



STALLION.AI

DICTIONARY OF KEY TERMS

stallion.ai

Stallion.ai - Dictionary of Key Terms

Internal Audit Terminology	3
Internal Audit	3
Documented Unmitigated Risk	3
Risk Areas	3
Internal Audit Report Findings vs. Internal Audit Report Observations	3
Control Objectives	4
Control objectives based on Standards/known frameworks	4
Trust Services Principles (Until 2017)/ Trust Services Criteria (Post-2017)	5
The Practice of Integrated Risk Management	6
Long-term Trend in industry; Continuous Auditing	6
Audit Planning & Internal Audit Process	7
Definition of the Audit Universe (Source)	7
The Internal Audit Process	8
Completeness of Audit (or Audit Program) Coverage	8
vs.	8
Audit Completeness	8
Audit Criteria	8
Planning trends in 2018	8

Internal Audit Terminology

Internal Audit

Internal audit is a dynamic profession involved in helping organisations achieve their objectives. It is concerned with evaluating and improving the effectiveness of risk management, control and governance processes in an organisation. (IIA Australia)

Documented Unmitigated Risk

Internal Audit Findings and observations that reveal breakages in processes through audit reports. Although the complete list of controls evaluated as part of the audit may be black-boxed, however, the report in that of itself indicates the performance of their aggregate control objectives.

Risk Areas

Risk areas are categories of risk specifically tailored to address the types of impacts that could befall the business should they materialize. it's the different ways things can go wrong.

Internal Audit Report Findings vs. Internal Audit Report Observations	
Internal Audit Report Findings	Internal Audit Report Observations
<p>Risk-and-Control associated notes regarding the performance of a control or materialization of a risk as part of audit fieldwork.</p> <p>These are what support the final conclusion of the audit report, as well as become the grounds for the top-of-list recommendations (Also noted in the audit report)</p>	<p>Process or operations related notes of interest that are documented as part of the audit report. These observations usually pertain to process particularities.</p> <p>Particular observations, or trends in observations may be mentioned as part of the recommendations section of the audit report</p>

Control

Activity performed consciously as part of a process that mitigates the occurrence of a known (and even some unknown) risks threatening an organization.

Control Objectives

Much like risk areas, control objectives are designed to be major subcategories of controls used to regroup all controls speaking to a program’s mandate, or higher-larger compliance/business performance/process goal. These “roll-up” goals can be at times cited, or alluded to in smaller, more focused audit reports’ criteria section. Control Objectives can be deemed to have been achieved/performed to a satisfactory level within the audit period, or otherwise, can be noted as not achieved. (Any failures will be explained in larger detail)

Control objectives based on Standards/known frameworks

Examples:

- ISO series have documented, structure principles upon which to evaluate compliance and performance.
- SOC reports Type 1 (Internal controls over financial reporting for service organizations)
- SOC reports Type 2 (Controls over information protection for service organizations)

SOC Report Comparison

	WHAT IT REPORTS ON	WHO USES IT
SOC 1	Internal controls over financial reporting	User auditor and users controllers office
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Shared under NDA by management, regulators and others
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Publicly available to anyone

ImageSource: <http://resource.onlinetech.com/soc-1-soc-2-soc-3-report-comparison/>

Trust Services Principles (Until 2017)/ Trust Services Criteria (Post-2017)

Service Organizations' clients trust that the processing and storage of their resources is handled with an openly communicated level of risk management. The service principles are the fundamental pillars of governance/accountability that are communicated to said clients.

The TSC serve as control criteria use in consulting engagements/attestations to assess and report on controls for information and systems. These controls may cover areas that include any subset of a business entity. (subsidiary, internal function, delivery of a service as part of a larger process)

The risk areas identified as pillars are: Security, Availability, Processing Integrity, Confidentiality, and Privacy. These 5 areas are applied as a focused extension of the 17 COSO principles of internal controls which would normally be applied to Internal controls over financial reporting (ICFR) reports. (see image below)

COSO's 17 principles of internal control-summarized

Control environment	Risk assessment	Control activities	Information and communication	Monitoring activities
<p>01 Demonstrates commitment to integrity and ethical values</p> <p>02 Exercises oversight responsibilities</p> <p>03 Establishes structure, authority and responsibility</p> <p>04 Demonstrates commitment to competence</p> <p>05 Enforces accountability</p>	<p>06 Specify suitable objectives</p> <p>07 Identifies and analyzes risk</p> <p>08 Assess fraud risk</p> <p>09 Identifies and analyzes significant change</p>	<p>10 Select and develops control activities</p> <p>11 Selects and develops general control over technology</p> <p>12 Deploys through policies and procedures</p>	<p>13 Uses relevant information</p> <p>14 Communicates internal</p> <p>15 Communicates externally</p>	<p>16 Conducts ongoing and/or separate evaluations</p> <p>17 Evaluates and communicates deficiencies</p>

The Practice of Integrated Risk Management

Practice of understand and manage the full scope of risks (strategic, operational, financial, digital, etc.) in order to manage new risk, as well as existing exposure through both domains (security, privacy, etc.) and verticals (operational to strategic risk)

Long-term Trend in industry; Continuous Auditing

With a ludicrous amount of automation, Internal audit functions will be in position to conduct internal investigations on an event basis, as all process-related information will be captured by a system.

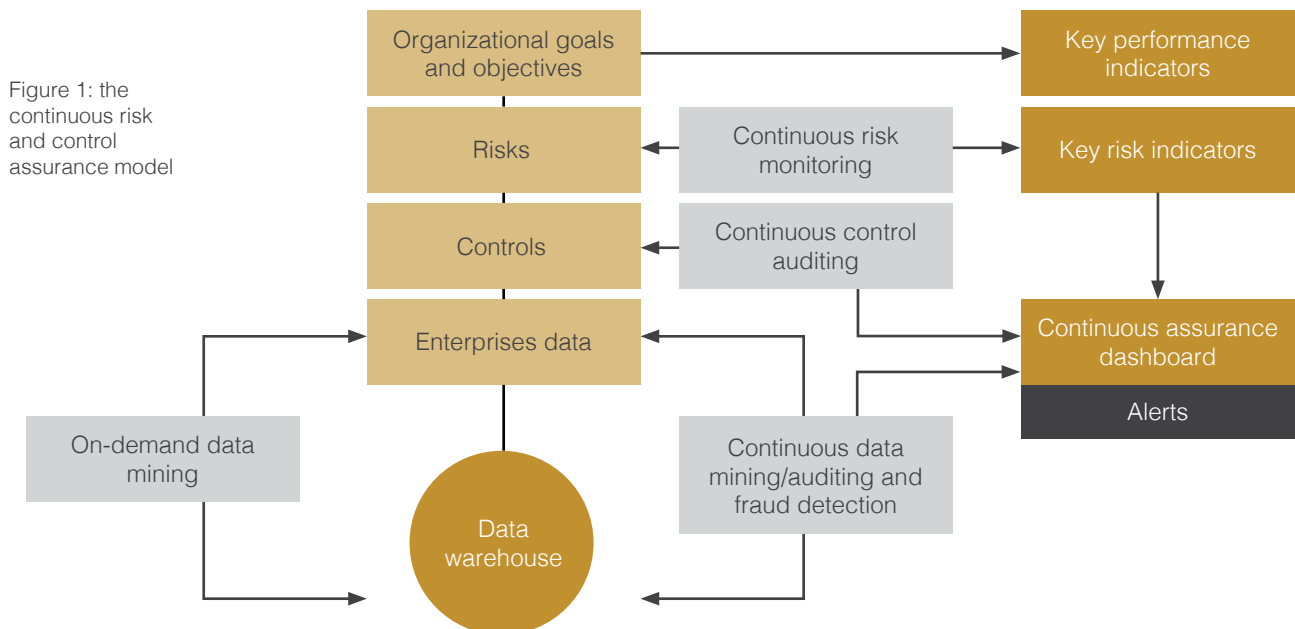


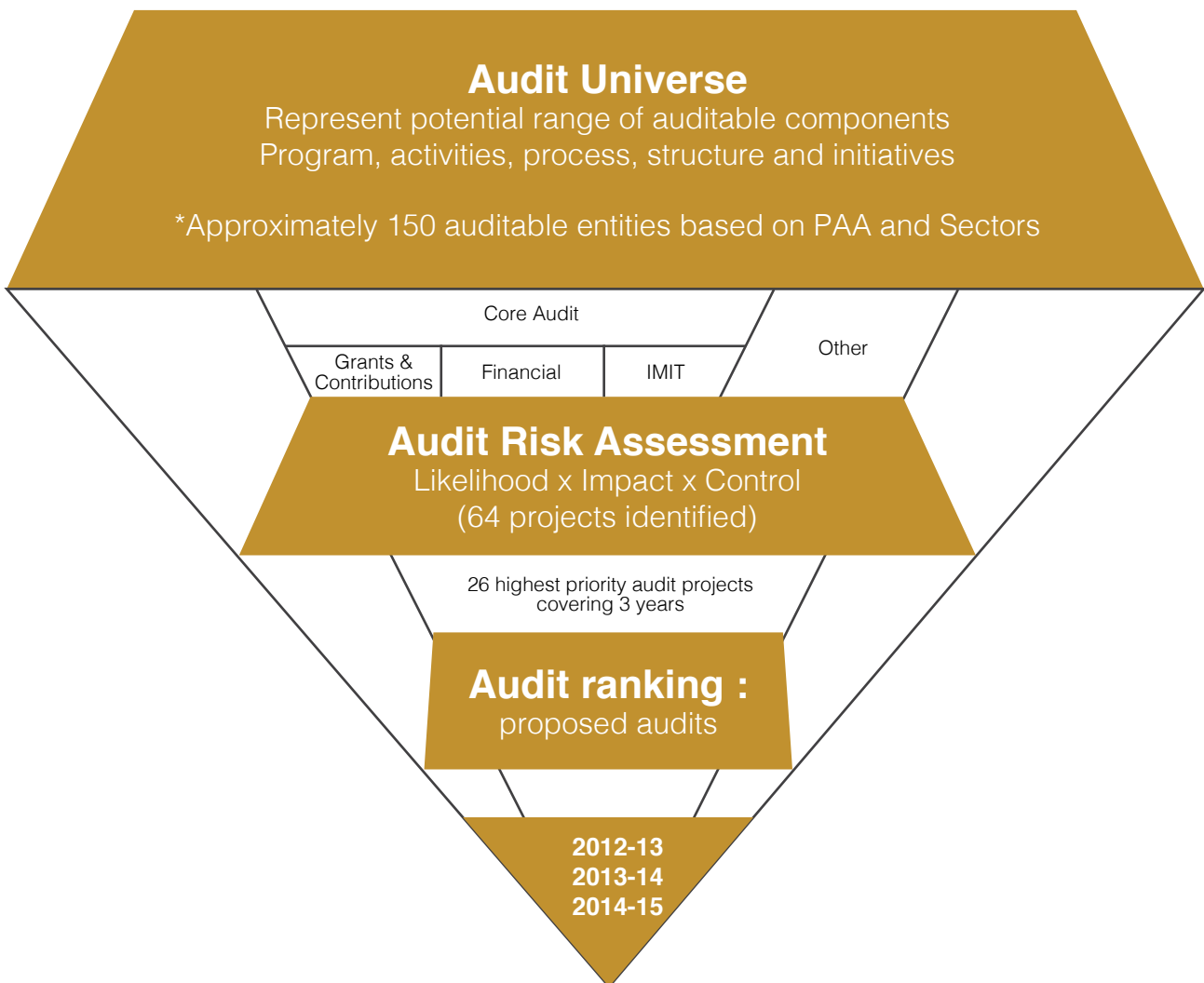
Table 1: Changes taking place in internal auditing

	Historic	Mainstream	Cutting-Edge
Focus	Audit entitles based on rotational plan	Prioritize audit entitles based on risk	Focus on strategic, business and process risk
Perspective	Historic	Historic	Historic
Style	Corporate police	“Father knows best”	Consultant and advisor
Mandate	Compliance with policies & procedures	Assurance on financial control ; compliance	Business assurance
Risk focus	Financial	Financial plus	Enterprises risks
Tool kit	Compliance work programs	Audit work program for key processes; control	Risk frameworks, self-assessments
Technology	None	Automated work papers	Automated testing and continuous monitoring

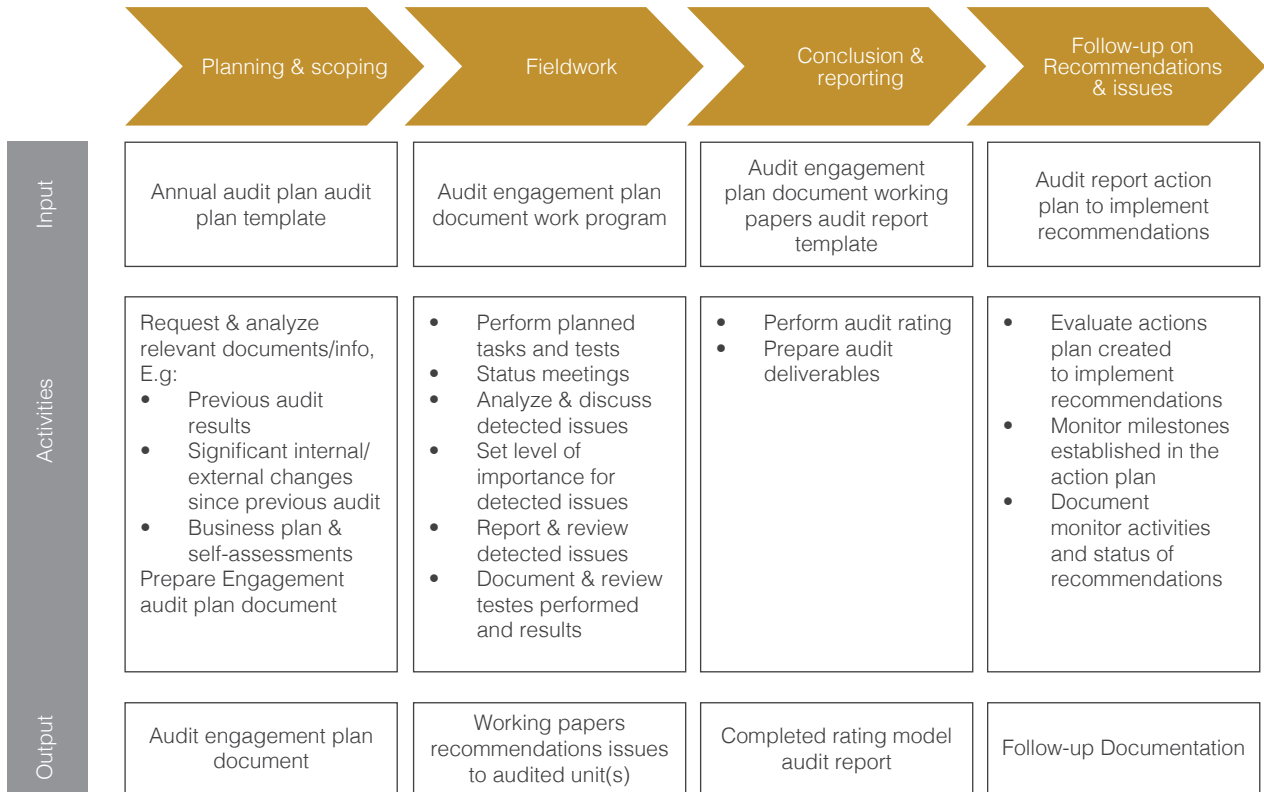
Internal Audit of the Future - SAP 2018

Audit Planning & Internal Audit Process

Definition of the Audit Universe (Source)



The Internal Audit Process



Source: Helsinki Metropolia University of Applied Sciences

Completeness of Audit (or Audit Program) Coverage vs. Audit Completeness	
Completeness of Audit Coverage (or Audit Program)	Audit Completeness
The qualitative degree to which the scope of audit (or audit Program) is representative of the unique types and subsections of business operations under evaluation.	... is determined by the perceived reliability and accuracy of the source from which audit evidence is obtained. This is determined during the "Conduct"/Fieldwork phase of an engagement.

Audit Criteria

are the high-level points of evaluation/points of focus that are directly tied to strategic and tactical objectives set in audit programs. These are used to lead as part of performing the evaluation business operations.



STALLION.AI

Contact Us:
hello@stallion.ai
+971 44 270774

Stallion Tech Inc.
900 Lady Ellen Place, Suit 114,
Ottawa, ON, K1Z 5L5, Canada
Contact: +1 (604) 781 9481

Office # 1104, Executive Tower D
(Aspect Tower), Al Abraj Street,
Business Bay, Dubai - UAE
Contact: +971 44 270774

hello@stallion.ai www.stallion.ai