

Passing Audits with Compliance Reports and Documentation



Russ Thomas

DATABASE MANAGER

@sqljudo www.sqljudo.com



Passing Audits



Proof
“Evidence”



Know your requirements;
that's on you



Visual proof and physical inspection

Screen shots

Copies of outputs

Source code

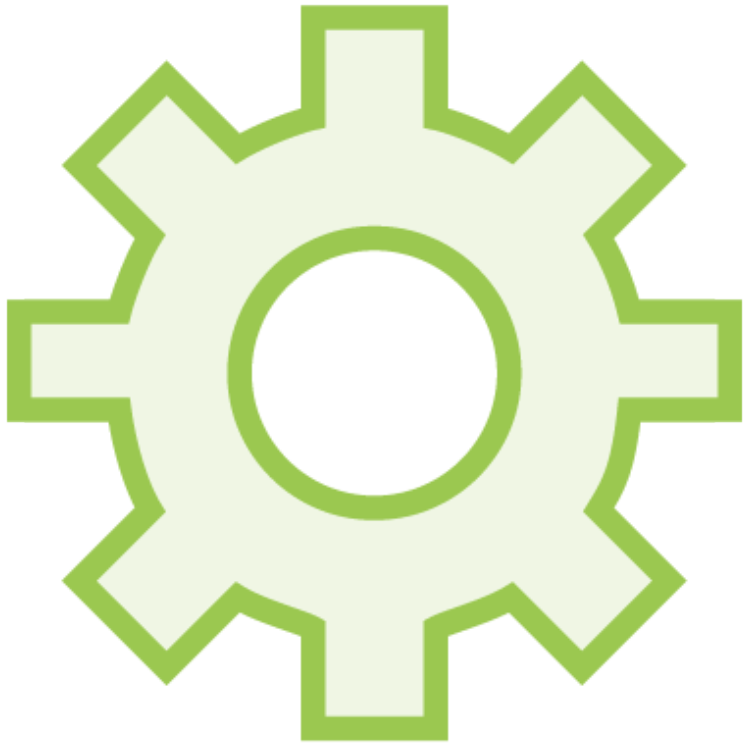




Approved reports

Built in system reports

Custom reports



Auditor provided tools / software

Tips and advice

Helping the auditor get what they need



Audit Evidence and Proof



Audit Review Process



Auditor



Subject Matter Expert

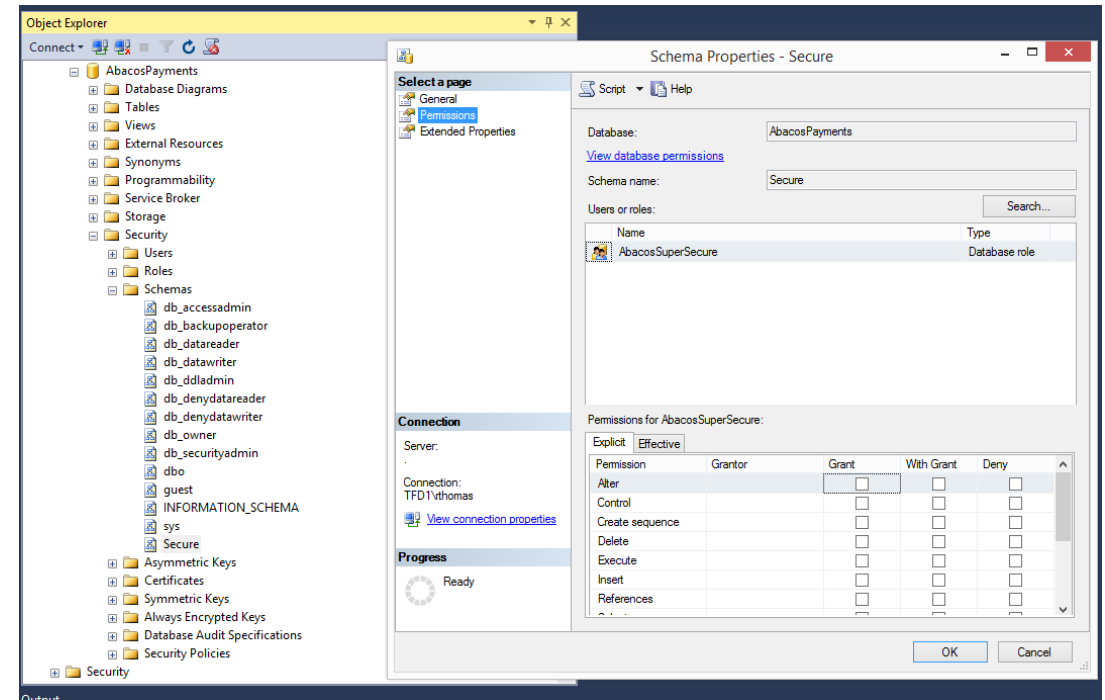
That's you!



Obtaining Proof



Show me who has access to the personally identifiable data



- AbacosPayments
 - Database Diagrams
 - Tables
 - Views
 - External Resources
 - Synonyms
 - Programmability
 - Service Broker
 - Storage
 - Security
 - Users
 - Roles
 - Schemas
 - db_accessadmin
 - db_backupoperator
 - db_datareader
 - db_datawriter
 - db_ddladmin
 - db_denydatareader
 - db_denydatawriter
 - db_owner
 - db_securityadmin
 - dbo
 - guest
 - INFORMATION_SCHEMA
 - sys
 - Secure
 - Asymmetric Keys
 - Certificates
 - Symmetric Keys
 - Always Encrypted Keys
 - Database Audit Specifications
 - Security Policies

Select a page

- General
- Permissions
- Extended Properties

Connection

Server:

Connection:
TFD1\thomas

[View connection properties](#)

Progress



Ready

Schema Properties - Secure

Script Help

Database:

AbacosPayments


[View database permissions](#)

Schema name:

Secure

Users or roles:

Search...

Name	Type
 AbacosSuperSecure	Database role

Permissions for AbacosSuperSecure:

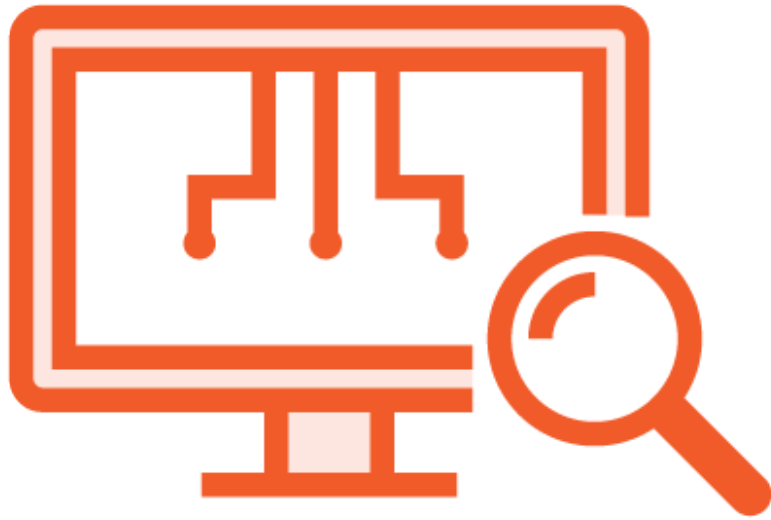
Explicit

Effective

Permission	Grantor	Grant	With Grant	Deny
Alter		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Control		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create sequence		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insert		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
References		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK

Cancel



Providing Visual Proof

- Get prepared ahead of time
- Keep your actions simple



Common Types of Proof

- Application Logs
- Source Code
- Configurations
- Copies
- Requests to demonstrate capability



If it's a legal and ethical request, it's expected that you can provide it.



Pre-prepared Compliance Reports



Prepared reports can greatly reduce the effort associated with compliance reviews



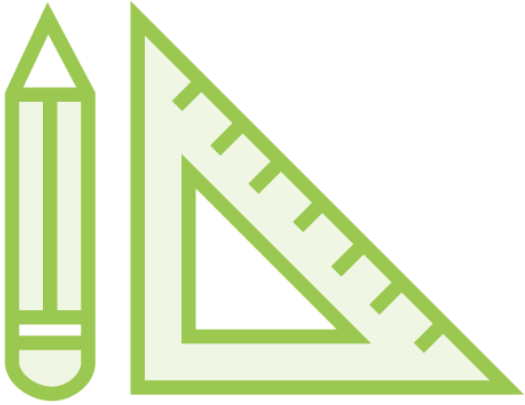
Ensure ahead of time what is required for the report to serve as proof



SQL Server comes with many pre-built reports



Report Development Lifecycle



Report Development



Source Control

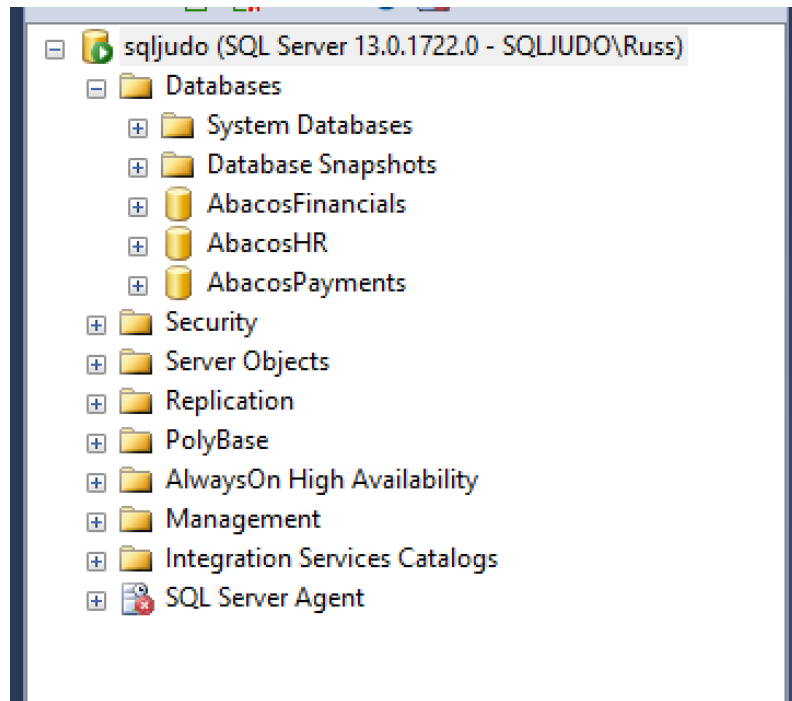


Change Control

Self Documenting Report



Report Parameterization





Final Tips and Tricks

- Be Flexible
- Understand the Role of the Auditor

Compliance Remediation



Relax



Most Audits Will Have
Items for Improvement



Thoroughly Prepare
for Follow Up



Losing certification or receiving penalties is typically a degenerative process, not a surprise event.





You should be familiar with compliance related topics in your industry

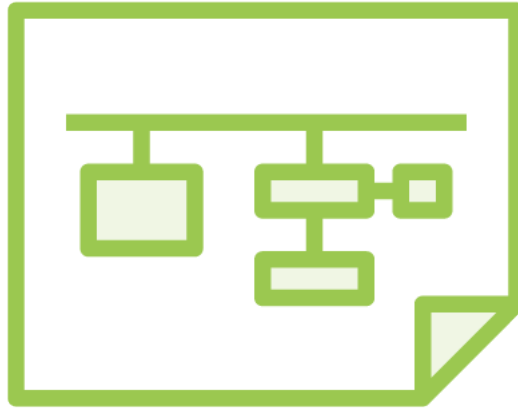
Auditors will ultimately be the subject matter experts



Your Options Abound



Feature Set to
Support Compliance is
Massive



Maintain a Consistent
Software
Development Lifecycle



Document Everything

```
-- Enable Database for CDC template
```

```
USE MyDB
```

```
GO
```

```
EXEC sys.sp_cdc_enable_db
```

Missing Topics





Some custom approaches to using CDC to support audit and compliance approaches are out there



THANKS!



Russ Thomas

DATABASE MANAGER

@sqljudo www.sqljudo.com

