Audit Report , GN on IS Audit & Audit in SAP

(Chapter - 7 : DISSA Course)

Arijit Chakraborty

August 28, 2021

Exam = Important terms / acronyms

1. ACL = Audit Command Language (CAAT Tool)
2. AIX = Unix Operating System for IBM servers
3. BCP = Business Continuity Plan
4. CAATs = Computer Assisted Audit Techniques
5. CR = Change Request (in SAP)
6. CRM = Customer Relationship Management (application software)
7. DB = Data Base
8. DMZ = De-Militarized Zone
9. DR = Disaster Recovery
10. ELC = Entity Level Controls
11. ERP = Enterprise Resource Planning (application software)
12. GITC = General Information Technology Controls

13. HOD = Head of Department
14. HP-UX = Unix Operating System for HP servers
15. LAN = Local Area Network
16. OS = Operating System
17. RHEL = Red Hat Enterprise Linux, a type of Linux Operating System
18. SA = Standards on Auditing
19. **SA/SOD** = Sensitive Access / Segregation of Duties
20. SAP = Systems, Applications and Products in data processing, ERP application software
21. SDLC = System Development Life Cycle, a software development methodology
22. SQL = Structured Query Language, high-level software language for database systems
23. UAT = User Acceptance Testing
24. VPN = Virtual Private Network
25. WAN = Wide Area Network

IS Report Format (CERT-In)

- **Audit Report content format**

1. Identification of auditee (Address & contact information)
2. Dates and Location(s) of audit
3. Terms of reference (as agreed between the auditee and auditor), including the standard for audit, if any
4. Audit plan
5. Explicit reference to key auditee organisation documents (by date or version) including policy and procedure documents

6. Additional mandatory or voluntary standards or regulations applicable to the auditee
7. Summary of audit findings including identification tests, tools used and results of tests performed
8. Analysis of vulnerabilities and issues of concern
9. Recommendations for action & follow up audits
10. Personnel involved in the audit, including ;

- Qualification
- Experience
- Role
- identification of any trainees
- Compliance of IS Audit standards , Guidance Note

IS Audit Report : – Government Entities : 2021

- **IS Audit report date -**
- May 30, 2021
- **Audit team:**
- *A. Morison*
- *R. Smith*
- *K. Khan*
- *F. Bakhsh*
- *S. Chowdhury*
- *M. Chow*
- *K. Wittstock*
- *R. Chettri*

Cover letter

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT 2021 – STATE GOVERNMENT ENTITIES

This report has been prepared for submission to Parliament under the provisions of section 24 of the *Auditor General Act 2006*.

Information systems audits focus on the computer environments of entities to determine if these effectively support the confidentiality, integrity and availability of information they hold.

This is the 13th year we have separately reported on State government entities' general computer controls (GCCs). The objective of our GCC audits is to determine whether entities' computer controls effectively support the confidentiality, integrity and availability of information systems.

I wish to acknowledge the entities' staff for their cooperation with this audit.

Chief IS Auditor

Executive Summary Auditor General's overview

- **A. Cyber-Attacks**
- *In the context of intensifying cyber attacks on all sectors, this report contains a number of important findings and recommendations resulting from our general computer controls audits and capability maturity assessments.*
- *All public sector entities should consider how they can apply the recommendations and case studies in the report to their operations with the expectation of an increasingly demanding threat environment into the future.*
- **B. Controls performance**
- *While entities improved their controls in 4 categories and remained constant in 1, information security continues to be an area of significant weakness.*
- *It is disappointing to see only 50% of entities met our benchmark in this area, a drop of 7% from last year.*
- *Poor information security controls leave entity systems and information vulnerable to misuse and may impact critical services provided to the public.*

- **C. COVID specific IS Risks**
- *The report also includes a summary of common issues related to remote access. During the COVID-19 response periods, entities supported their workforces with flexible working from home arrangements.*
- *This transformation also brought security challenges as entities changed the way they operate, in some cases significantly.*
- **D. WFH – Remote working**
- *Remote work is stated to become more prevalent and entities may continue to operate with a mix of remote and on-site workforces. Entities should consider these findings and ensure that adequate policies, strong access controls and monitoring are in place to address the inherent risks associated with remote working arrangements. This will require them to develop plans and implement controls to manage a range of hybrid environment risks*
- **E. Changes in Audit Standards**
- *Upcoming changes to the Auditing Standards clarify and enhance the need for auditors to understand general computer controls and their impact on the financial report. In particular, auditors are required to assess controls for each aspect of the IT environment including the network, operating system, database and application layers.*

IS Audit Approach

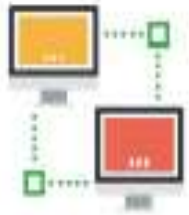
- *The model we have developed for our audits is based on accepted industry good practice.*
- *Our assessment is also influenced by various factors including the:*
- • *business objectives of the entity*
- • *level of entity dependence on IT*
- • *technological sophistication of entity computer systems*
- • *value of information managed by the entity*
- *For our capability assessments, entities improved their controls in 4 of the 6 audited categories. However, we continue to find a large number of weaknesses that could compromise the confidentiality, integrity and availability of information systems.*
- *Information security remains our biggest area of concern with only 50% of entities meeting our benchmark in this category, a drop of 7% from last year.*

Recommendations for ITGC

ITGC Categories

We focused on the following 6 categories:

Information security



IT operations

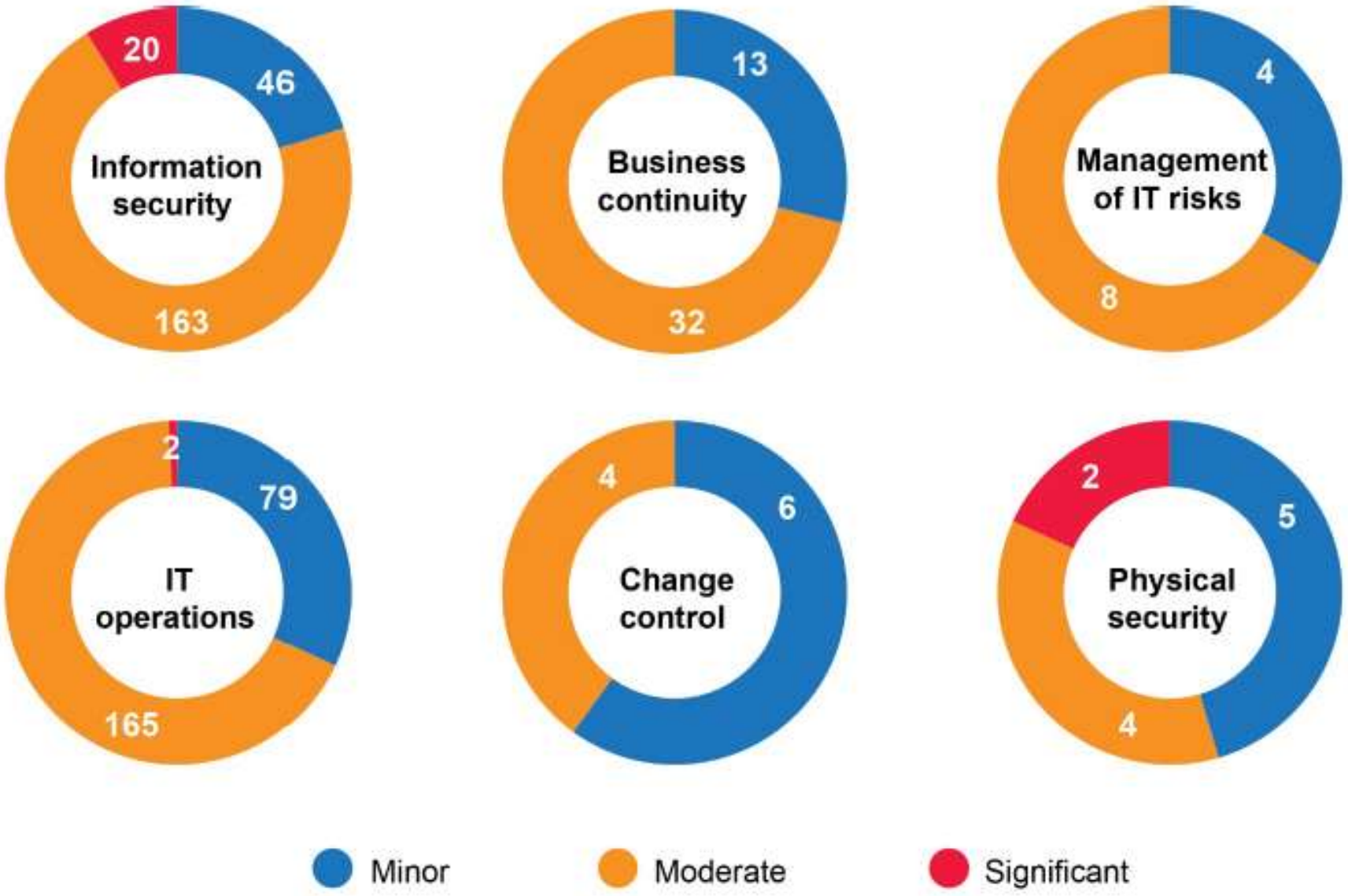
Business continuity

Change control

Management of IT risks

Physical security

Ratings for ITGC findings : each control category



Capability maturity model assessment results

- **% of entities rated level 3 or above**

The percentage of entities rated level 3 or above for individual categories was as follows:

Category	2019-20 %		2018-19 %
Information security	50	↓	57
Business continuity	62	↑	54
Management of IT risks	78	–	78
IT operations	82	↑	80
Change control	85	↑	80
Physical security	91	↑	89

Information security

- *We assessed whether entity controls were administered and configured to appropriately restrict access to programs, data and other information resources.*
- *Our audits include an assessment against better practice controls for information and cyber security.*
- *These controls may include:*

Information classification

Removable media control

Secure cloud and storage

Email security

Cyber security monitoring

Segregation of duties

Application hardening and control

IS controls included in GCC audits

Information security policy

Security awareness program

Vulnerability management

Multi-factor authentication

User account management

Strong passwords/ passphrases

Data encryption

Limit admin privileges

Network segregation

Security gateway

Prevent unauthorised devices

Database security

Malware protection

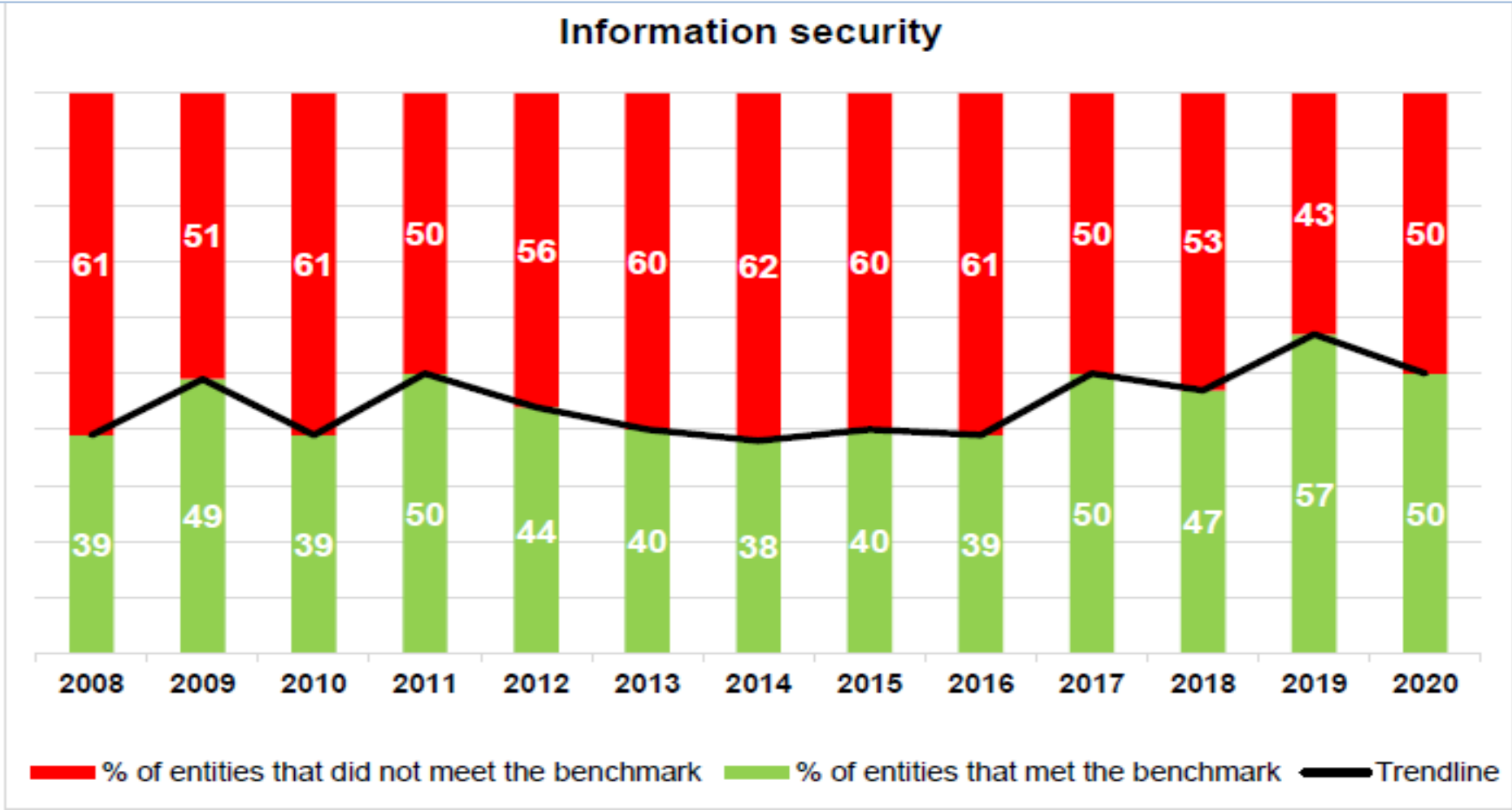
Patch applications

Patch operating systems

Web gateway and content filter

IS – % of entities that met/did not meet benchmark

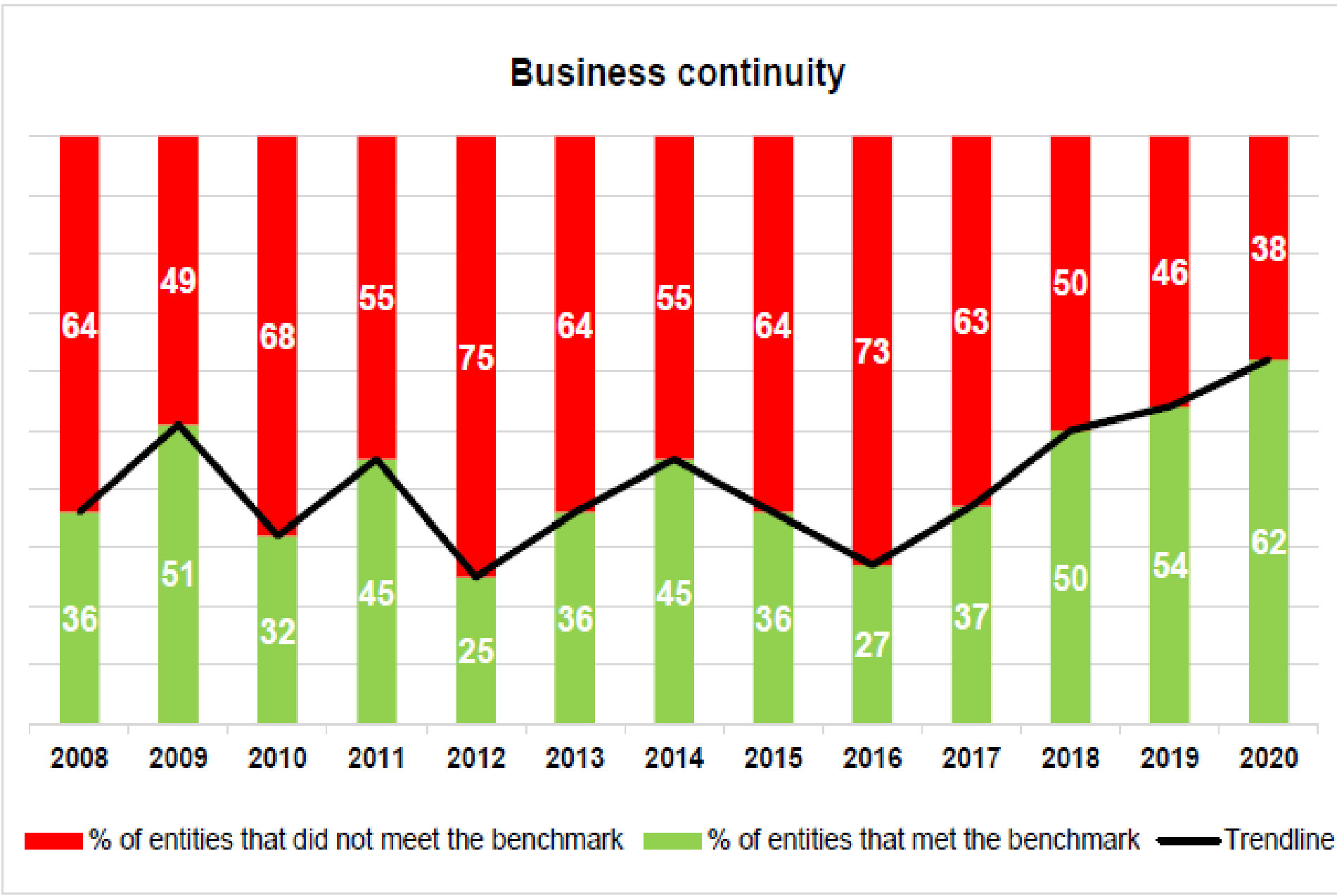
- *The number of entities who met our benchmark for information security decreased from 57% in 2018-19 to 50% in 2019-20.*
- *We continue to see little improvement in this space over the last 13 years.*



Business continuity- IS Auditor comments

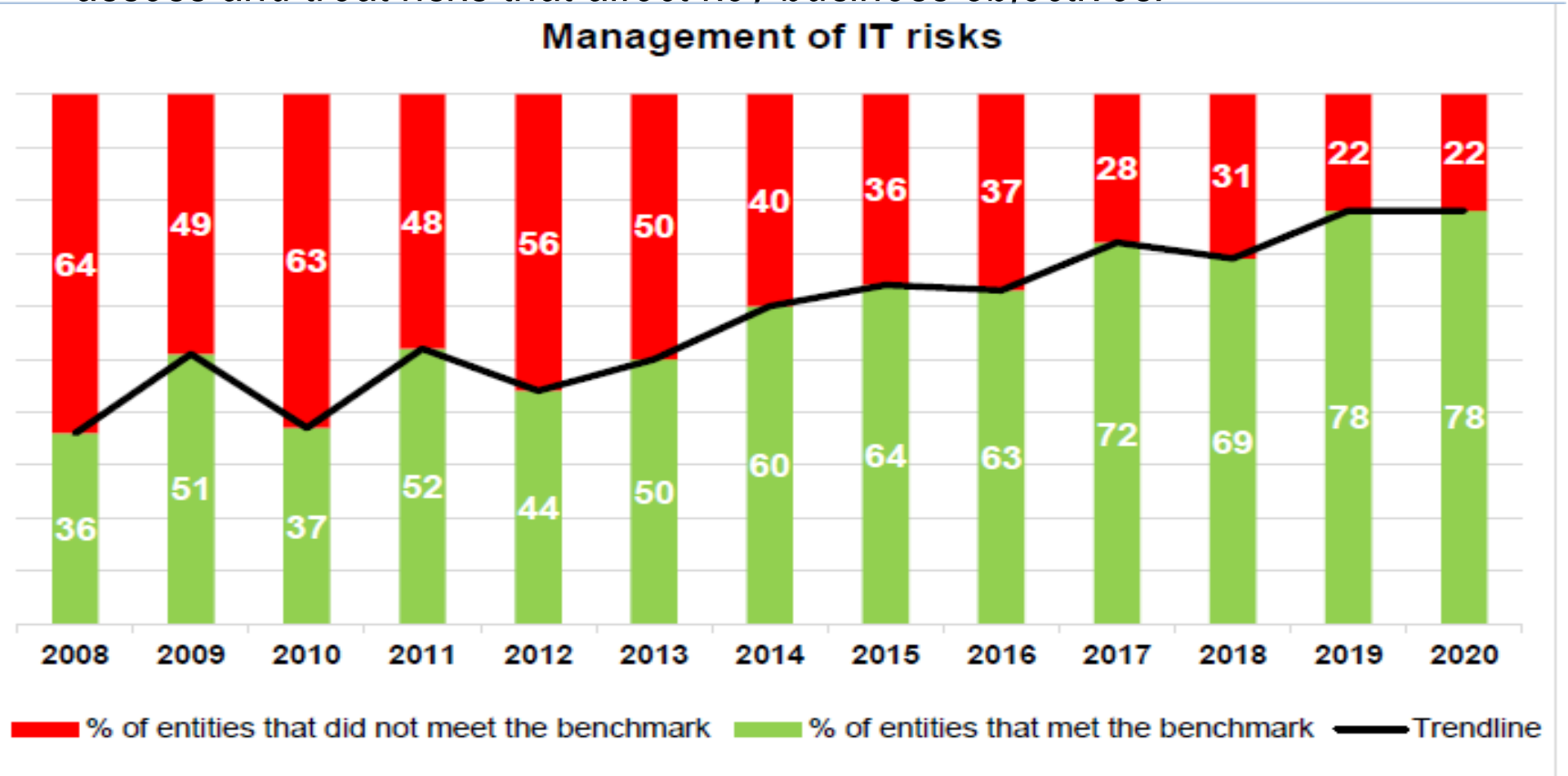
- *The percentage of entities that met our benchmark for this category in 2019-20 was the highest since we started benchmarking 13 years ago. This may, in part, be attributable to the need for entities to respond to COVID-19 pandemic. However, we found many still do not have adequate business continuity and disaster recovery arrangements in place.*
- *Interruptions to business can have serious impacts on the critical services entities deliver to the public. To ensure business continuity, entities should have an up-to-date BCP, DRP and incident response plan (IRP). The BCP defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the DRP. The IRP needs to consider potential incidents and detail the immediate steps to ensure a timely, appropriate and effective response.*
- *Entities should test these plans on a periodic basis. Such planning and testing helps entities assess and improve their processes to recover information systems in the event of an unplanned disruption to business operations and services. Senior executives should monitor that plans are developed and tested in accordance with the risk profile and appetite of the entity*

Business continuity – % of entities that met benchmark



Management of IT risks

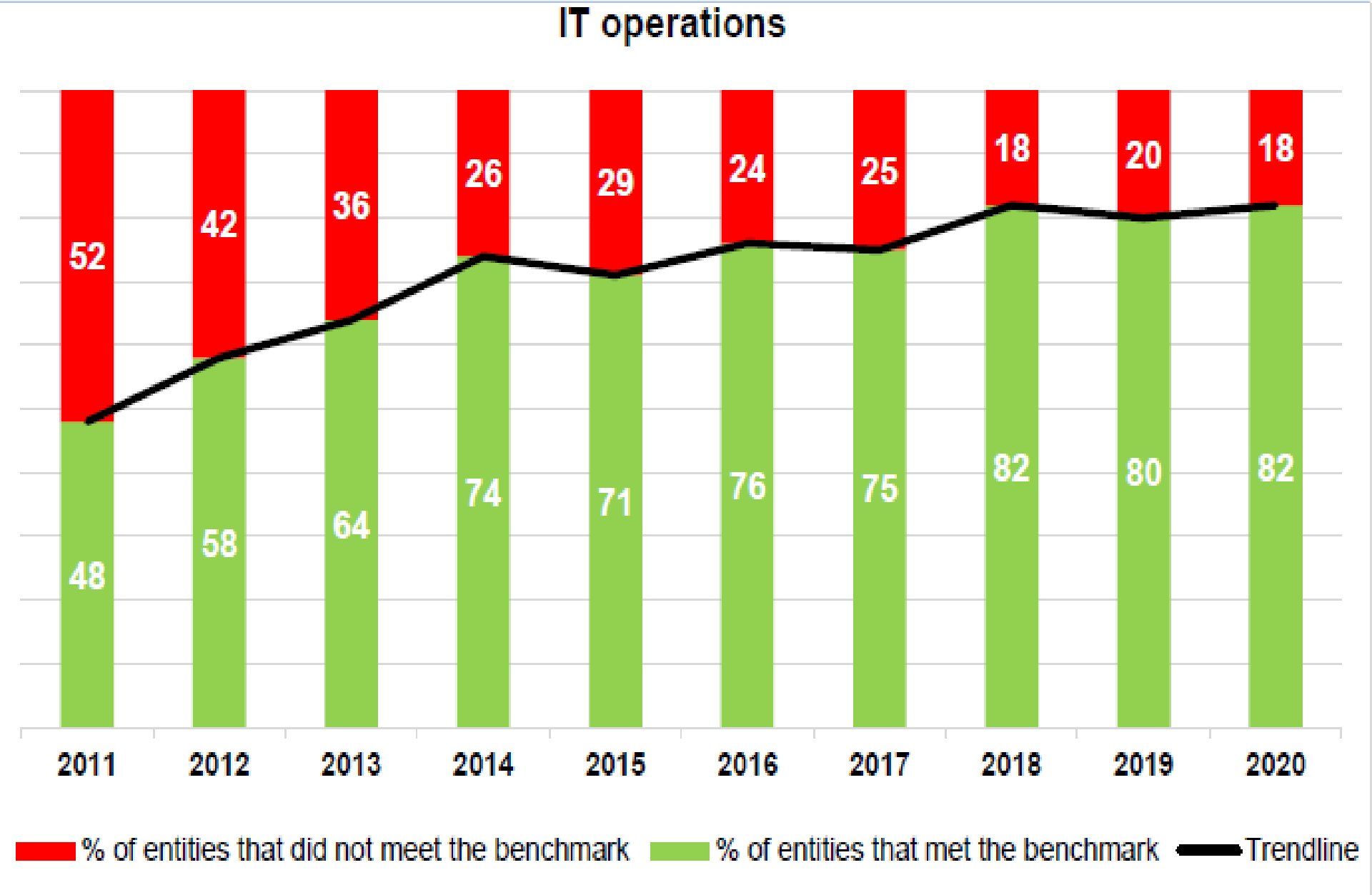
- *Consistent with last year, 78% of entities met our expectations for managing their IT risks. There has been steady improvement in this category, with 42% more entities meeting the benchmark since our first assessment in 2008.*
- *All entities should have risk management policies and practices that identify, assess and treat risks that affect key business objectives.*



IT operations

- *There has been steady improvement in the IT operations category since we added it to our assessment criteria in 2011. This year, entities continued to improve with 82% reaching our benchmark.*
- *Effective management of IT operations is key to maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures. We assessed whether entities had adequately defined their requirements for IT service levels and allocated sufficient resources to meet these requirements. We also tested whether service and support levels within entities were adequate and met good practice.*
- *Other tests included if:*
- *• policies and plans were implemented and working effectively*
- *• repeatable functions were formally defined, standardised, documented and communicated*
- *effective preventative and monitoring controls and processes had been implemented to ensure data integrity*

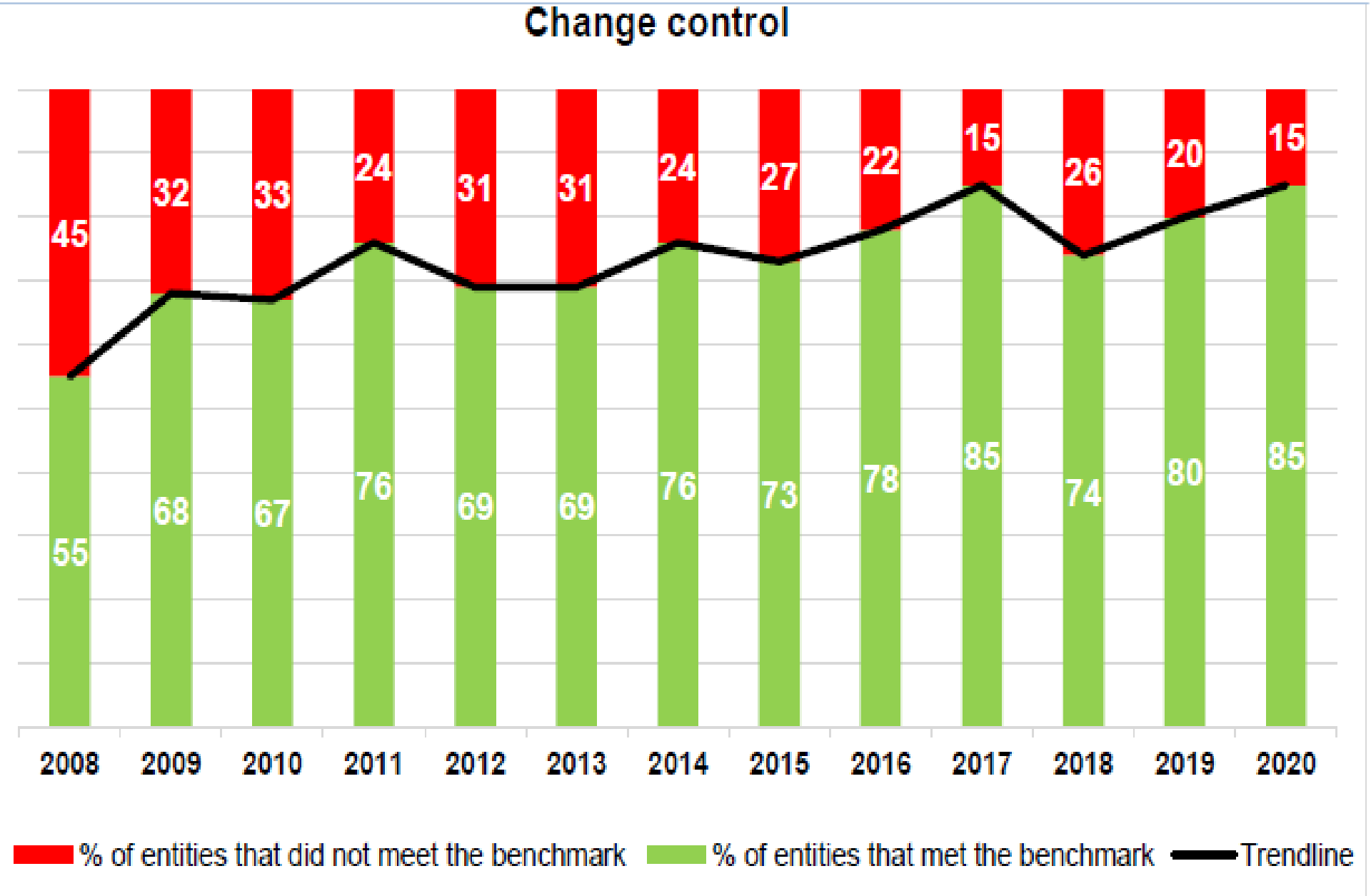
IT operations – % of entities that met benchmark



Common Control weaknesses

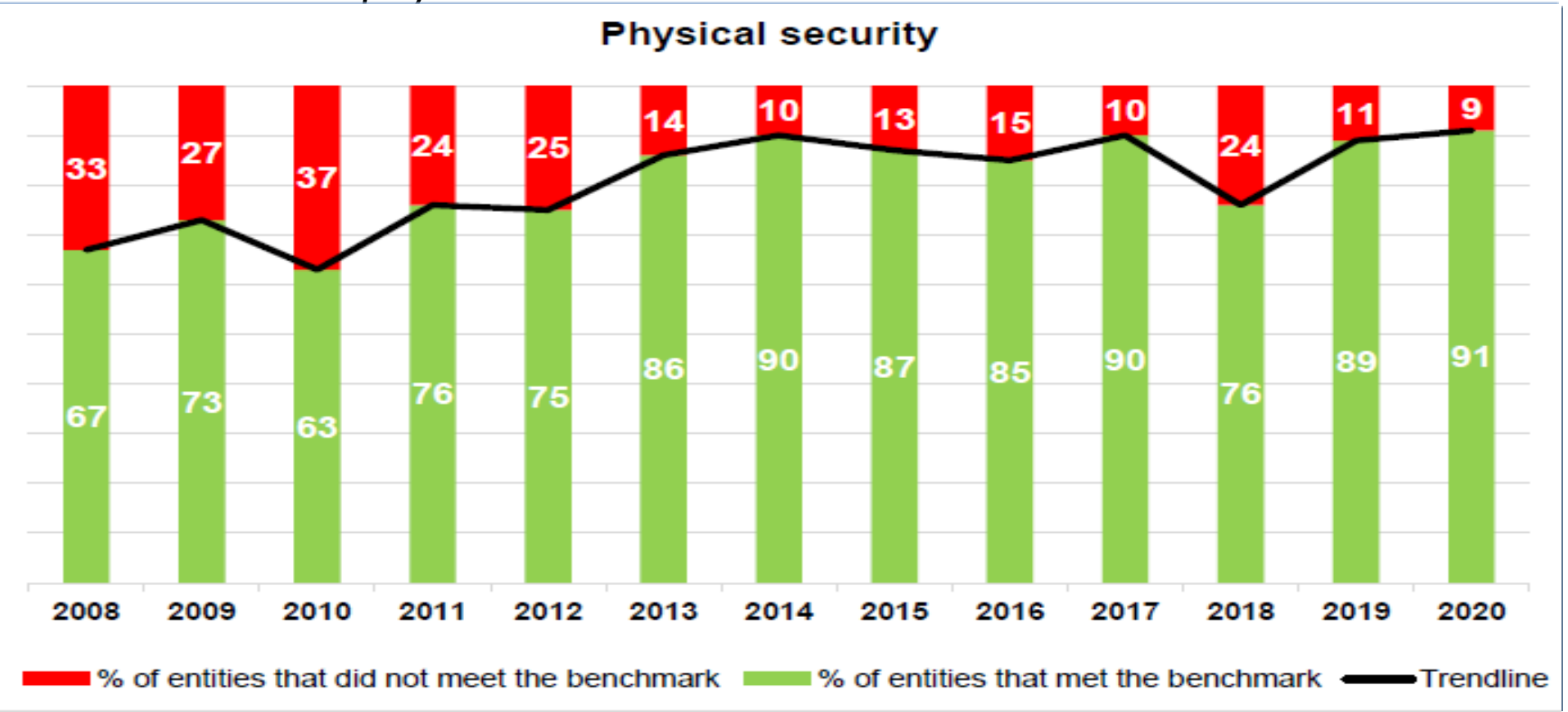
- *Without appropriate IT risk policies and practices, entities may not identify and mitigate threats within reasonable timeframes.*
- *Entities may not meet their business objectives when risks are not identified and appropriately managed.*
- ***Change control***
- *Entities' change control practices continue to improve with 85% meeting our benchmark in 2019-20.*
- *We examined if system changes are appropriately authorised, implemented, recorded and tested.*
- *We reviewed any new applications acquired or developed to evaluate if the changes were made in line with management's intentions*
- *An overarching change control framework is essential to ensuring changes are made consistently, reliably and efficiently. When examining change control, we expect entities to be following their approved change management procedures*

Change control – % of entities that met benchmark



Physical security

- *91 % percent of entities met our expectations for the management of physical security. 24 % percent more entities are now meeting the benchmark since our first assessment in 2008.*
- *We examined if entities' IT systems were protected against environmental hazards and related damage. We also reviewed if entities had implemented and monitored physical access restrictions*



ICAI Guidance Note on IS Audit

- Board of Advanced Studies & Research of the Institute of Cost Accountants of India has taken an initiative to release a **Guidance Note on Information System Audit** for *the Industry at large.*
- Institute has considered inputs from C&AG, SEBI and other regulators

‘Information Security’ Check List

- **Security Policy - Governance, Implementation & Review:**

Whether there exists a well-documented Information security policy?	Yes / No
When was the policy last approved by the Board of directors / Management?	MM / DD / YY
What is the review frequency of the policy?	Quarterly / Half-yearly / Yearly
When was the last review conducted?	MM / DD / YY
What was the last review purpose?	a. Periodic.
	b. Incident driven.
	c. Infrastructure changes.
Whether the policy addresses legal and regulatory requirements?	Yes / No
Who is the security policy owner for maintenance and review?	a. Board of directors.
	b. Security Committee.
	c. CISO.
Whether IS Committee is constituted comprising of representatives from all verticals?	Yes / No
What is the meeting frequency of the IS committee?	Quarterly / Half-yearly / Yearly

Part 2

Whether the role and responsibilities of IS committee is clearly defined?	Yes / No
Whether the role and responsibilities of CISO is clearly defined?	Yes / No
Whether the policy is communicated to relevant users?	Yes / No
What is the medium of communication?	a. Email.
	b. Intranet.
	c. In-house Periodic trainings.
	d. Induction training for new Recruits.
	e. Undertaking.
Whether supporting procedures / sub-policies have been developed for organizational security?	Yes / No
Who reviews the supporting procedures / sub-policies?	a. CISO.
	b. IS Committee.

Part 3

Whether security policy is in line with global best practices guidelines like ISO 27001 (and other frameworks like COBIT etc.) and / or as per requirements of RBI circular?	Yes / No
Whether every procedure / sub-policy has a designated owner?	Yes / No
Whether the policy takes into consideration the long-term business strategy of the organisation?	Yes / No
Whether the organisation has considered IS security for budgetary allocation?	Yes / No
Whether independent audit is conducted to ensure adherence to security policy?	Yes / No
Frequency of internal audit.	Quarterly / Half-yearly / Yearly
Frequency of external audit.	Quarterly / Half-yearly / Yearly / Bi-annually

Asset Classification and Control - Accountability of Assets: ICMAI GN - Checklist

Whether the organization has distinguished its information assets?	Yes / No
Whether an inventory database is maintained for all information assets?	Yes / No
Whether there is a designated owner for each distinguished asset?	Yes / No
How is the inventory database maintained	Centrally / Locally
Whether a separate asset inventory exists for data centre and DR site?	Yes / No
Whether there is a designated owner for the data centre asset inventory?	Yes / No
Whether a process exist for updation of asset inventory?	Yes / No
Whether each information asset is labeled?	Yes / No
Whether information classification guidelines exist and are enforced?	Yes / No
Whether the classification level of information asset is reviewed periodically?	Yes / No

Who is responsible for deciding the asset classification level?	a. IS Committee.
	b. CISO.
	c. Asset owner.
Whether classification level for each asset is recorded in inventory database?	Yes / No

Human Resource Security:

How do you communicate individual security roles and responsibilities to employee end users?	a. Employment contract.
	b. Induction trainings.
	c. Periodic IS awareness trainings.
Is there a training calendar for IS awareness trainings?	Yes / No
Number of IS awareness trainings conducted in a year.	
Number of induction trainings conducted in a year.	
Whether a background verification check is part of the recruitment process of the organisation?	Yes / No
How the background verification check is conducted?	a. In-house.
	b Outsourced.
Whether employment contract covers non-disclosure / confidentiality clause?	Yes / No
Whether written acknowledgement w.r.t understanding and acceptance ofemployment contract is obtained?	Yes / No
Whether employment contract covers appropriate controls to address post-employment responsibilities?	Yes / No

Third Party Security / Vendor Management:

How do you communicate individual security roles and responsibilities to third party users?	a. Third party contract.
	b. Periodic IS awareness trainings.
	c. Both.
Whether a background verification check is a mandatory requirement in third party contracts?	Yes / No
What process there is to ensure background verification check is performed?	a. SLA review.
	b Third party audit.
Whether third party contract mentions adherence to security policy and procedures of the organization?	Yes / No
Whether third party contract covers non-disclosure / confidentiality clause?	Yes / No
Whether written acknowledgement w.r.t understanding and acceptance of third-party contract is obtained?	Yes / No
Do you conduct due diligence for third parties / vendor before outsourcing?	Yes / No
Do you conduct onsite security audit of third party / vendor before outsourcing?	Yes / No
Have you identified the risks associated with third party contractors working on- site?	Yes / No
Do you conduct periodic reviews of all accesses provided to third parties / Vendor?	Yes / No
What is the frequency of such reviews?	Monthly / Quarterly / Yearly
Whether the CISO reviews all security controls w.r.t third party contracts?	Yes / No

ICMAI GN on IS Audit
'Migration to IT System'- Ex - SAP

- **Detailed analysis of the existing systems, bringing out**:
- Scope and functions of the systems.
- Volume, type and periodicity of transactions.
- Records maintained in the system, with specimen copies of forms used.
- Flow of information through the system.
- Significant weak points in the system and bottlenecks experienced in the actual operation of the system.

- **Detailed description of the proposed IT System indicating clearly**:
- The functions which will be transferred to the computer.
- The functions which will continue to be performed manually and the extent to which and manner in which these are proposed to be modified in the context of introduction of IT System.
- The records to be maintained manually with specimen copies of forms in which they are proposed to be maintained; and
- An overall narrative description and accompanying flow chart of the general flow of information through the system.

- **The design specifications, which describe the logic of the proposed IT system, including**:
- Flow charts showing significant operations to be performed by each proposed computer run.
- For each computer programme, a brief description of the functions to be performed, types of input and the resulting products.
- Input and output forms and file lay-out, including the descriptions of physical characteristics of the data elements to be contained in the transaction records and data files and the media to be used.
- The system of codification and the compatibility envisaged between different types of codes.
  - The time-schedule of operations, with specific target dates prescribed for each operation and
- Description of controls to be provided over data.
- Inputs, including the types and purpose of edit and other purification and validation routines.
    - Processing, including the plan for back-up operations.
    - Storage, including plans for reconstruction of data files; and
    - Outputs.
- Deviations from the provisions of the relevant rules, codes or manuals.

Information requirement

- **IT System Migration Audit**
- plan of switch over to the new IT System, including:
- The phased programme of conversion.
- Any special difficulties anticipated in conversion,
- measures proposed to be taken to overcome them with particular reference to the special action, if any necessary for cleaning up or purification of manual records before transfer to IT System.
- Copies of Procedure ,Officer Orders, Manual etc. prepared in connection with the New System.

ICMAI GN on IS Audit

- **Government Sponsored Schemes IS Audit**
- Government (Central or State) Sponsored Schemes Audit is a way of measuring, understanding, reporting and ultimately improving an organization's social and ethical performance.
- **Government Sponsored Schemes Audit helps to narrow gaps between vision/ goal and reality, between efficiency and effectiveness and so creates an impact upon governance.** The success of process of Government Sponsored Schemes Audit lies in its potential to make certain aspects of organizational activity more transparent to external stakeholders, who may then be empowered to hold management accountable for their actions insofar as they are affected by them.
- Government Sponsored Schemes Audit is based on the need of organizations to create a balance in the way they plan and measure their commercial and non-commercial operations, and to prove that there is consistency between what an organization says it will do and what it actually does.
- IS Auditors can play a vital role in the Government IS Audit reporting framework **by ensuring the effectiveness of the Government Sponsored Schemes program in non-corporate as well as corporate sector, which in turn would contribute positively to the society at large.**

Recap of SAP

- SAP = Systems Applications And Products In Data Processing.
- SAP, by definition, is also the name of the BRP (Business Resource Planning) software & name of the company.
- SAP Software = European (Germany) multinational.
- It has over 425,000 customers in over 180+ countries.
- Develop software solutions for managing business operations and customer relationships.

 SAP software products provide powerful instruments for helping companies to manage their financials, logistics, HR & other business areas.

The backbone of SAP software offering is SAP ERP system = One of the most advanced ERP system from currently available ones.

SAP R/3

- SAP = Systems, Applications and Products in Data Processing (R = real time, 3 = 3 tier)
- German Based Company
- 3rd Largest Independent Software Vendor in the World
- SAP: ERP Market Leader
- 80% Fortune 500 Companies Use SAP
- Over 21,500 Customers in 120+ Countries
- Over 15 million users
- **SAP R/3**
- Client/Server Technology
- Highly Customizable
- Based on Industry Specific Best Practices
- Multi-lingual: International

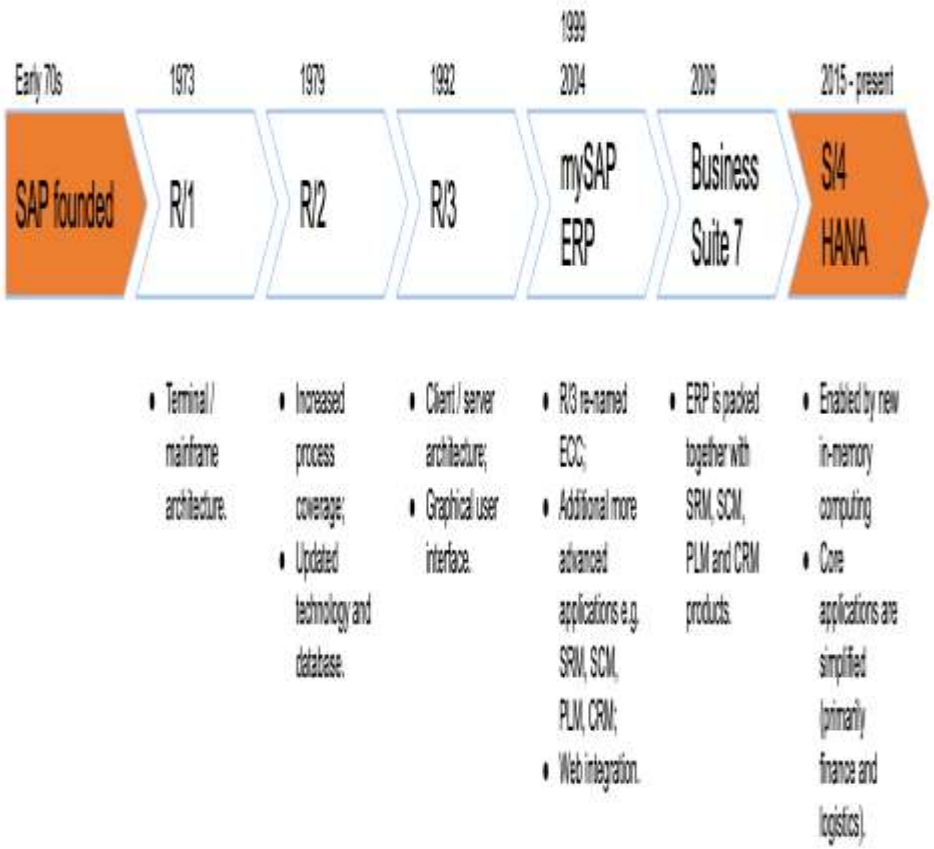
SAP S/4 HANA

- SAP S/4HANA stands for SAP Business Suite 4 SAP HANA.
- Next big wave of innovation to SAP customers, similar to transition from SAP R/2 to SAP R/3.
- **3 options are available:**

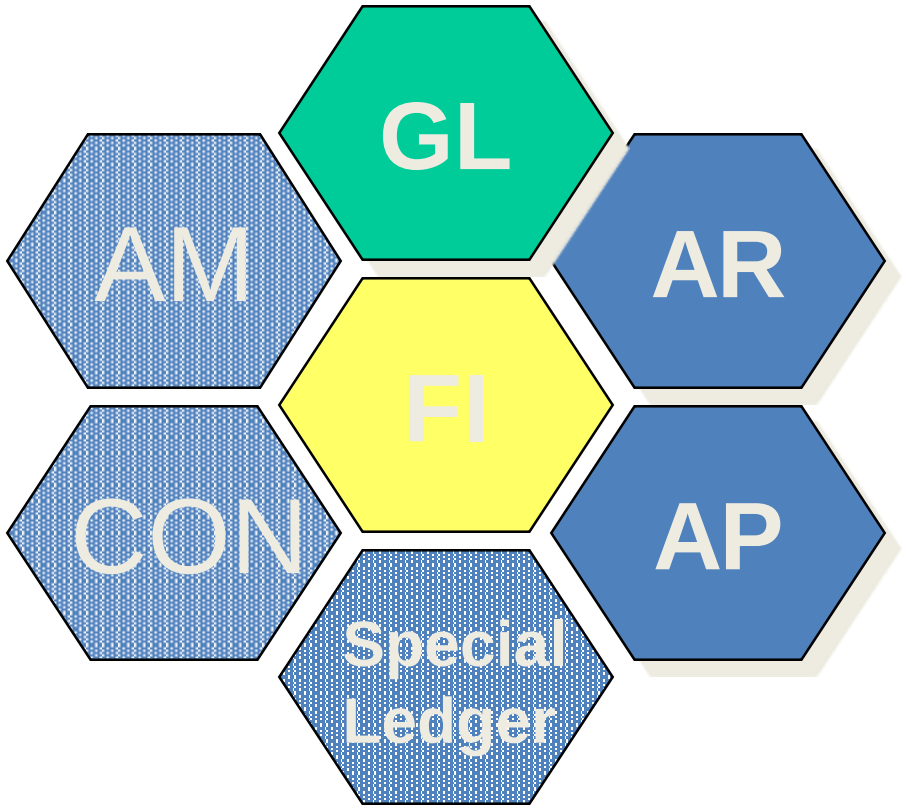
❖ On-premise

❖ Cloud

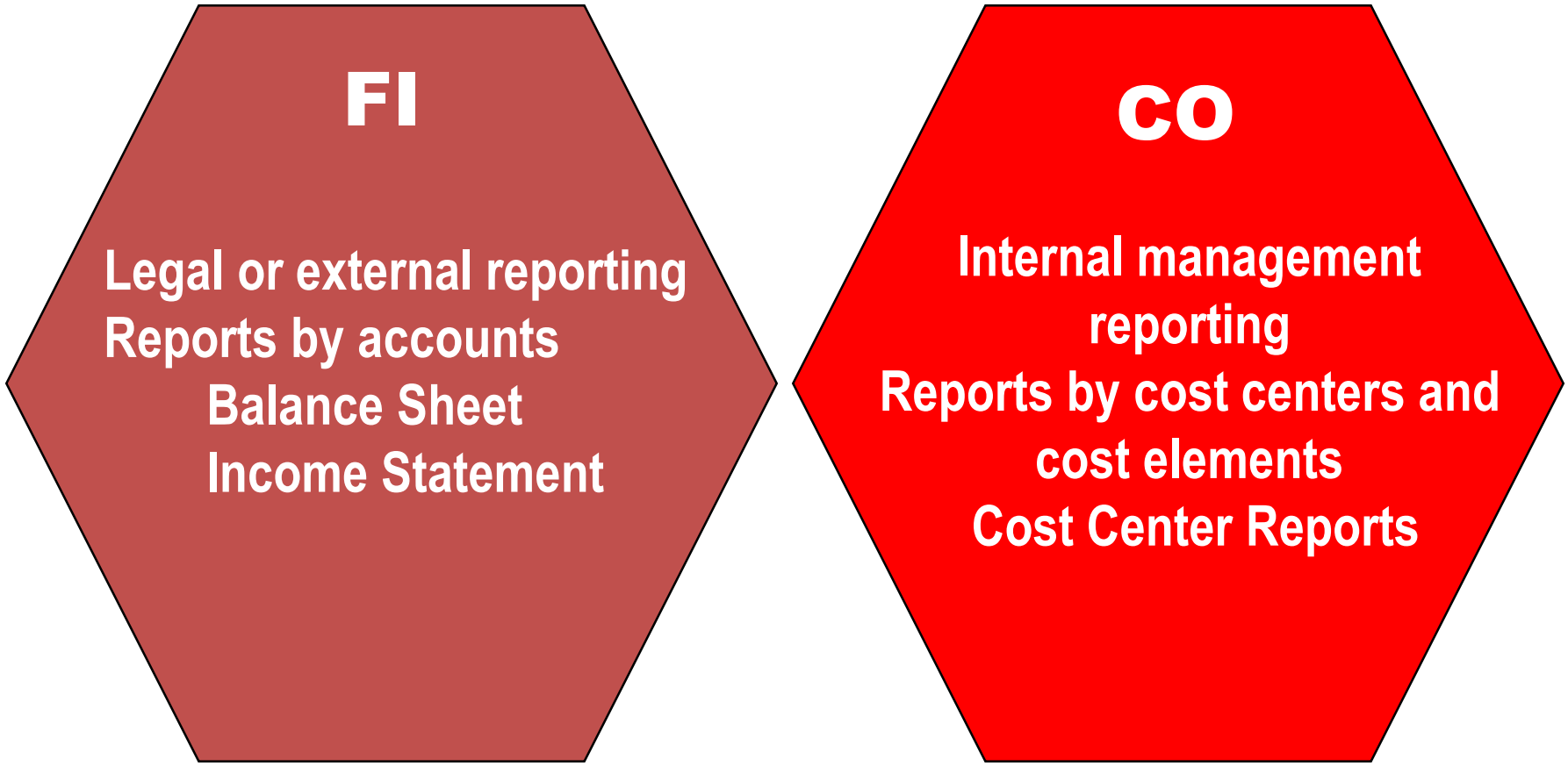
❖ Hybrid deployments to give real choice to customers.



FI Overview



FI & CO comparison



SAP - Advantages

1. One central database
2. Real time processing
3. Allows integration of legacy systems
4. Document Balancing
5. Manages Work flow

- **Disadvantages**

1. Data integrity must be maintained by all users
2. Numerous tables and Documents
3. Audit trails can disappear in data extractions

Exam related MCQ

1. SAP HANA was launched in

a) 2005
b) 2008
c) 2010
d) 2015

- Answer – c
- 2. _____ is the default programming language for SAP applications.

a) SAP GRC
b) SAP R/2
c) ABAP
d) None of the above

- Answer = c
- 3. _____ is a set of data that is needed for processing of transaction data and remains unchanged over large number of such transactions.

a) Constant
b) Meta
c) Uniform
d) Master

- **Answer- d**

- **4.** Controlling (CO) is usually a part of which Module of SAP ?

a) Sales & Distribution

b) Human Resource

c) Accounting

d) Materials management

- Answer – c
- 5. One of the latest version of SAP is :
- *A. SAP R1*
- *B. SAP S/2*
- *C. SAP R/3*
- *D. SAP S4 HANA*
- 6. The letter ‘S’ in S4 HANA stands for / implies ?
- *A. Systems*
- *B. Suite (business)*
- *C. Strategy*
- *D. none of the above*
- Answer= b

Thank You