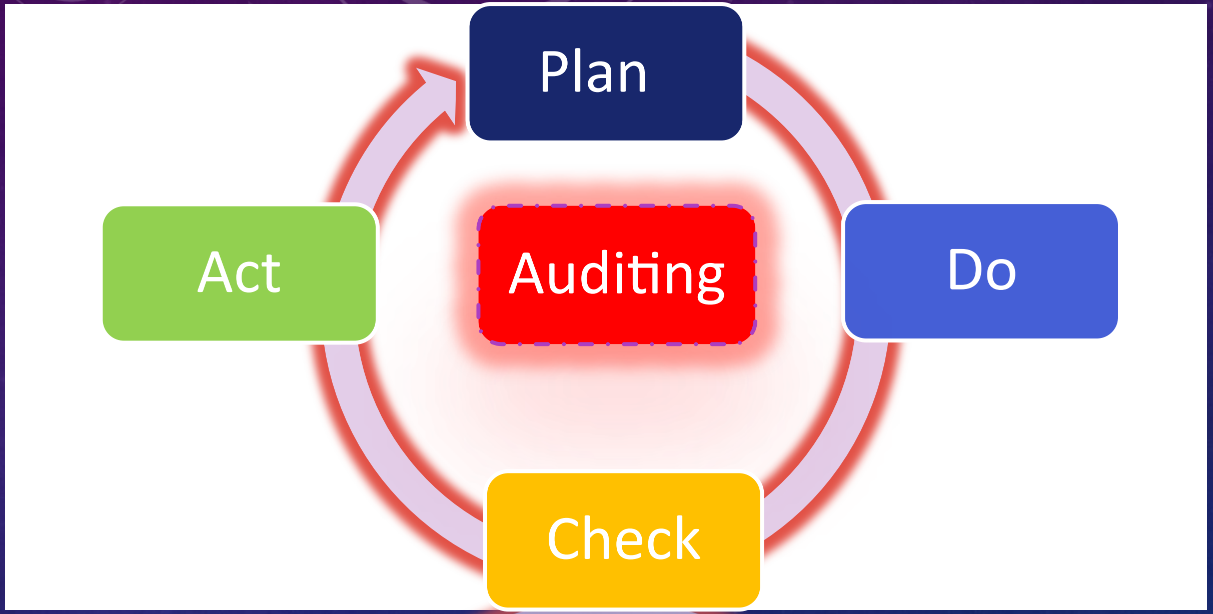
AUDIT → THE COMPLEMENTING PART OF THE ICS-PUZZLE



IN CONTROL STATEMENT (abbreviation ICS)

Auditing the completing part of the ICS puzzle

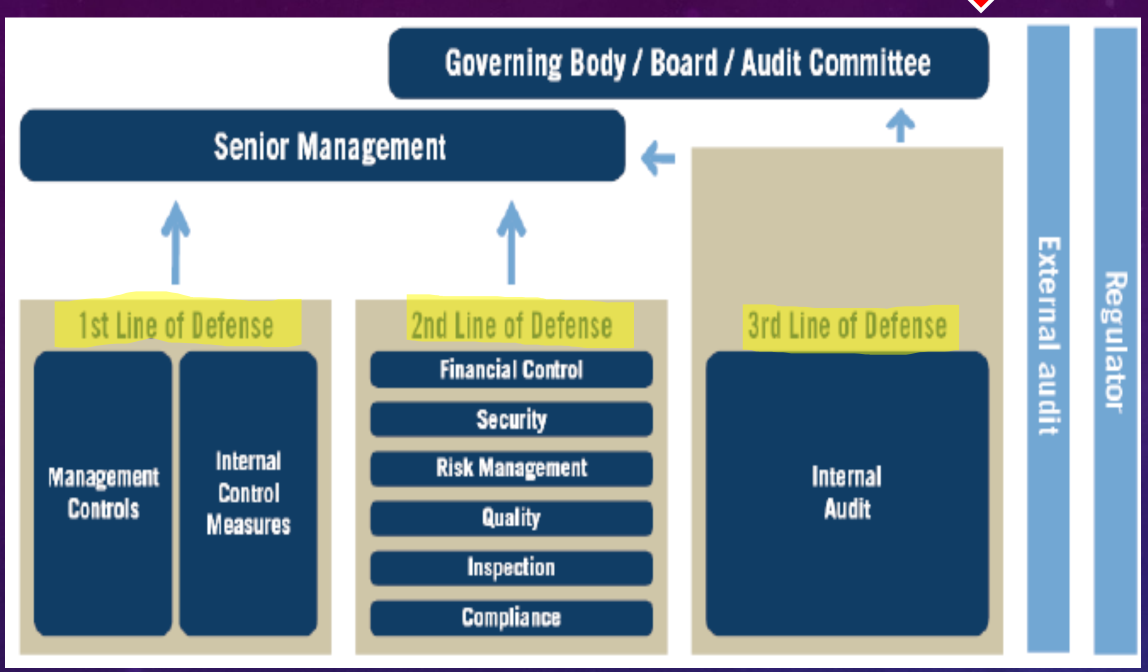
WHAT DO I WANT TO ACHIEVE...... TODAY

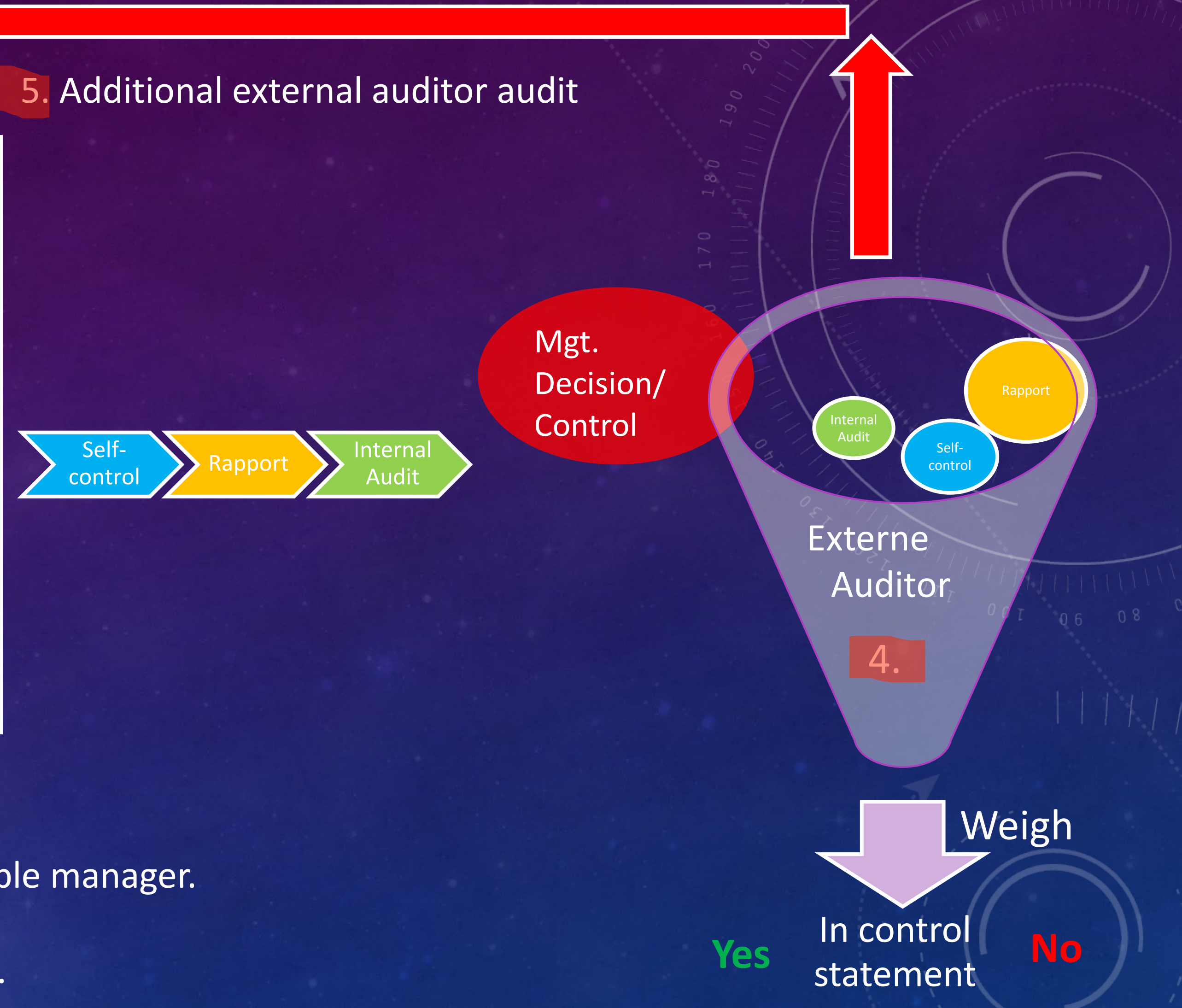
- Please put your hands up: Who has a positive mindset about 'an audit'.
- Changing your mindset with regard to (Internal) Auditor.
- What do I want to achieve today: More green hands up at the end of my presentation!!

WHY (INTERNAL) AUDITING

- Auditors – although people sometimes think otherwise – were not created to thwart system specialists or managers.
- In the overall context – the span of control – they do have a function.
- My role today is to take you into this mindset....that of that Audit function.
- There are many standards frameworks: BIO/BIR, NIS, NIST, BASEL, NOREA, ISACA, NIS2 and soon DORA.
- Auditors are used to determine the extent to which you comply with standards frameworks.
- Auditors are typically used to demonstrate the degree of integrity and confidentiality of data.
- There are external auditors who come to do audits for Ministry v. Finances for specific year-end closing or from DVI at DORA audit.
- There are internal auditors who carry out audits throughout the year to regularly determine and adjust the situation by identifying deviations or (residual) risks.
- A manager must always weigh and decide to what extent the risks are acceptable for his/her team or for the company.

LINES OF DEFENCE MODEL





1. First line= business/process-owner/responsible Manager.
2. Risk, Quality, Security management to support the Responsible manager.
3. Internal Audit.
4. External Auditor looks at the total control within the company. To give his/her total opinion on In Control Statement.
5. External auditor can carry out additional checks himself.

HOW IS AN AUDIT CONDUCTED?

An audit is scheduled in consultation with the Management/Audit Committee, the subject of the audit is coordinated. Output and end date will be determined in consultation with management.

F

Report with fixed end date so big management pressure!!

Team Manager/Team Members Will Be Notified about the audit

Audit is held and questions are asked about audit topic.

Findings are formatted in draft report and are coordinated with audited to remove 'noise' from findings

D/F

Final report is adopted and findings are sent to the Board of Directors

Final findings are presented within the relevant teams and are taken into account in ICS.

F

WHO HAS WHAT INTEREST IN THE AUDIT?

Auditor	Wants to investigate whether the design and operation does not impair data integrity.
Management	Don't want audit findings that could hinder ICS.
Team-manager	Wants to do a demonstrably good job so that his/her team is not an obstacle to ICS.
Security-Audit	Indicates the extent to which data integrity is guaranteed for those applications that are of financial importance during random checks by the auditor.
Data Integrity	Data integrity is the most important part of the audit. Being able to demonstrate data integrity of the data that is is a basis for an qualified in-control statement

WHAT TYPES OF AUDITS ARE THERE WITH WHICH PURPOSE?

What	Description	Who	Why
Internal control / Internal audit	Auditing is carried out by an internal audit team or by an internal auditor.	• Internal Control/ • Internal Auditor	Be aware early on audit findings that may be hindering ICS. Less work by external auditors on the teams
Control proces	Verification is performed to determine if a particular process has been followed properly (ITIL).	• Internal Control	Contributes as an overall picture to the degree of control.
Security-Audit	Auditing is performed to determine how authorizations are assigned to employees.	• Internal Auditor (Pre Audit) • External auditor	Pre Audit: Gives a better picture of the interior, so that there are still possibilities to make adjustments. Determine whether security design can compromise data integrity.
Data Integrity	Comprehensive security control that determines whether risks are sufficiently covered to ensure data integrity.	• Internal Auditor (Pre Audit) • External auditor	Pre Audit: Gives a better picture of the interior, so that there are still possibilities to make adjustments. If external auditors determine that the data integrity cannot be guaranteed, an ICS will not be issued!!

SECURITY AUDIT-1-SOME EXAMPLES (RISKS)

RACF	Risk to manage	Prove
Who has 'high rights' S|O|A?	With these rights, action can be carried out unseen.	RACF/SMF30, 80-83
Who can access APF Authorized datasets?	Via APF backdoor, permissions can be adjusted and actions can be performed unseen.	RACF permissions or notification from SIEM
Use of Assembler code	With this code, flip can be made "Special" outside of RACF via ACEE.	How is it detected?
Which Exits are used?	There are exits that carry a risk that gives users high privileges.	Demonstrate the analysis on the implemented system exits.
How is System Automation set up?	SO can the RACF bypass.	
How is SMF logging set up?	Logging should not be able to be deleted or modified by employees.	How is SMF log shielded?

SECURITY AUDIT-2 (RISKS)

RACF	Risk to manage	Demonstrate/monitoring
Which permissions are in WARNING mode	RACF shielding is bypassed in WARNING mode. Everyone has access.	RACF selects,printouts and monitoring.
Who has access to PARMLIB datasets?	Through APF backdoor, someone can give themselves 'high rights'. Supervisor state can be obtained through APF.	Good Security monitoring tools.
How are the OPERCMDS and FACILITY class profiles set up?	Who can execute SETPROG command? This ensures APF authorizations.	Detection of use SETPROG. Use security monitoring tools.
Who/what has PRIVILEGED/TRUSTED access?	Privileged and trusted ensure that someone can make changes 'unseen'.	Detection of Privileged and Trusted Usage.
Who can become UID(0)?	UID(0) gives too high rights to employees.	What procedures are in place? How is use enforced?
What are SETROPTS settings like?	Deviations can pose risks. Password settings, system settings RACF.	Setting SETROPTS.
How is USS set up.. who can BPX. Want to become a SUPERUSER?	Over-authorizations.	Security monitoring tools.

DATA INTEGRITY-1-SINGLE CONTROL ASPECTS

WHAT	RISK	Demonstrating/Testing
Segregation of Duties not properly implemented.	No or insufficient segregation of duties applied. Employee can do too much himself without the intervention of others.	RACF permissions via database unload. How is the security/segregation of duties set up using RACF?
How are permissions of the most important financial systems set up?	Authorizations are not set up according to the 'Least privilege' principle	Setting up RACF permissions.
CICS commands en CICS transactions inrichting?	Want to see which CICS transactions can mutate data?	CICS program description
Is there a data manipulation procedure and how is it set up/protected?	Who can perform data manipulation? Who checks correct execution?	Discharge by the client.
Is Security monitoring set up? Have good use cases been set up and used?	Quick response and response time can limit potential damage	Via SIEM monitoring and use of SPLUNK
Activity UAUDIT users checked?	What activities are carried out by UAUDIT users?	SMF 80-83 check.
Backup and recovery set up properly and usage tested?	Who can access backup? And it is tested whether backup is usable and complies with the legal retention period.	RACF and Backup logging.
Special attribute on demand by using PAM?	Users constantly have high rights in use instead of on demand and record why	PAM logging analyse.

TOOLS ANALYSIS RACF IN THE NEW WAY

What	Description	For what
Use tooling PyRACF/ZDEVOPS	Python tooling to parse RACF unload for analysis purposes.	Provides a better overview of the RACF configuration more quickly.
Via JCL job unload RACF-dbase	Current RACF unload	Basis for RACF analyses.
PyRACF (https://github.com/wizardofzos/pyracf.wiki.git)	Parse the full RACF unload in a Python dataframe	Analysis of the entire RACF database for security and data integrity aspects.
Analyse RACF permissions	Implementing RACF o.b.v. Least privalidge principle	As few rights as possible.
	Check permissions for major financial systems	Permissions are decisive for establishing data integrity.
Role design and role management RACF	How are the RACF roles set up?	Check Need-to-know of Need-to-do
	Is roll design and dispensing regularly checked?	
Is up-to-date SIEM monitoring used?	Is there up-to-date security monitoring in place?	Immediate intervention on undesirable events.
Which tool does it use? SPLUNK	How to set it up?	Direct SMF data analysis.

WHAT ARE THE CONSEQUENCES OF NOT HAVING ICS DATA INTEGRITY?

- Suppose Audit findings show that Security Audit and Data Integrity Audit cannot be guaranteed?
- Suppose that major financial applications are NOT SUBJECT TO DATA INTEGRITY APPROVAL issued by the External Auditor?
- What can be the consequence of this??
- The external auditor does NOT issue an In-Control-Statement.
- Means your company is NOT in control of its internal control or internal control.
- Consequences: Further administrative attention from above/Board of Directors.
- High fines imposed by external audit companies.
- Bad publicity for company to the outside world.
- Additional audits of audit services in the coming period or guardianship.

MY LAST PAGE OF THIS PRESENTATION

- Please put your hands up: Who has a positive mindset about 'an audit' now?
- Who has questions????
- Thank you for your attention.