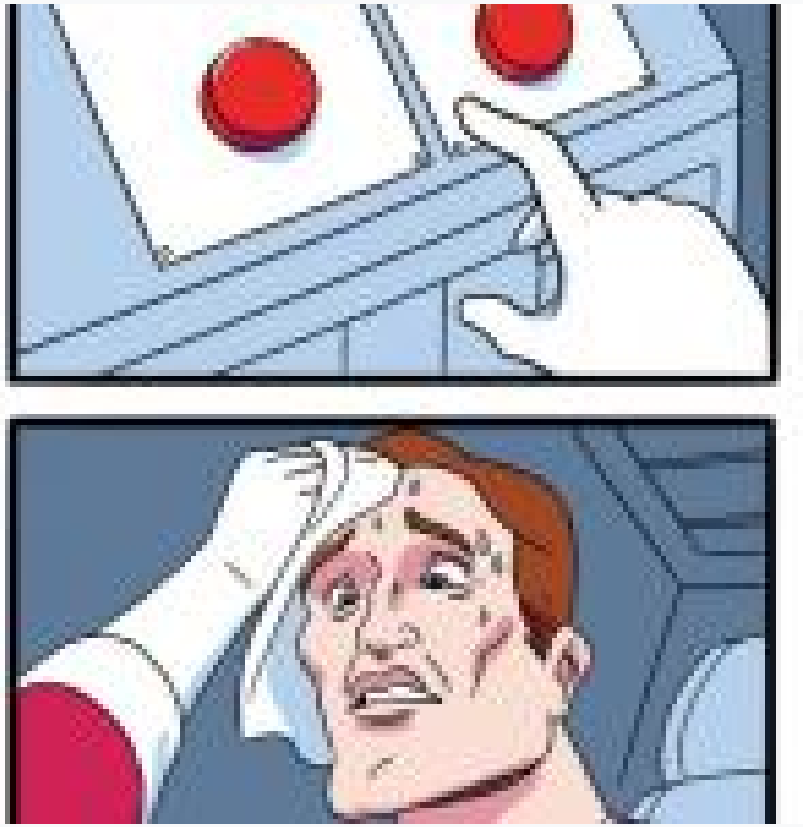
🎯 Defining the Scope for Audit

What is Audit Scope?

Scope = What you're actually going to audit

- Time period (FY 2024? Last quarter?)
- Business units (Finance? HR? IT?)
- Processes (Procurement? Payroll?)
- Systems (SAP? Salesforce?)

"Scope creep is real, folks!" 📈



🚧 Scope Definition: The Good, Bad & Ugly

✅ Good Scope

- "*Audit accounts payable processes for Q1-Q3 2024*"

❌ Bad Scope

- "*Audit everything financial*"

💀 Ugly Scope

- "*Just check if we're compliant*"

Meme Alert: "*That escalated quickly*" - *when scope goes from 2 weeks to 6 months*

📋 Case Study: TechCorp Scope Disaster

The Situation

- **Initial Request**: "Quick IT audit for compliance"
- **What Really Happened**:
  - Started with network security
  - Expanded to data governance
  - Added vendor management
  - Included disaster recovery
  - Threw in some GDPR compliance

The Result

- 3-month audit became 18 months
- Budget: 300% over
- **Lesson**: Define boundaries early! 🚨

🎯 SMART Scope Framework

Specific	What exactly are we auditing?
Measurable	How will we measure success?
Achievable	Can we realistically do this?
Relevant	Does this matter to the business?
Time-bound	When does this need to be done?

"SMART goals are like GPS for auditors" 🗺️

🔍 Identifying Critical Requirements

Types of Requirements

Regulatory Requirements

- SOX, GDPR, HIPAA, PCI-DSS
- Industry standards (ISO 27001, NIST)

Business Requirements

- Risk tolerance
- Operational needs
- Compliance deadlines

Technical Requirements

- System access
- Data availability
- Tool requirements

📊 Requirements Prioritization Matrix

High Impact	Medium Impact	Low Impact
High Urgency	🔥 Critical	⚡ Important
Medium Urgency	⚡ Important	📝 Monitor
Low Urgency	📝 Monitor	📋 Nice-to-have

"This is fine" dog sitting in fire = ignoring critical requirements

🏦 Case Study: FinanceFirst Requirements Fail

The Problem

FinanceFirst ignored critical SOX requirements while focusing on minor process improvements.

The Impact

- $2.3M in penalties
- 6-month compliance extension
- CEO resignation
- Stock price dropped 15%

The Lesson

Critical requirements aren't suggestions! ⚠️

"Priorities: Because everything can't be urgent"

Assessing IT Security

The CIA Triad

Confidentiality

- Who can access what?
- Data classification
- Access controls

Integrity

- Is data accurate?
- Change management
- Data validation

Availability

- Can users access when needed?
- Uptime requirements
- Disaster recovery

🔐 IT Security Assessment Framework

Technical Controls

- Firewalls, encryption, antivirus
- Access management systems
- Monitoring tools

Administrative Controls

- Policies and procedures
- Training programs
- Risk assessments

Physical Controls

- Building security
- Server room access
- Device management

"*Security is like an onion - it has layers, and it makes you cry*" 🧅

🚨 Real-World Security Horror Stories

Case 1: RetailCorp USB Incident

- Employee found USB in parking lot
- Plugged into work computer
- Ransomware infected entire network
- **Cost**: $4.2M, 3 weeks downtime

Case 2: HealthSystem Password Crisis

- Default passwords never changed
- "password123" on critical systems
- Data breach: 50,000 patient records
- **Cost**: $12M in fines + lawsuits

"*I don't always test security, but when I do, I do it in production*" 🤦

🔍 Security Assessment Checklist

Network Security

- [ ] Firewall configurations
- [ ] VPN security
- [ ] Network segmentation
- [ ] Intrusion detection

Access Management

- [ ] User provisioning/deprovisioning
- [ ] Privileged access reviews
- [ ] Multi-factor authentication
- [ ] Password policies

Data Protection

- [ ] Encryption at rest/transit
- [ ] Data classification
- [ ] Backup procedures
- [ ] Data retention policies

📊 Obtaining Information: The Art of Audit Intelligence

Information Sources

Primary Sources

- System reports
- Financial records
- Process documentation
- Direct observations

Secondary Sources

- Prior audit reports
- Vendor assessments
- Industry benchmarks
- Regulatory guidance

🕵️ Information Gathering Techniques

Interviews

- Structured questionnaires
- Open-ended discussions
- Follow-up sessions

Documentation Review

- Policies and procedures
- System configurations
- Change logs
- Exception reports

Testing & Sampling

- Walkthrough tests
- Statistical sampling
- Substantive testing
- Automated analytics

"*Trust, but verify*" - *The auditor's motto* ✅

📈 Case Study: CloudTech Information Gold Mine

The Challenge

CloudTech had 47 different systems with no central documentation.

The Solution

- **Week 1**: System inventory mapping
- **Week 2**: Key user interviews
- **Week 3**: Automated data extraction
- **Week 4**: Cross-validation of findings

The Result

- Found 12 critical control gaps
- Identified $800K in duplicate licensing
- Reduced audit time by 40%

Key Learning: *Good information gathering is half the audit!*

🎭 Information Gathering: Expectations vs Reality

Expectations

"We'll just pull some reports and review documentation"

Reality

- Systems are down during extraction
- Documentation is from 2019
- Key person is on vacation
- Reports don't match actual processes
- Excel files are password protected
- Nobody knows who owns what

"*Fine, I'll do it myself*" - *Thanos (every auditor ever)*

🛠️ Information Gathering Tools & Techniques

Technology Tools

- **ACL/IDEA**: Data analytics
- **TeamMate**: Audit management
- **Power BI**: Data visualization
- **Python/R**: Custom analytics

Traditional Methods

- Process walkthroughs
- Observation sessions
- Document requests
- Survey questionnaires

Modern Approaches

- API integrations
- Continuous monitoring
- RPA for data collection
- AI-powered analytics

⚠️ Common Information Gathering Pitfalls

The "Too Much Information" Problem

- Drowning in data, starving for insights
- 500 GB of logs, but what do they mean?

The "Not Enough Information" Problem

- Key reports missing
- Access restrictions
- "We don't track that"

The "Wrong Information" Problem

- Outdated documentation
- Mismatched data sources
- Sample bias

"*Information without context is just noise*" 📢

🎯 Putting It All Together: The Audit Recipe

Step 1: Define Clear Scope

"What are we actually doing here?"

Step 2: Identify Critical Requirements

"What absolutely must be checked?"

Step 3: Assess IT Security

"How secure are we really?"

Step 4: Gather Quality Information

"Show me the data!"

Remember: *Garbage in = Garbage out* 🗑️➡️🗑️

💡 Pro Tips for Audit Success

For Scope Definition

- Start small, expand if needed
- Get written approval for scope changes
- Document assumptions clearly

For Requirements

- Map to business objectives
- Validate with stakeholders
- Keep compliance matrix updated

For IT Security

- Think like an attacker
- Test controls, don't just read about them
- Consider emerging threats

For Information Gathering

- Multiple sources for validation
- Document everything
- Build relationships with key contacts

 Final Audit

"When you successfully complete an audit on time and under budget"

"Is it possible to learn this power?"

"Not from a junior auditor..."

📚 Key Takeaways

Remember the 4 Pillars

1. **Scope**: Clear boundaries save time and sanity
2. **Requirements**: Critical vs nice-to-have
3. **IT Security**: Assume breach, verify everything
4. **Information**: Quality over quantity

The Golden Rule

"An audit is only as good as its planning"

Questions? Let's discuss! 🙋‍♀️🙋‍♂️

📖 Additional Resources

Standards & Frameworks

- COSO Internal Control Framework
- ISO 27001/27002
- NIST Cybersecurity Framework
- PCAOB Auditing Standards

Tools & Technology

- Audit management software
- Data analytics platforms
- Security assessment tools
- Documentation management systems

"*The best auditor is a prepared auditor*" 🎯

Thank you! 👏