metacoda®

How will the EU General Data Protection Regulation (GDPR) impact you?
Keep your SAS® data assets and platform secure.

1st December 2016
Michelle Homes

§sas® Silver Partner

GDPR – General Data Protection Regulation

- Who is aware of the GDPR EU regulation?

- Do you know if your organisation needs to comply?

- What are the sanctions if you don't comply?

GDPR – General Data Protection Regulation

- Apply from 25th May 2018

- Harmonise data protection laws

- Regulation promotes techniques such as anonymization, pseudonymization and encryption

- Sanctions: Up to 20,000,000 EUR or up to 4% of the annual worldwide turnover

173 STATEMENTS

GDPR consists of 173 statements, detailing the legislation

99 ARTICLES

GDPR Consists of 99 Articles of Legislation

72 Hour Breach Notification

ARTICLE 83

Administrative Fines
"10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher"

11 FACTORS

These Factors are key to the size of the fine.   PART 1
Such as
"Data protection by design and by default".
"Security of processing"

TECHNOLOGY

Technology use is expected in 20% of the Articles.

LEGAL

Legal Interpretation is needed in at least 6% of the Articles, and 12% of the statments

COMPLIANCE

Compliance especially automated compliance will assist in 20% of the Articles.

MONITORING

Monitoring of Data Processing applies to 19% of all the Articles.

SPECIFIC DATA AREAS THAT ARE IN THE REGULATION

Childrens Data
Direct Marketing
Pseudonymisation of Data
Health Data
Right of Access
Right to be Forgotten

Natural persons may be associated with online identifiers
Devices, IP Addresses, RFI Tags, Cookie identifiers,Applications,Tools
That leave traces to indentification

DATA PROTECTION OFFICER

The data protection officer shall have at least the following tasks:
(a) to inform and advise the controller or the processor of their obligations
(b) to monitor compliance with this Regulation
"The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks."
Published from www.vciso.co GDPR Report 2016

http://vciso.co/gdpr-questions-you-need-to-answer-within-30-days/

Michelle Homes

GDPR FINES
Administrative Fines   PART 2

ARTICLE 83/4
"Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:"

2% 10,000,000 EUR

ARTICLE 83/5
"Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:"

4% 20,000,000 EUR

ARTICLE 83/6
"Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."

4% 20,000,000 EUR

STATEMENT 148
"In order to the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation"

Not Just Fines

STATEMENT 151
"The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty"

Criminal Penalty

Fines On Global Revenue
Up to 2% 10,000,000 EUR
Up to 4% 20,000,000 EUR
Appropriate Measures
Criminal Penalty Denmark

Published from www.vciso.co GDPR Report 2016

metacoda

173 STATEMENTS
GDPR consists of 173 statements, detailing the legislation

99 ARTICLES
GDPR Consists of 99 Articles of Legislation
72 Hour Breach Notification

11 FACTORS

GDPR FINES
Administrative Fines PART 2

ARTICLE 83
Administrative Fines
"10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher"

DATA PROTECTION OFFICER
The data protection officer shall have the following tasks:
(a) to inform and advise the controller or processor of their obligations
(b) to monitor compliance with this Regulation
"The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks."
Published from www.vciso.co GDPR Report 2016

STATEMENT 151
"The rules on administrative fines may be applied in such a manner that in each individual case the fine is imposed by competent national courts as a criminal penalty"

Fines On Global Revenue
Up to 2% 10,000,000 EUR
Up to 4% 20,000,000 EUR
Appropriate Measures
Criminal Penalty Denmark

Published from www.vciso.co GDPR Report 2016

Strengthening citizens' fundamental rights in the digital market and focuses on personal data

http://vciso.co/gdpr-questions-you-need-to-answer-within-30-days/

Michelle Homes

metacoda

How does this affect AU businesses

- Some Australian businesses covered by the Australian Privacy Act 1988 (Cth)(the Privacy Act) (known as APP entities), may also need to comply with the GDPR if they offer goods and services in the EU or monitor the behaviour of individuals in the EU.

- Article 30: except for a "an enterprise or an organisation employing fewer than 250 persons"

- Office of the Australian Information Commissioner resource: https://oaic.gov.au/resources/engage-with-us/consultations/australian-businesses-and-the-eu-general-data-protection-regulation/consultation-draft-australian-businesses-and-the-eu-general-data-protection-regulation.pdf

Personal Data - Responsibility & Accountability

Data Protection Impact Assessments (DPIA)

"Data protection by design and by default"

"Data protection by design and by default"

Essential elements in EU data protection rules

Keep personal data secure

Michelle Homes

Data security governance

…mindset that embraces governance and show some formalism in securing their data

Earl Perkins Research VP

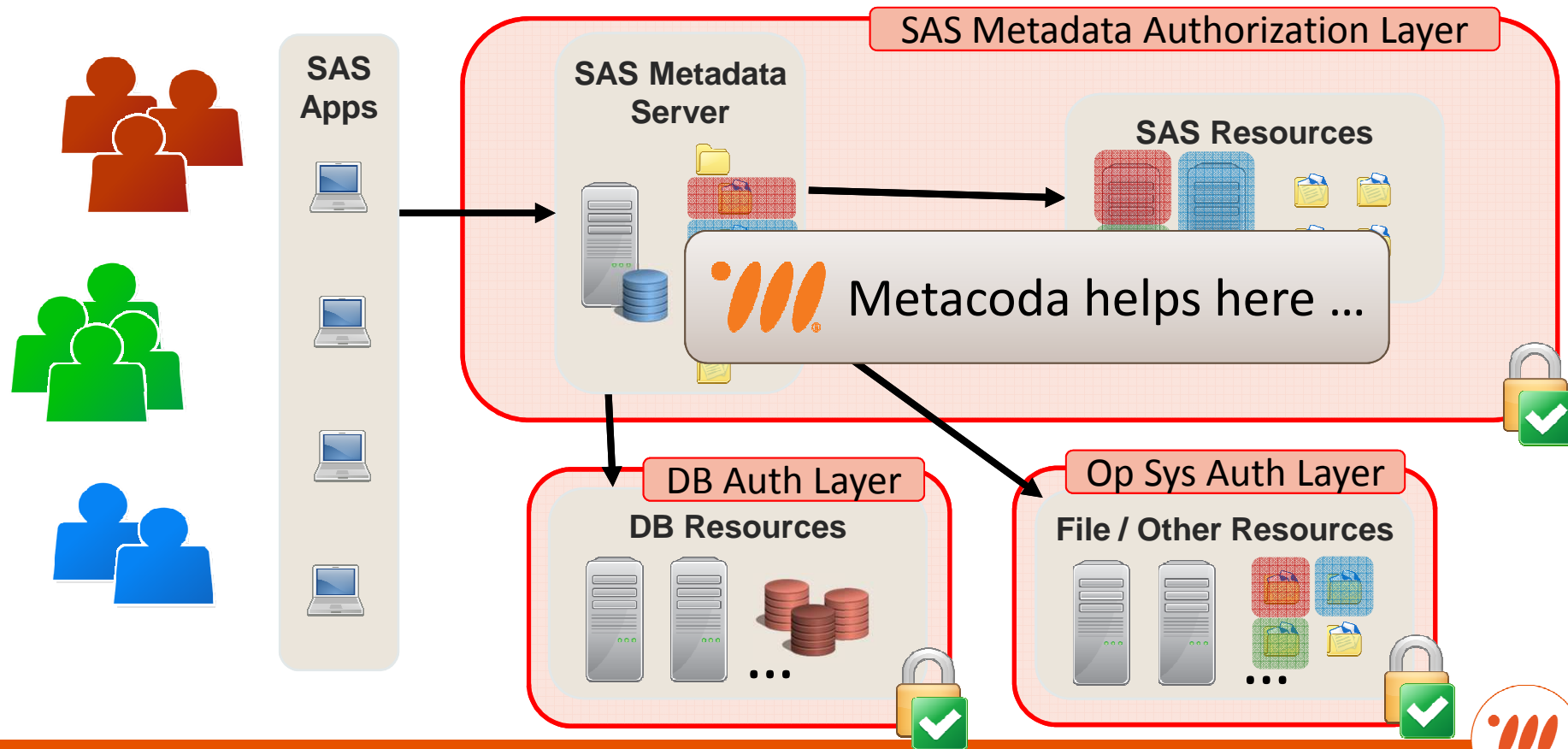Gartner Security & Risk Management Summit, July 2016

http://www.gartner.com/smarterwithgartner/six-trends-in-cybersecurity/

Michelle Homes

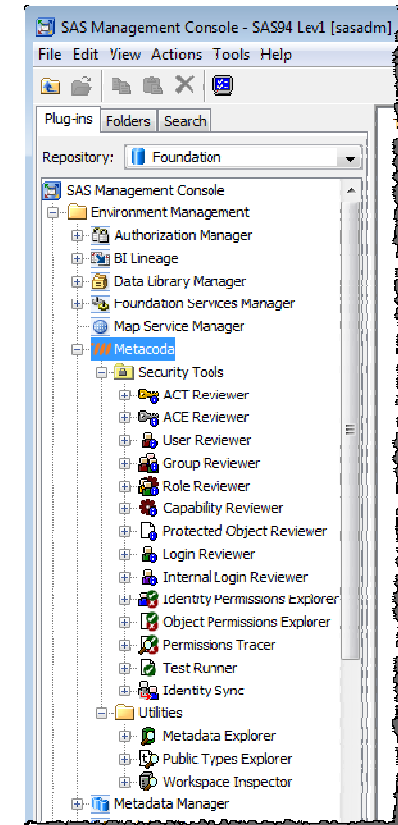metacoda

A few questions…

- What is the impact/cost to your organization of someone getting access to data/reports they shouldn't?

- When was your last SAS platform security project?

- When was it last tested? How extensive? How long did it take?

- Have there been any changes since it was last tested?
  - Deliberate, accidental, expected, unexpected?

- How do you know if it's still secure today?

Where do we fit?

SAS Apps

SAS Metadata Authorization Layer

SAS Metadata Server

SAS Resources

Metacoda helps here ...

DB Auth Layer

DB Resources

Op Sys Auth Layer

File / Other Resources

Michelle Homes

metacoda

About Metacoda

- **SAS Silver Partner** ... since 2007

- Provide add-ons to SAS® Software for enhanced metadata visibility and exploitation
  - Metacoda Identity Sync
  - Metacoda Security Plug-ins
  - Metacoda Testing Framework
  - Metacoda Utility Plug-ins - free
  - Custom Tasks (for SAS Enterprise Guide & AMO) - free

- Goals:
  - Improve your productivity through enhanced metadata visibility
  - Helping to keep your SAS® platform secure

A few social media quotes….

David Moors
@moorsd
⚙ Following

@metacoda your plug-ins have saved me days not hours with validating metadata for the LBG upgrade. Customer service is also totes amaze 😊

Quentin Baudewijns 1st
Consultant at SAS Belgium & Luxembourg

Loading metadata identities into SAS Metadata from AD using the tool was very easy. It worked like a charm. This is a great tool!

Wouter Germishuys 1st
Analytics Operations Manager at Telstra

I wish all software companies had the customer engagement that Metacoda has. Their tools are excellent and is industrial strength. Keep on building awesome tools and we will buy them :-)

Wouter Germishuys 1st
Analytics Operations Manager at Telstra

The Metacoda set of plugins is worth it's weight in gold if you have SAS deployment. We couldn't have migrated our system without the plugins. Please keep building excellent tools.

Leslie Shroot 1st
Senior Consultant at Servian

Used this with a client yeasterday. All I can say is WOW!

Michelle Homes   See more at http://www.metacoda.com/en/products/testimonials/

metacoda

Business Problems We Solve

- Keeping SAS Users & Groups in sync with Active Directory
    - Including large & complex directories ... all without code!
    - **Metacoda Identity Sync**

- Knowing/documenting your SAS Metadata Security
    - Easily showing an Auditor ...
        - » ... what someone has access to
        - » ... who has access to something
    - **Metacoda Security Plug-ins**

- Verifying & proving to an Auditor your SAS Metadata Security is still intact and you can quickly detect and act on changes
    - **Metacoda Testing Framework**

Michelle Homes

Metacoda Testing Framework

Helping keep a SAS platform secure over time.

Michelle Homes

Metadata Security Testing: Why?

Over time we get changes from various user roles …

Production (Lev1)
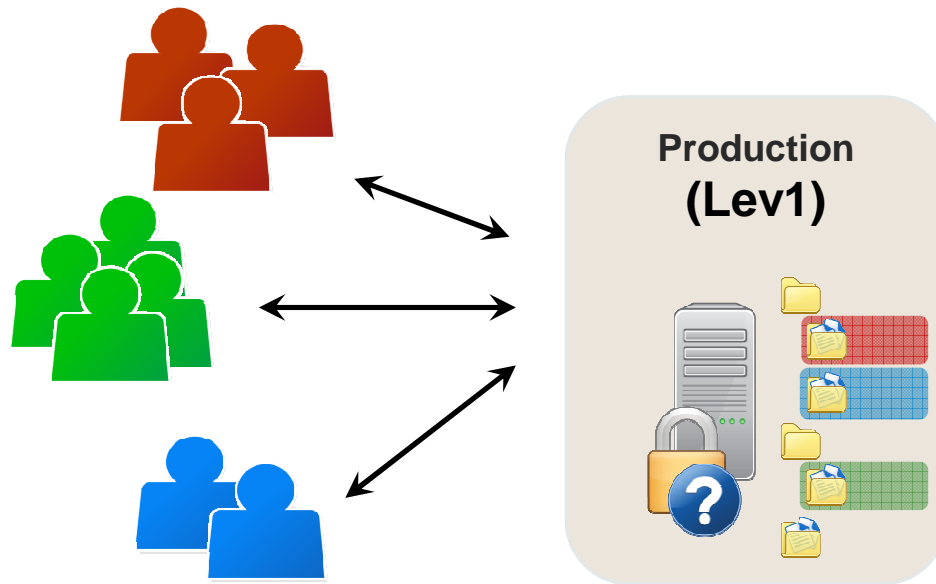
- … is it still adequately secured?
  - tomorrow?
  - next week?
  - next month?

metacoda

Metadata Security Testing: Why?

- Test for consistency across multiple environments …
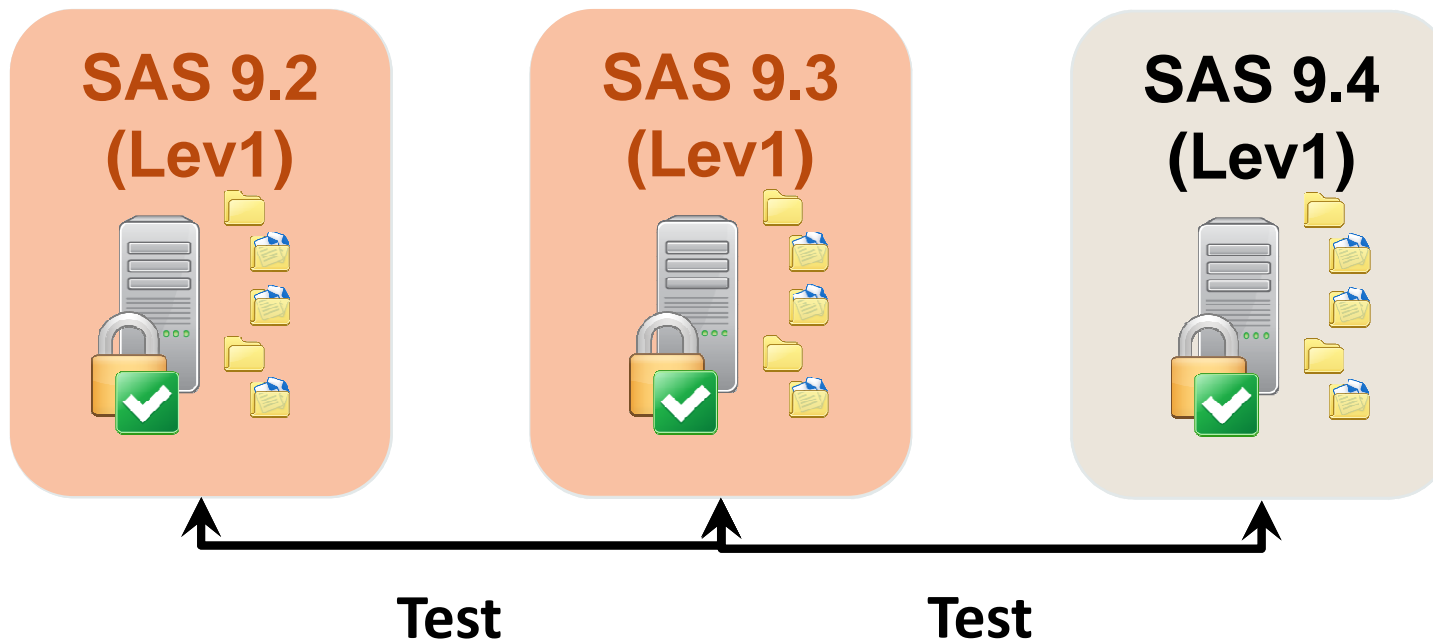
Problems with Manual Testing

- From our experience:
    - It's almost exclusively an **ad-hoc manual** process
    - It takes **too long**, it's **inconsistent** & it's **error-prone**

- Consequently it's not done …
    - with enough **coverage** & **reliability** to detect problems
    - with enough **frequency** to detect them promptly

- So we looked at how we could **automate** it ….
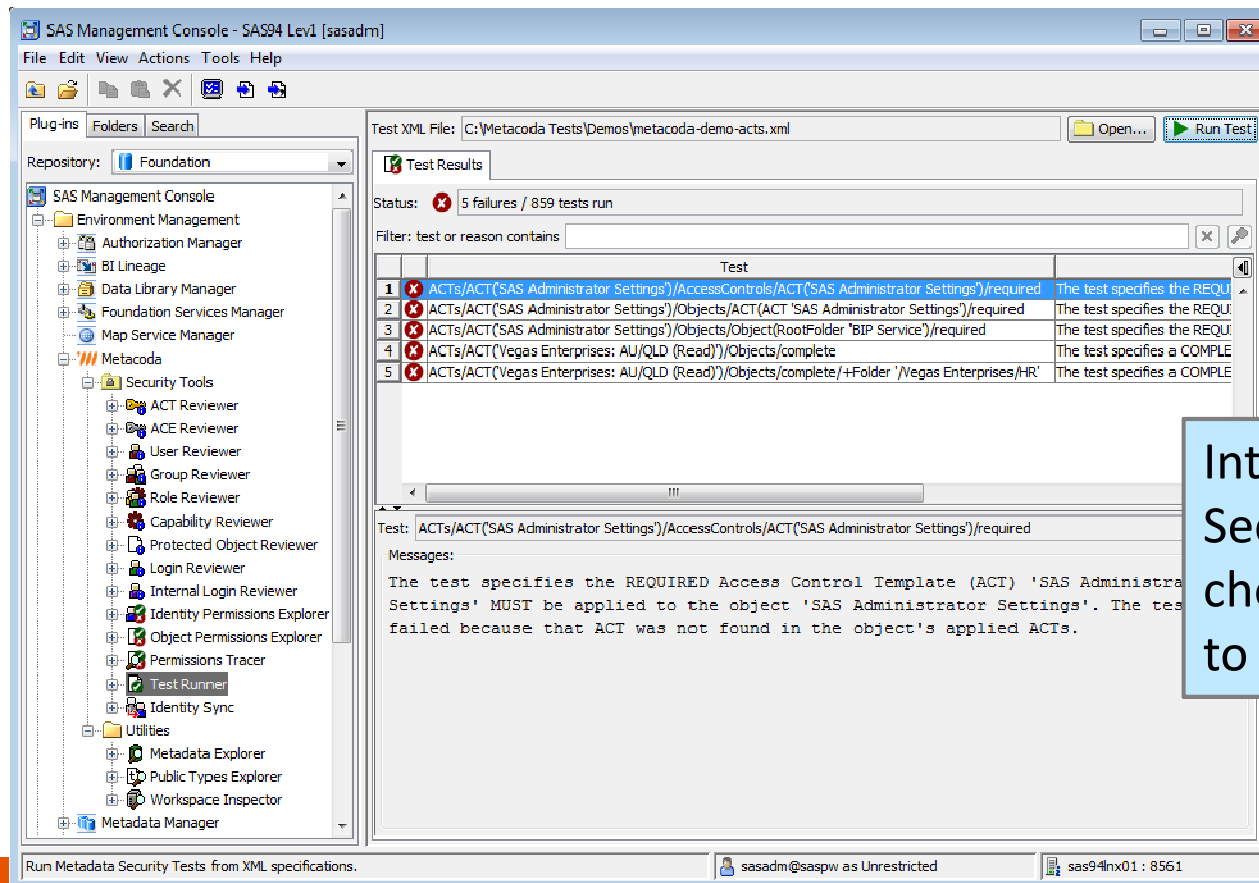
Metadata Security Testing

- An automated SAS metadata security testing framework includes:

    - Ability to export metadata security test specifications, as XML files, from an existing metadata server.

    - Test Runner: a new plug-in used to interactively run metadata security test specifications from XML files.

    - A batch interface for automated scheduled metadata security tests with HTML results and alert emails.

Michelle Homes

Metadata Security Test XML Export
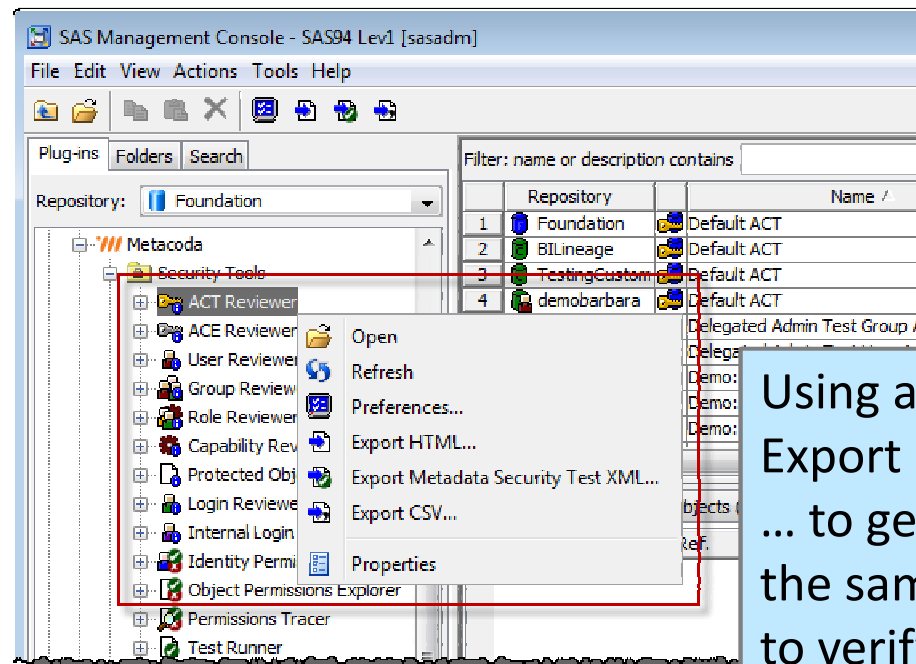
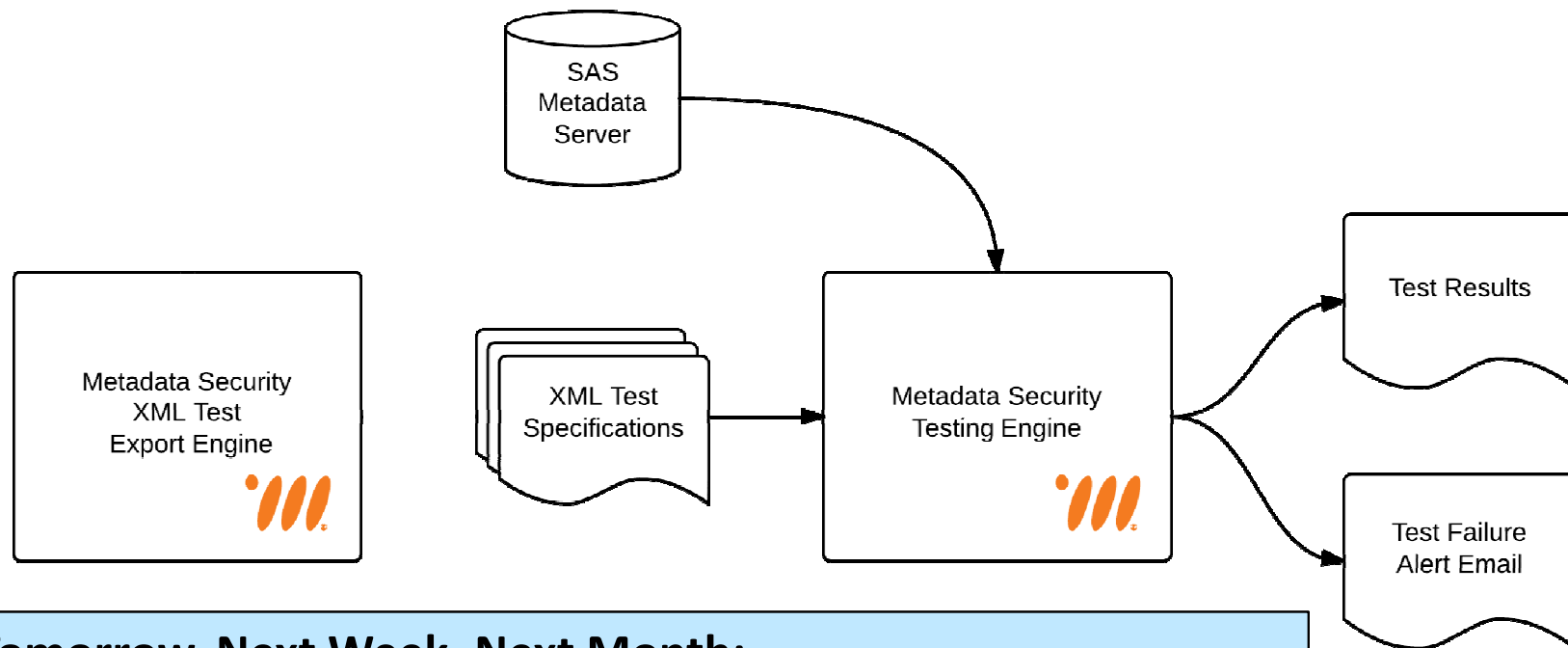
Using a known-good implementation …
Export Metadata Security Test XML
… to generate test scripts for future testing of the same installation (or a similar installation) to verify no significant changes.

Michelle Homes

Test Runner

Interactively run Metadata Security Test XML scripts to check for no failures prior to scheduling tests in batch.

Michelle Homes

Testing a Single Environment: Test & Repeat

SAS Metadata Server

Metadata Security XML Test Export Engine

XML Test Specifications

Metadata Security Testing Engine

Test Results

Test Failure Alert Email

Tomorrow, Next Week, Next Month:
Compare current state to desired state using previously
exported Metadata Security Test XML files

Michelle Homes

metacoda

Consistency Testing Different Environments

Testing Best Practices

- U.S. & Danish Models: similar with differences…

- U.S. Model as seen in the Security Admin Guide
    - Combination of ACTs and Explicit Permissions (ACEs) applied to folders

- Danish Model as used by SAS Denmark (and many others)
    - Best Practice Implementation of SAS Metadata Security at Customer Sites in Denmark, Cecily Hoffritz & Johannes Jørgensen, SAS Global Forum 2011 Paper 376-2011
    http://support.sas.com/resources/papers/proceedings11/376-2011.pdf
    - ACTs only (no ACES): "Green & Grey is Great!"
    - "6 Golden Rules"

Best Practices: Overview

- Prior knowledge & planning essential

- Apply security for Groups vs Users (use identity hierarchy)

- Apply security to Folders vs Objects (use inheritance paths)

- Prefer ACTs over Explicit Permissions (ACEs)

- Deny permissions only to PUBLIC or SASUSERS

- Org Groups only ever grant access (never deny)

- Automated scheduled testing with Metacoda Security Testing Framework

Posts/Papers about Testing ...

- Blog: Testing Conditional Grants in SAS Visual Analytics
  http://platformadmin.com/blogs/paul/2015/09/testing-conditional-grants-sas-va/

- Blog: Testing Recommended Practices with SAS Metadata Security
  http://platformadmin.com/blogs/paul/2015/06/testing-recommended-practices/

- Blog: SAS Metadata Security Testing
  http://platformadmin.com/blogs/paul/2014/03/sas-metadata-security-testing/

- SAS Global Forum 2014 Paper
  http://support.sas.com/resources/papers/proceedings14/1761-2014.pdf

Michelle Homes

Helping to keep your SAS® platform secure

Keep personal data secure

Time to invest in security - warns EC official Paul Nemitz

https://iapp.org/news/a/invest-in-security-to-comply-with-gdpr-warns-ec-official/

Michelle Homes

Want to learn more - webinars

- 6th December - EU Personal Data Protection 2018 - Remain compliant and avoid hefty financial penalties
https://attendee.gotowebinar.com/register/5119082425760435 972

- 6th December - Identity Management in SAS 9.4 Metadata Environment
http://www.sas.com/en_us/events/users-groups/16q4/metadata-server-environment.html

EU Personal Data Protection 2018
How to remain compliant

Join Live Webinar

sas

SUGA
SAS® Users Group for Administrators

metacoda®

Michelle Homes

Contact Us

✉ Email: info@metacoda.com

〽 Web: www.metacoda.com

🐦 Twitter: twitter.com/metacoda

f Facebook: facebook.com/Metacoda

in LinkedIn: linkedin.com/company/metacoda

▶ YouTube: www.youtube.com/user/metacoda

Thanks for hanging out with us in 2016!

@metacoda #HappyHolidays #MerryChristmas

Helping to keep your SAS® platform secure