PTAB Insights into the ISO16363 Audit of GPO’s govinfo Repository System

PTAB

22 May 2019

http://www.iso16363.org

Purpose

- Explain why and how the ISO 16363 audit of GPO's govinfo repository system was carried out
- Describe the international processes involved
- Describe PTAB's specific procedures
- Gives examples to show
  - – the breadth and depth of investigation by PTAB
  - – the level of preparation of GPO
- Discuss the benefits of certification, including its international recognition.

ISO 16363

- Guides an auditor in making a judgment about whether a repository can be trusted to preserve digitally encoded information
- Large number of "metrics" arranged hierarchically so that the auditor examines specific details
- Each metric has examples and more detailed explanatory discussion to assist repositories doing self-audits to prepare for ISO audit

Relationship between standards

- **ISO 14721:2012**, ***A Reference Model for an Open Archival Information System (OAIS)*** is the reference model for what is required for an archive to provide long-term preservation of digital information.
- **ISO 16363:2012*, Audit and certification of trustworthy digital repositories*** sets out comprehensive metrics for what an archive must do, based on OAIS, covering Organizational Infrastructure, Digital Object Management, and Infrastructure and Security Risk Management.

Relationship between standards

- **ISO 16919:2014**, ***Requirements for bodies providing audit and certification of candidate trustworthy digital repositories*** specifies the competencies and requirements for auditors and serves as an extension to **ISO/IEC 17021 *Requirements for bodies providing audit and certification of management systems***, providing additional requirements specific to auditing Trustworthy Digital Repositories.

Nonconformities

- Major nonconformity is a non-fulfilment of a requirement that affects the capability of the management system to achieve the intended results
  - The major nonconformities must be addressed in the 6 months following the on-site visit by agreeing with PTAB:
    - Root cause analysis
    - Plan for corrective action
    - Verification that the action has been successful
- Minor nonconformity is a non-fulfilment of a requirement that does not affect the capability of the management system to achieve the intended results
  - Plan must be agreed and should be implemented by the next audit

Why be certified?

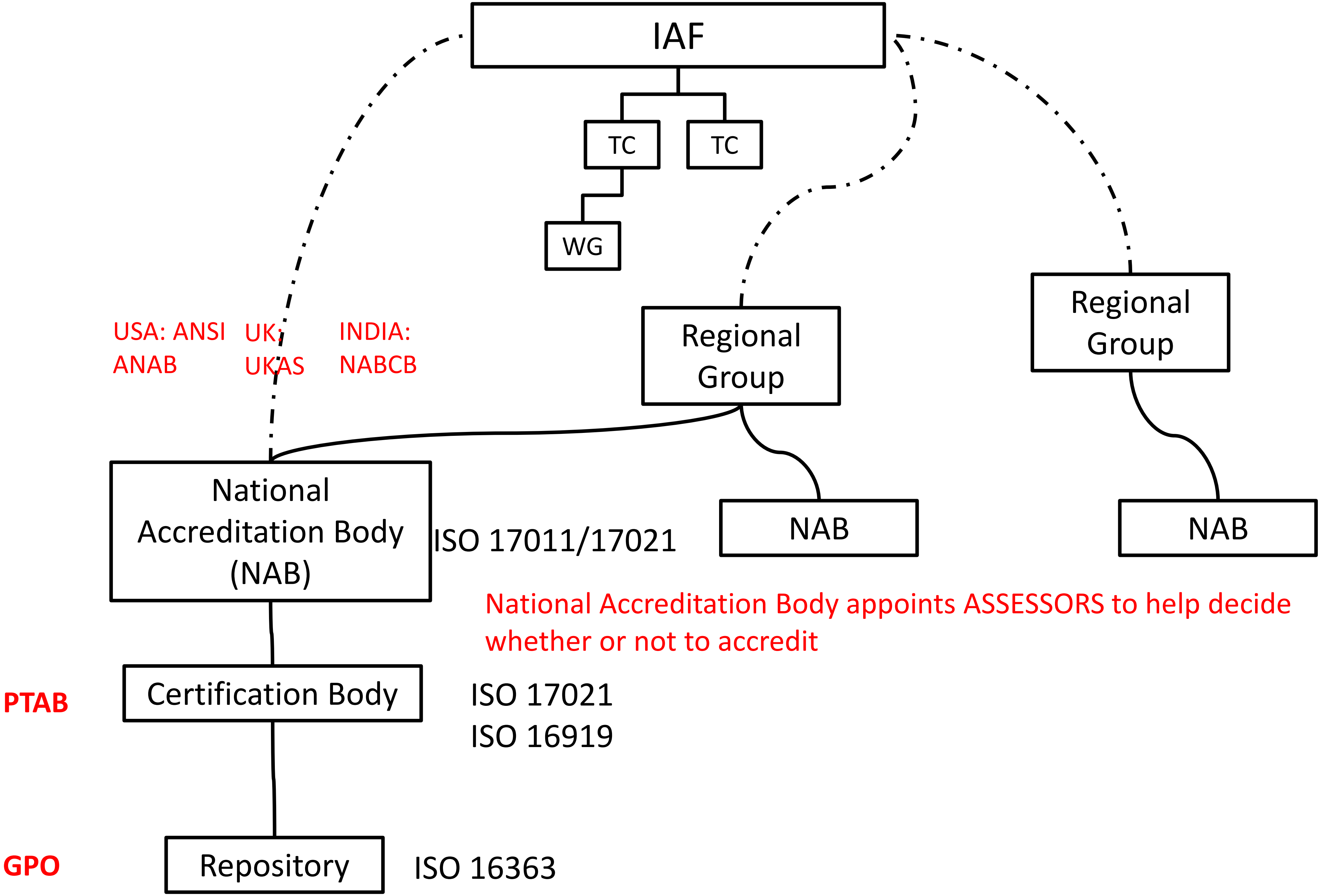
- To provide proof that the repository is doing a good job
- To help users make a choice between competitive repositories
- To instill confidence in depositors – so they are more likely to deposit
- To instill confidence in consumers– so they are likely to increase their usage and have greater trust in the information provided
- To instill confidence from upper management
- To instill confidence from funders – i.e. that they are not wasting their money
- Certification under ISO 16363 demonstrates and reinforces GPO's commitment to its mission of ensuring permanent public access to U.S. Government information through the preservation of content in digital formats.

The ISO audit process

- There are many audit processes, some local, some international
- ISO audits are the type of audits which touch very many aspects of all our lives:
  - Food
  - Medical
  - Travel
  - Security
  - ISO 9000
  - …

Aims of ISO audit and certification

- Inspire confidence by ensuring audits are conducted with:
  - impartiality;
  - competence;
  - responsibility;
  - openness;
  - confidentiality;
  - responsiveness to complaints;
  - risk-based approach.
- Using the process – ISO 17021:2015 - which is tried and tested for many activities, in many countries, with many organisations
  - Process requires periodic surveillance and recertification audits
- ISO 16919 specialises ISO 17021 to address digital repositories



IAF

TC

TC

WG

Regional Group

Regional Group

USA: ANSI ANAB

UK: UKAS

INDIA: NABCB

National Accreditation Body (NAB)

ISO 17011/17021

NAB

NAB

National Accreditation Body appoints ASSESSORS to help decide whether or not to accredit

PTAB

Certification Body

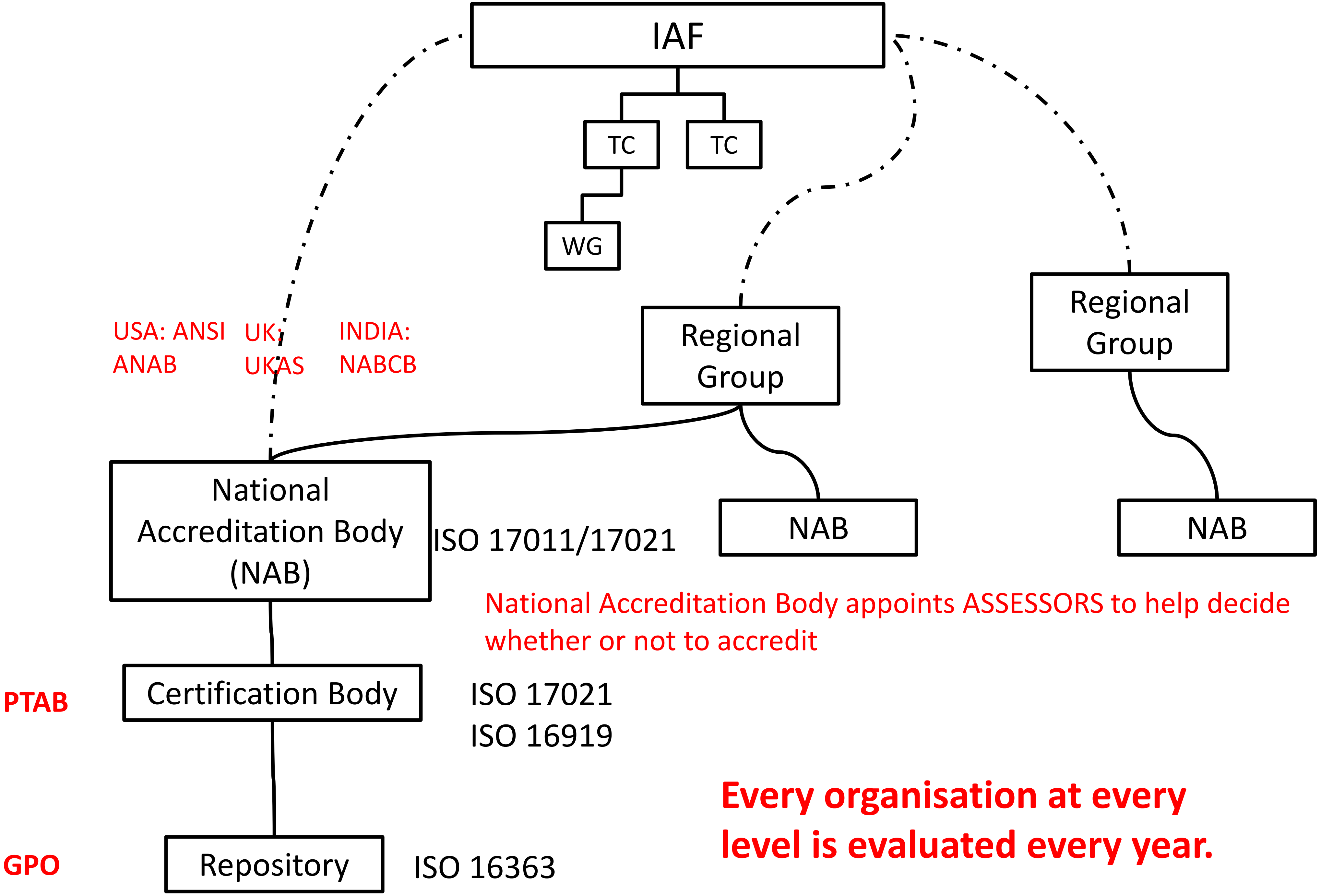
ISO 17021
ISO 16919

GPO

Repository

ISO 16363

TD 001



IAF

TC

TC

WG

Regional Group

Regional Group

USA: ANSI ANAB

UK: UKAS

INDIA: NABCB

National Accreditation Body (NAB)

ISO 17011/17021

NAB

NAB

National Accreditation Body appoints ASSESSORS to help decide whether or not to accredit

PTAB

Certification Body

ISO 17021
ISO 16919

GPO

Repository

ISO 16363

Every organisation at every level is evaluated every year.

TD 001

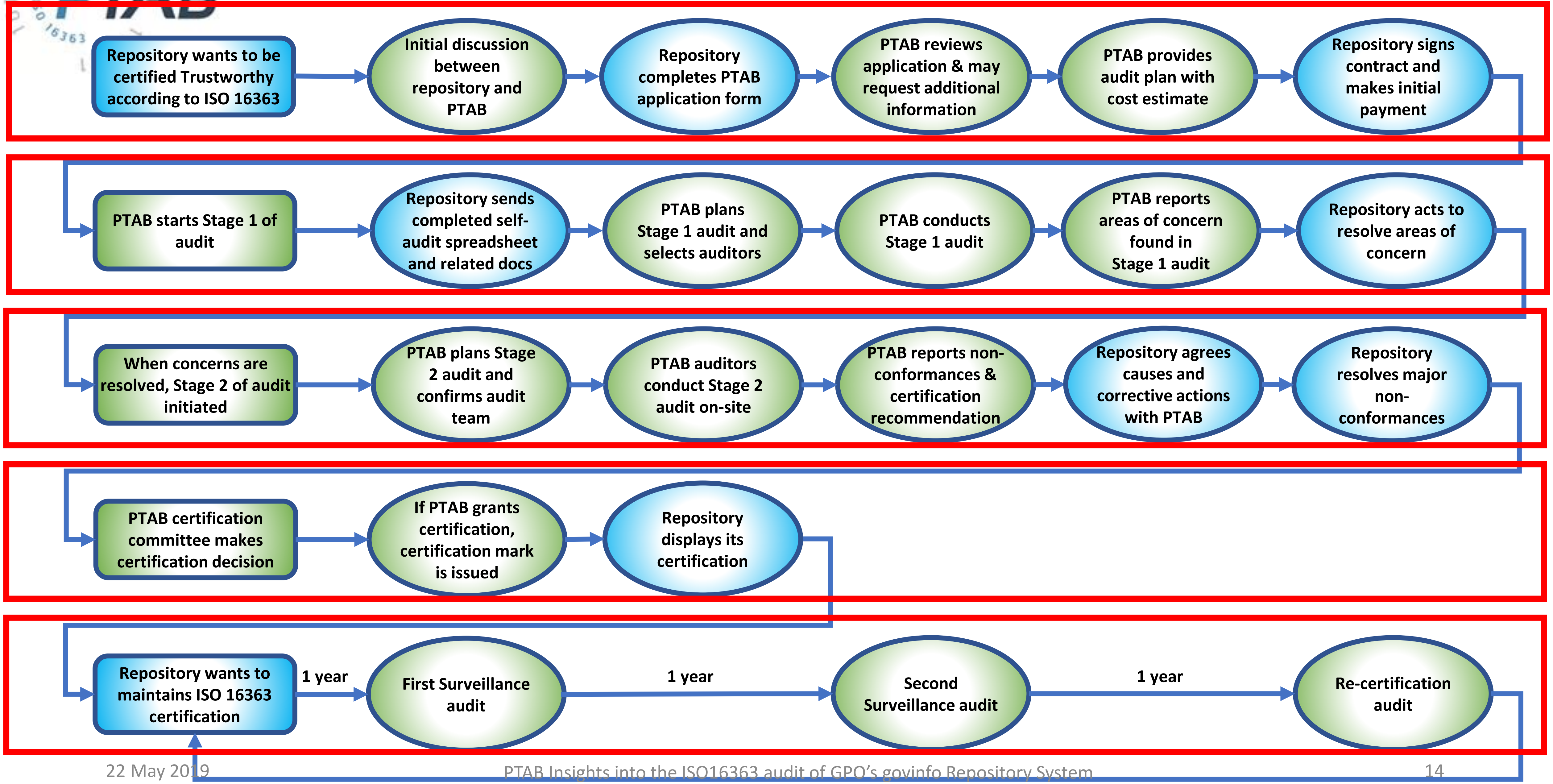
Who audits?

- Audit organizations must:
  - Have people with the required competences, supported by the audit body’s management system
  - Use the tried and tested ISO 17021:2015 processes and methods to give confidence
  - Use ISO 16919:2014 processes and methods that adapt the general processes for digital repositories
  - Be evaluated annually by assessors

ISO Process – the audit body must:

- Determine whether it is able to perform the audit. If so, it must
- Develop the audit program which must include
  - An initial certification with these components
    - Stage 1 – often an off-site review of documentation - identifying areas of concern that could be classified as a nonconformity during stage 2.
    - Stage 2 – on-site review using a defined process to identify nonconformities
    - Repository resolves issues
    - Certification committee makes decision on whether or not to award certificate
  - Annual surveillance audit in year 1 and year 2 after the initial certification
  - Re-certification audit in year 3, to begin the cycle again

Overview of the PTAB process



Repository wants to be certified Trustworthy according to ISO 16363

Initial discussion between repository and PTAB

Repository completes PTAB application form

PTAB reviews application & may request additional information

PTAB provides audit plan with cost estimate

Repository signs contract and makes initial payment

PTAB starts Stage 1 of audit

Repository sends completed self-audit spreadsheet and related docs

PTAB plans Stage 1 audit and selects auditors

PTAB conducts Stage 1 audit

PTAB reports areas of concern found in Stage 1 audit

Repository acts to resolve areas of concern

When concerns are resolved, Stage 2 of audit initiated

PTAB plans Stage 2 audit and confirms audit team

PTAB auditors conduct Stage 2 audit on-site

PTAB reports non-conformances & certification recommendation

Repository agrees causes and corrective actions with PTAB

Repository resolves major non-conformances

PTAB certification committee makes certification decision

If PTAB grants certification, certification mark is issued

Repository displays its certification

Repository wants to maintains ISO 16363 certification

1 year

First Surveillance audit

1 year

Second Surveillance audit

1 year

Re-certification audit

GPO Stage 1 audit

a) Evaluate the GPO's site-specific conditions and to undertake discussions with the GPO's personnel to determine the preparedness for stage 2;

1) identify "areas of concern" – things that could be non-conformities
2) allows time for GPO to fix the issues
3) make sure that on-site audit goes smoothly

b) Obtain necessary information regarding the scope of the management system, including: GPO's site(s);

1) processes and equipment used;
2) levels of controls established (particularly in case of multisite clients);
3) applicable statutory and regulatory requirements;
4) review the allocation of resources for stage 2 and agree on the details of stage 2 with the GPO;

c) Provide a focus for planning stage 2 by gaining a sufficient understanding of GPO's management system and site operations in the context of the management system standard or other normative document;

Investigation of GPO's readiness for audit

- GPO is large, having holdings totalling 65TB, with 1.5M AIPs, 45M retrievals per month in 2017 and supported by a staff of 40 FTE
- GPO collected detailed evidence for each metric
  - 800+ MB in 900+ files in 100+ folders (with some duplication)
- Reviewed by PTAB auditors
  - Adequate information in the AIP?
  - Enough Representation Information?
  - Adequate understandability?
  - Integrity checking inadequate?
  - Backups not held far enough from repository?
- GPO fixed had time to fix the issues and provided extra evidence
- PTAB updated review

→ GPO ready for on-site audit

GPO Stage 2 – the on-site visit

- Time limited and focussed, following the agreed agenda
- Need to assess information and evidence about conformity to all metrics:
  - Interviews with staff
  - Observation of processes and activities
  - Review of additional documents and records such as computer logs
- Opening and closing meetings must include information specified by ISO 17021 to ensure transparency. Also regular feedback
- Includes recommendation on certification
- Final feedback is in the detailed audit report

Day 1 schedule

Day_1	6th Dec 2018	Lead
Time	**Activity**	
09:00	Arrival	
09:15	**Opening meeting:** Introductions, confirmation of plans and expectations.	**PTAB**
09:45	**Review of points arising from Stage 1 of audit** to ensure that all areas of concern and questions are answered at this point or else will be resolved during remainder of the audit.	**PTAB**
10:45	**Walkthrough by client** Overview of the repository operations, and information flow from Ingest to Dissemination and overview of Preservation activities including policies, adherence to Information Model and Mandatory Responsibilities. This should, if possible, consist mainly of demos of actual ingest and access sessions, to provide an overview of the actual GPO processes;	**GPO**
13:00	**Lunch**	
13:30	**Team 1** **Digital Object Management** – section 4 of ISO 16363 4.1 Ingestion: Acquisition of Content, 4.2 Ingestion: Creation of AIP, 4.3 Preservation Planning, **Team 2** **Organizational Infrastructure** - section 3 of ISO 16363	**PTAB**
17:30	**Internal meeting** of the team	**PTAB**
17:45	**Feedback to Client** on day's findings.	**PTAB**

TD 001

Day 2 schedule

Day_ 2	7th Dec 2018		
Time	**Activity**		**Lead**
09:00	**Arrival** and start of Audit	Travel to ACF	
09:15	**Digital Object Management** – section 4 of ISO 16363 4.4 AIP Preservation		
09:45		**ACF Site Inspections + Staff Interviews** **Infrastructure and security risk management –** section 5 of ISO 16363 5.1 Technical Infrastructure and risk management	**PTAB**
12:15		Travel back to GPO HQ	
13:00	**Lunch Break**		
14:00	**Digital Object Management** – section 4 of ISO 16363 4.5 Information Management, 4.6 Access Management	5.1 Technical Infrastructure and risk management (continued) 5.2 Security risk management	**PTAB**
16:00	**Internal meeting of the team**, Finalization of report, etc		
17:00	**Closing meeting**		**PTAB**
17:45	**Close of Stage 2 Audit**		

Examples of in-depth questioning and examination

- Demonstration of ingest software
- Interviews with staff about security of electronic signatures
- Interviews with staff regarding creation of metadata and verification of its accuracy
- Frequency of review of risk register
- Investigations about single points of failure, including people
- Further details of Archival Information Package contents

Audit report

- ISO 17021 provides list of areas the report must cover
- The audit report shall provide an accurate, concise and clear record of the audit to enable an informed certification decision to be made

Nonconformities found

TD 001

Nonconformities found

- None

Nonconformities found…but

- This does not mean that the GPO system is perfect
  - All metrics are addressed, but all aspects of every metric for every aspect of the GPO system cannot be covered in any single audit.
  - Using GPO's documentation of the metrics, the auditors identified areas for extended focus.
  - On this basis it was judged that the repository can achieve its aims in terms of preservation
- Recommendations for Improvements
  - Continue to work with Producers to improve standardization of the SIPs submitted.
  - Continue to monitor the impact of multiple software packages used by govinfo to facilitate operation of the system for full integration and most efficient operation of the system.
  - Current preservation system works well for current holdings, but GPO may need to prepare for new publishing paradigms.
- Subsequent audits
  - will examine other aspects
  - may identify changes in systems and/or people which affect certification

TD 001

Certification decision

- The actual decision is made by a separate Certification Committee
  - Members of this committee have been isolated from information about the GPO audit in order to maintain impartiality
  - The Audit Report provides information on which the audit decision is taken including
    - comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client;
    - confirmation of the information provided to the certification body used in the application review;
    - confirmation that the audit objectives have been achieved;
  - Also ensures that the Audit Team has followed PTAB’s procedures

Certification was awarded to GPO

- Certification Committee decision on 28th December 2018
- Email notification
- Physical certificate sent to GPO
- PTAB website recorded the certification to allow validation

Summary

- PTAB has been accredited as a Certification Body for ISO 16363
- PTAB’s procedures are consistent with ISO 17021 and ISO 16919
- GPO applied for audit and certification for the govinfo repository
- The GPO repository was found to be well designed and implemented and the staff extremely knowledgeable, with no single point of failure
- Certification was awarded so **GPO’s govinfo system is now internationally certified as a Trusted Digital Repository and** demonstrates and reinforces GPO's commitment to its mission of ensuring permanent public access to U.S. Government information through the preservation of content in digital formats.
- For the certification to be maintained, surveillance audits (by 27 Dec 2019 and 2020) and recertification audit (by 27 Dec 2021) must be passed

TD 001

References

- **ISO/IEC 17021-1:2015** *Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements*, available from http://www.iso.ch
- **ISO 16363:2012** also known as *Audit and Certification of Trustworthy Digital Repositories*. Magenta Book. Issue 1. September 2011., available from https://public.ccsds.org/Pubs/652x0m1.pdf also
- **ISO 14721:2012** also known as *Reference Model for an Open Archival Information System (OAIS)*. Magenta Book. Issue 2. June 2012, available from https://public.ccsds.org/Pubs/650x0m2.pdf
- **ISO 16919:2014** also known as *Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories*. Magenta Book. Issue 2. March 2014, available from https://public.ccsds.org/Pubs/652x1m2.pdf
- GPO certification page on PTAB website, see http://www.iso16363.org/iso-certification/certified-clients/united-states-government-publishing-office/

QUESTIONS?