



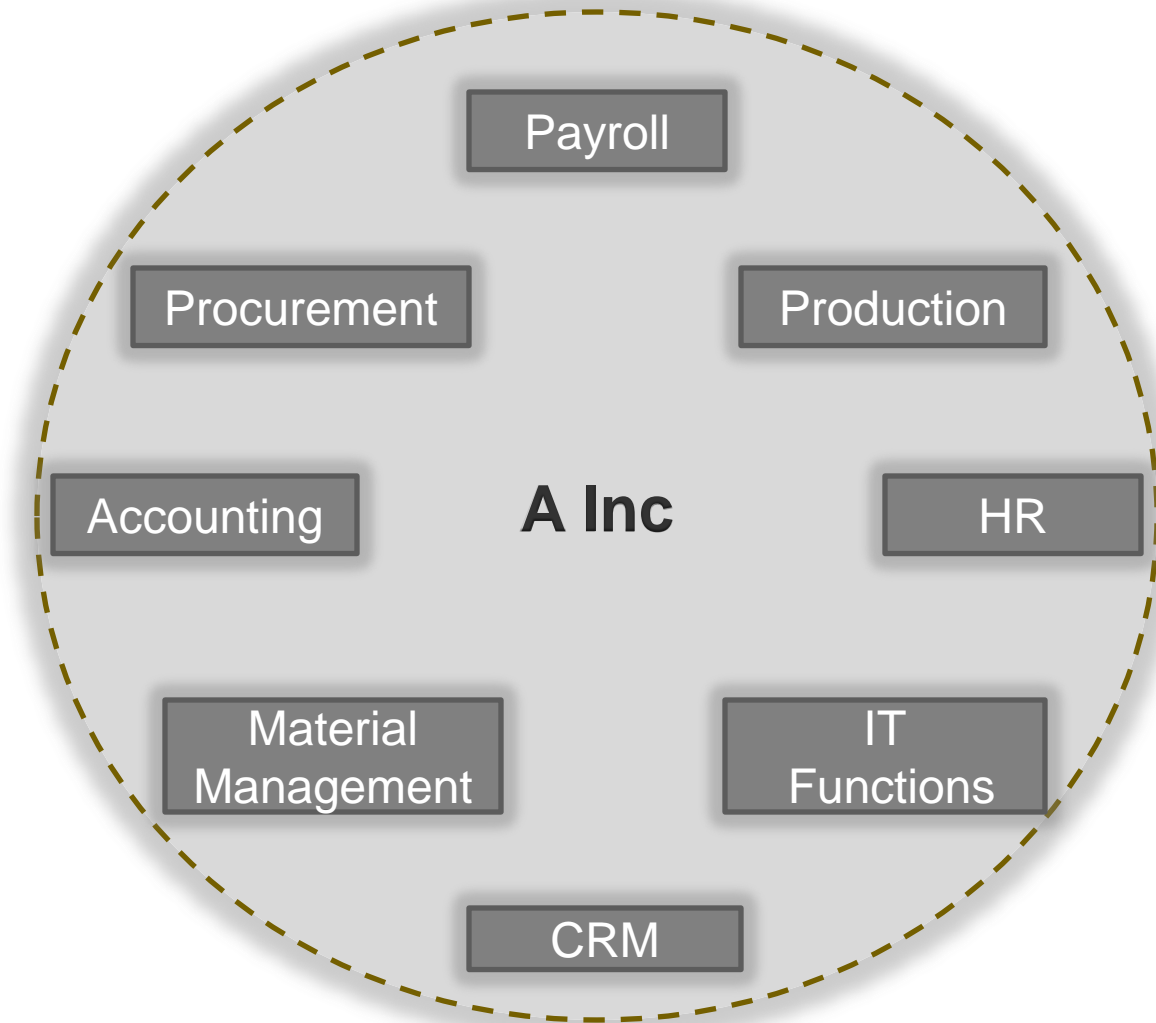
# **SAS 70**

## **Role of Service Auditors**

Sadagopan Raghavan T (ACA, Grad CWA, CISA)  
Manager – Ernst & Young

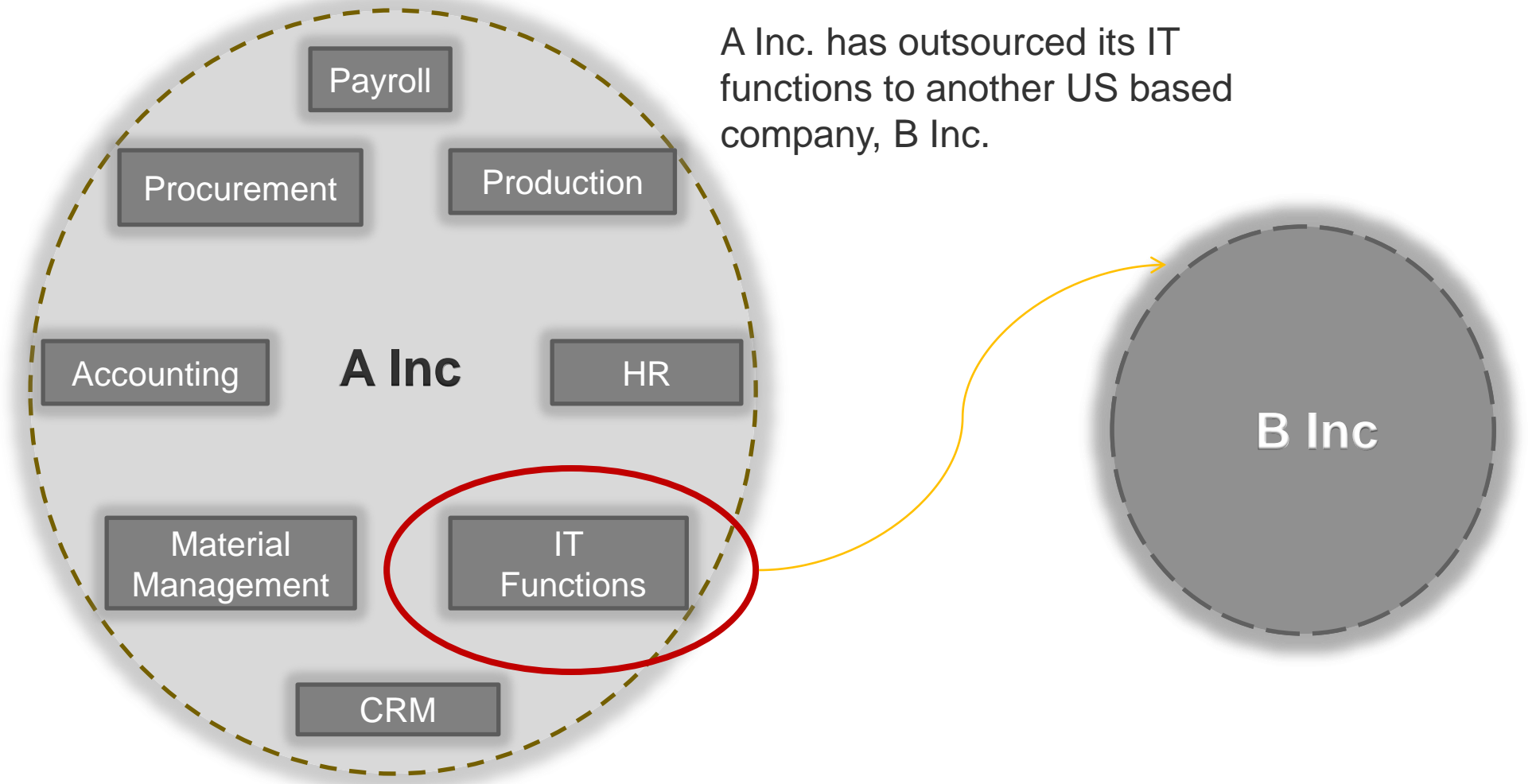
# Setting the context

---

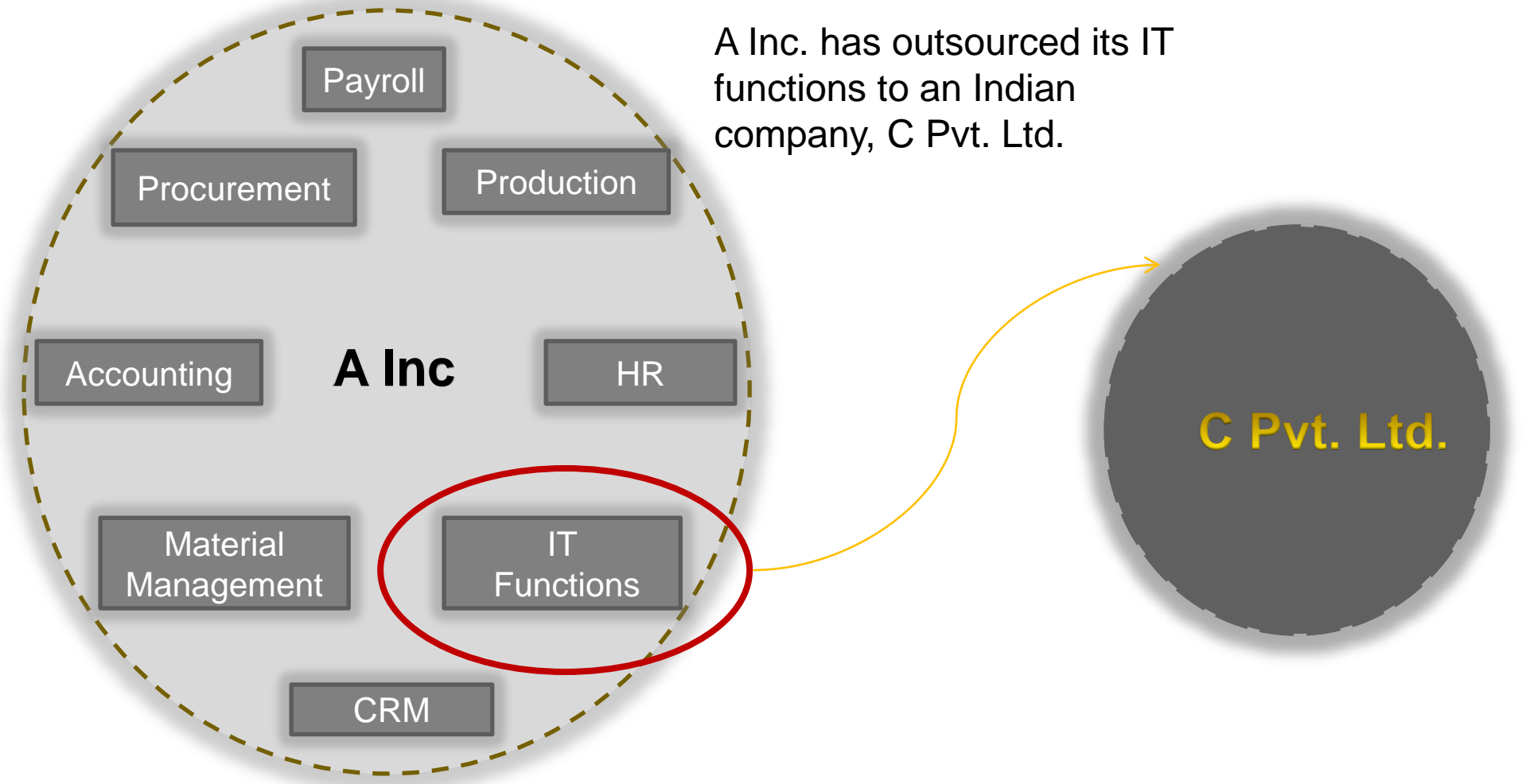


The Core Functions of the organization are managed internally by A Inc, a Company based out of USA.

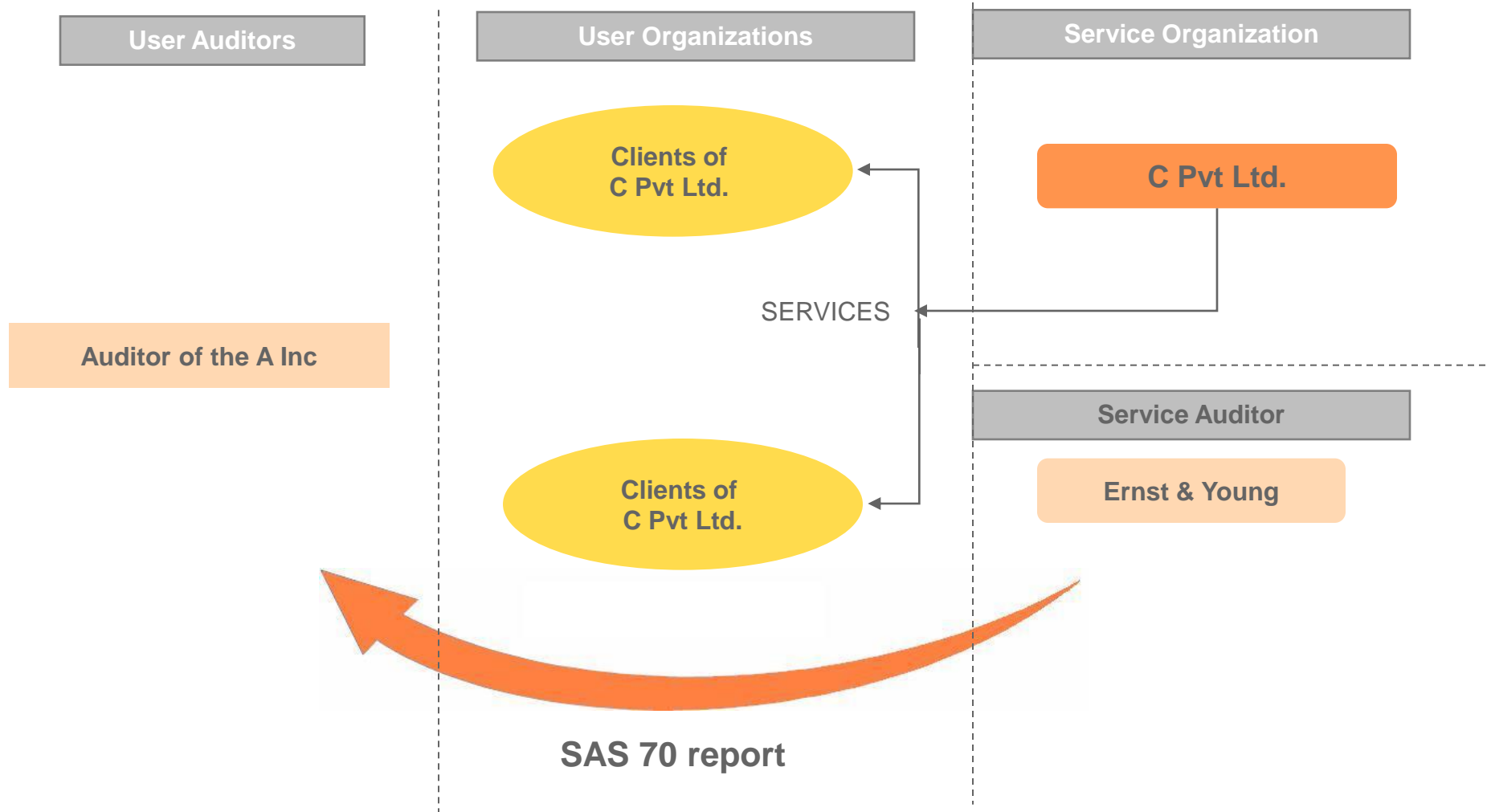
# Setting the context



# Setting the context



# Setting the context



---

# Key Terms

---

**SAS 70** - The AICPA's Statement on Auditing Standards No. 70 "Service Organizations"  
(SAS 70)

**"User organization"** - The entity that has engaged a service organization and whose financial statements are being audited.

**"User auditor"** - The auditor who reports on the financial statements of the user organization.

---

# Key Terms

---

**“Service Organization”** - The entity (or segment of an entity) that provides services to a user organization that are part of the user organization's information system.

**“Service auditor”** - The auditor who reports on controls of a service organization that may be relevant to a user organization's internal control as it relates to an audit of financial statements.

---

# Key Terms

---

**Control Objective** - A Statement of the desired result or purpose to be achieved by implementing control procedures in a particular activity.

**Controls** - Policies and procedures, practices & organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected

---

# Why do we need SAS 70

---

What do we need SAS 70

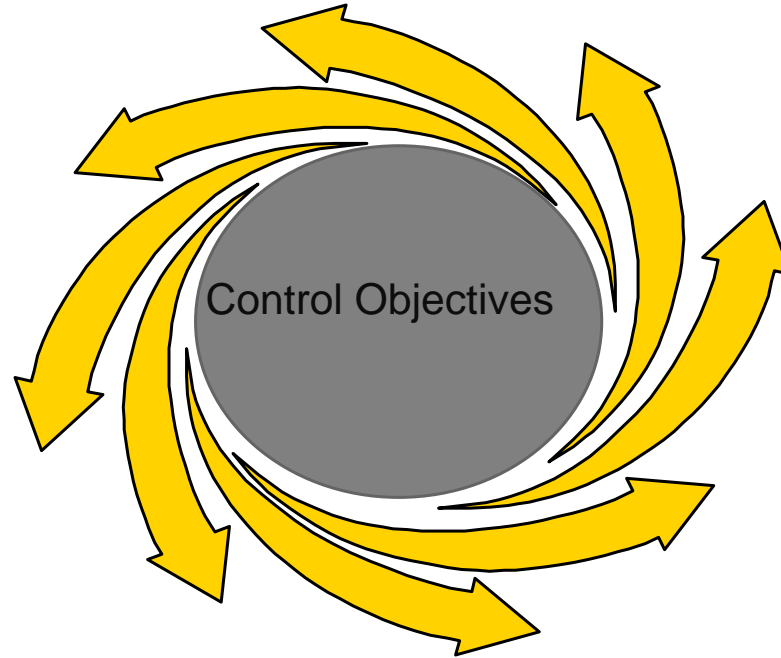
For the User Auditors to **rely on the controls** in operation **at the Service Organization**

Which have a **bearing on the financial statements** of the **user organization**,

For the purpose of their **audit at the User Organization**.

# Types of Service Organizations

---



## Software Development:

Emphasis on SDLC processes, and maintenance activities, backup and other Information technology general controls

## Infrastructure Management:

Emphasis on Incident Management, Service Management, and Change Management

## Business Processing Outsourcing:

Emphasis on Transaction Processing, and other Information technology general controls

# Types of SAS 70 Report

---

| Opinion  | Type I | Type II |
|--|--------|---------|
| Whether the service organisation's description of its controls presents fairly, in all material respects, the relevant aspects of the service organisation's controls that had been placed in operation as of a specific date. | ✓      | ✓       |
| Whether the controls were suitably designed to achieve specified control objectives  | ✓      | ✓       |
| Whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified                    | ✗      | ✓       |

---

# Structure of a SAS 70 report

---

Section I – Service Auditors Report **Service Auditor's Responsibility**

Section II – Description of Controls provided by **Service Organization's responsibility**

- ▶ General Information
- ▶ Overview of Internal Control Environment
- ▶ Description of Controls (Control Objectives & Detailed control description)
- ▶ User Control considerations

Section III – Information provided by the Service Auditor **Service Auditor's responsibility**

- ▶ Objectives and Scope of the Review
- ▶ Tests of Control Environment Elements
- ▶ Control Objectives, Related Controls, Tests of Operating Effectiveness and Results of Testing

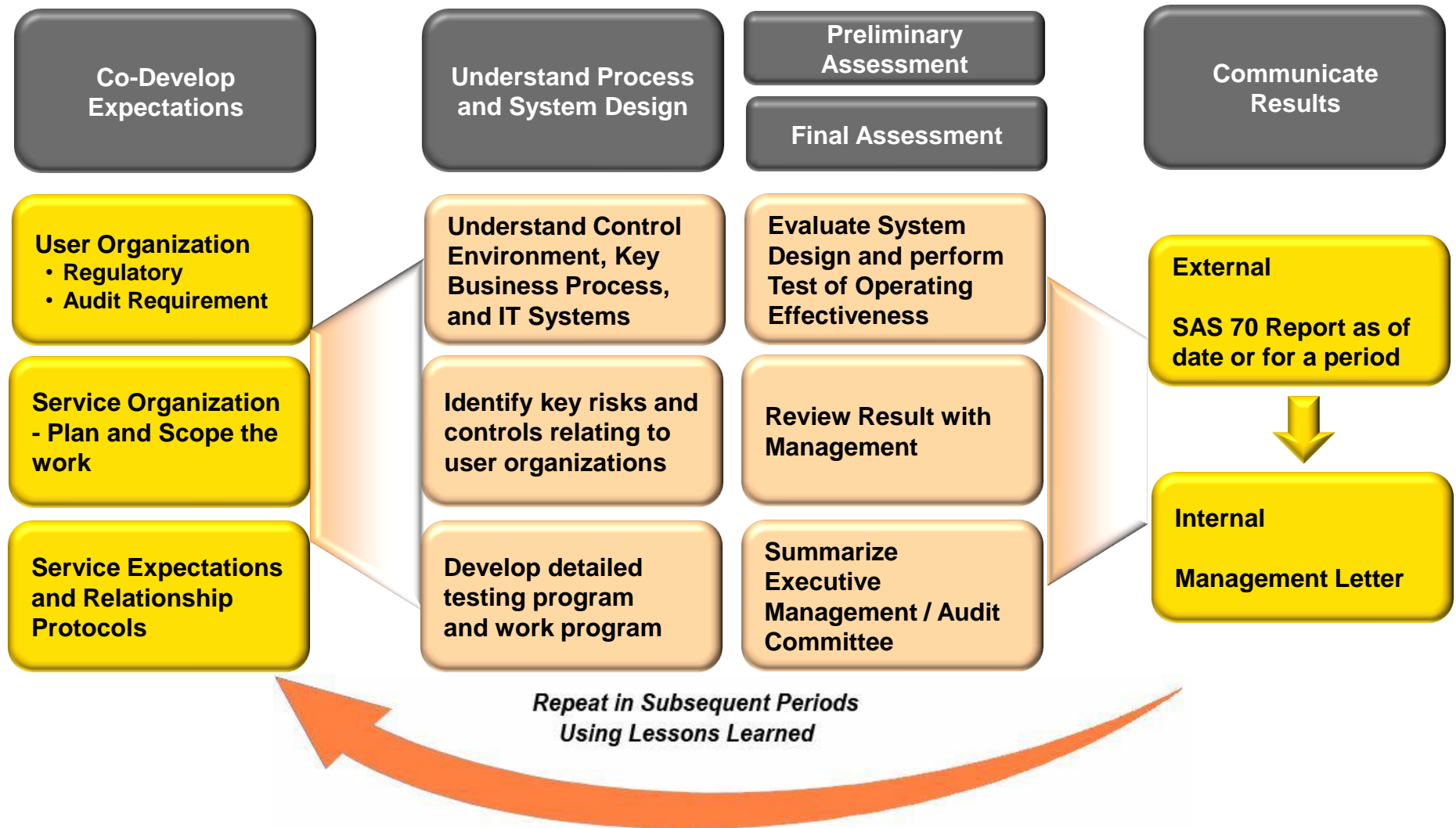
Section IV – Additional information provided by the service organization **Responsibility Service Organization**

---

# Structure of a SAS 70 report

---

# Approach and Methodology



# Co-Develop Expectations

## Activities

## Deliverables

SA

- ▶ Refine mutual understanding of scope of the SAS 70 examination;
- ▶ Understand key business goals and objectives;
- ▶ Understand regulatory requirements relating to infrastructure management of user organization;
- ▶ Determine expectations related to services, deliverables, timelines and communication protocols;
- ▶ Perform planning procedures; and
- ▶ Co-Develop Control Objectives.

- ▶ Agreed communication protocols and escalation mechanism and
- ▶ Project schedule.

SO

- ▶ Communicate user organization's specific control requirements;
- ▶ Identify key business process personnel forming a core SAS 70 team;
- ▶ Provide a SAS 70 liaison; and
- ▶ Confirm expectations with respect to services, deliverables, timelines, and communication protocols.

# Understand Process and System Design

## Activities

## Deliverables

SA

- ▶ Validate our understanding of the control environment, process flow, and IT systems;
- ▶ Refine control objectives;
- ▶ Refine 'What Could go Wrong' / 'Primary Control Procedures' with respect to each control objective; and
- ▶ Identify key controls that support attribute of the control objectives.

- ▶ Validated Description of Controls (Section II of Report).

SO

- ▶ Prepare description of controls documentation and
- ▶ Co-develop the control objectives with the user organizations and their auditors.

# Preliminary Assessment of Controls

## Activities

## Deliverables

SA

- ▶ Identify controls to be tested;
- ▶ Perform preliminary-assessment of controls;
- ▶ Evaluate suitability of control design; and
- ▶ Communicate / discuss issues and changes with Service Organization.

- ▶ Issue Log and
- ▶ Changes to Description of Controls (if any).

SO

- ▶ Review and validate control findings;
- ▶ Agree on EY's recommendations for controls remediation; and
- ▶ Develop action plans to implement recommendations.

# Perform Tests of Operating Effectiveness

|    | Activities  | Deliverables  |
|----|---|---|
| SA | <ul style="list-style-type: none"><li>▶ Perform operating effectiveness testing;</li><li>▶ Discuss findings, if any;</li><li>▶ Conclude on operating effectiveness; and</li><li>▶ Complete sections III and IV of the report.</li></ul> | <ul style="list-style-type: none"><li>▶ Periodic status reports and</li><li>▶ Periodic issue summary and disposition.</li></ul> |
| SO | <ul style="list-style-type: none"><li>▶ Provide access to personnel, documents and systems for controls testing and</li><li>▶ Provide management responses to findings during operating effectiveness testing.</li></ul>                |   |

# Communicate Results

|    | Activities   | Deliverables  |
|----|--|---|
| SA | <ul style="list-style-type: none"><li>▶ Perform executive review of report and</li><li>▶ Issue SAS 70 Type 2 report.</li></ul>                           | <ul style="list-style-type: none"><li>▶ SAS 70 Type 2 report.</li></ul> |
| SO | <ul style="list-style-type: none"><li>▶ Provide Letter of Representation and</li><li>▶ Share the SAS 70 Type 2 report with user organizations.</li></ul> |   |

---

# Control Objectives

---

## Application Development and Maintenance

- ▶ Controls provide reasonable assurance that **software coding, testing, quality assurance, and delivery activities** are **segregated**.
- ▶ Controls provide reasonable assurance that User Organization's requirements, which form the basis of development and/or customization, are **documented, analyzed, and agreed upon** by Service Organization.
- ▶ Controls provide reasonable assurance that software development and/or customization activities are planned, time and effort of the project are **monitored, and appropriate corrective action is taken as needed**.
- ▶ Controls provide reasonable assurance that the software is developed /customized as per the requirements finalized with User Organization, and it is **reviewed and/or tested before release**.

---

# Control Objectives

---

## Application Development and Maintenance

- ▶ Controls provide reasonable assurance that change requests received during the development life cycle are **documented, analyzed, and tested before release**.
- ▶ Controls provide reasonable assurance that the **correct version** of the software, **meeting the User Organization's requirements**, is shipped to User Organization.
- ▶ Controls provide reasonable assurance that change to software during support activities are **documented, analyzed, and tested before release**.

---

# Control Objectives

---

## IT General Controls

- ▶ Controls provide reasonable assurance that **physical access** to computer equipment, storage media, and program documentation is restricted to properly authorized individuals and environmental safeguards have been enforced.
- ▶ Controls provide reasonable assurance that **logical access** to Service Organization's system resources at its development centers is restricted to properly authorized individuals. Controls provide reasonable assurance that requests for logical access to User Organization's system resources are appropriately authorized.
- ▶ Controls provide reasonable assurance that information security over **confidential information** received from User Organization is appropriately maintained to prevent unauthorized access.

---

# Control Objectives

---

## IT General Controls

- ▶ Controls provide reasonable assurance that programs and data are regularly **backed up** and are stored at a secure off-site facility.
- ▶ Controls provide reasonable assurance that only **licensed software** is used for development/maintenance activities.

---

# Control Objectives

---

## Infrastructure Management

- ▶ Controls provide reasonable assurance that **Change Requests** are analyzed, accepted, planned, implemented, and are tested before release.
- ▶ Controls provide reasonable assurance that **Incident Requests** raised within Remedy are classified, responded, and resolved.
- ▶ Controls provide reasonable assurance that **Service Requests** raised within Remedy are classified and resolved.
- ▶ Controls provide reasonable assurance that **Problem Requests** raised within Remedy are analyzed, reviewed, and resolved.
- ▶ Controls provide reasonable assurance that **Microsoft security patches** are scheduled and tested before implementation in the Production Environment.

---

# Control Objectives

---

## BPO – Payroll Processing

- ▶ Controls provide reasonable assurance that input for payroll processing is **received from Authorized User Organization Personnel**.
- ▶ Controls provide reasonable assurance that payroll processing is performed **completely, accurately, and in a timely manner**.
- ▶ Controls provide reasonable assurance that payroll output data is **stored in a secure manner and are transmitted** to Authorized User Organization Personnel.
- ▶ Controls provide reasonable assurance that changes made to applications used for payroll processing are **documented, analyzed, tested, and approved before release**.

# Nature of Testing Strategies

---

- ▶ Inquiry
- ▶ Observation
- ▶ Inspection
- ▶ Re-performance

*Strategy often includes tests of controls conducted through an interim date, with procedures performed to update the evaluation of the controls through year-end.*



---

# Test Plan

---

---

# Sampling

---

- ▶ **Random selection** - Random selection is the selection of a sample in such a way that, for a given sample size, every sampling unit has the same probability of being selected as every other sampling unit in the population, and every possible combination of sampling units in the population has an equal chance of being selected.
- ▶ **Systematic selection** - Involves the auditor determining a uniform interval by dividing the number of physical units in the population by the sample size. A starting point is selected in the first interval, and one item is selected throughout the population at each of the uniform intervals from the starting point.
- ▶ **Haphazard selection** - Involves the auditor selecting sampling units without any conscious bias or predictability, that is, without following a structured technique and without any special reason for including or omitting items from the sample (e.g., avoiding difficult to locate items, or always choosing or avoiding the first or last entries on a page).

# EY Sampling Guidelines

---

| <b>Nature of Control and Frequency of Performance</b>    | <b>Minimum Number of Items to Test (Extent of Test of Controls)</b> |
|--|---|
| Manual control, performed many times per day             | At least 25   |
| Manual control, performed daily                          | At least 25   |
| Manual control, performed frequently but less than daily | 10% of the number of occurrences or at least 25                     |
| Manual control, performed weekly                         | At least 5  |
| Manual control, performed monthly                        | At least 2  |
| Manual control, performed quarterly                      | At least 2  |
| Manual control, performed annually                       | Test annually   |

| <b>Sample Size</b> | <b>Acceptable Error Rate</b> |
|--------------------|------------------------------|
| 25                 | 0                            |
| 40                 | 1                            |
| 60                 | 2                            |
| 90                 | 3                            |

---

# Qualified Reports

---

## Disclosure of an inaccuracy or omission in the service organization's description of its controls

### (Explanatory paragraph preceding the opinion paragraph)

The accompanying description states that XYZ Loan Servicer uses operator identification numbers and passwords to prevent unauthorized access to the system. Our inquiries of staff personnel and observation of activities indicate that such procedures are employed in Applications A and B but are not required to access the system in Applications C and D.

### (Opinion paragraph)

In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned applications presents fairly, in all material respects, the relevant aspects of XYZ Loan Servicer's controls that had been placed in operation as of June 30, 20X1.

---

# Qualified Reports

---

## Disclosure when a control objective has been omitted

### (Explanatory paragraph preceding the opinion paragraph)

The accompanying description of the controls does not include a control objective for the complete, accurate, and timely recording of loan payments by XYZ Loan Servicer. We believe that this control objective and the related controls that might achieve the control objective should be specified in the description of the controls because they are relevant to user organizations.

### (Opinion paragraph)

In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Loan Servicer's controls that had been placed in operation as of June 30, 20X1.

---

# Qualified Reports

---

## Disclosure of a significant deficiency in the design of the service organization's controls

### (Explanatory paragraph preceding the opinion paragraph)

As discussed in the accompanying description, XYZ Loan Servicer reconciles loan payments received with the output generated. The reconciliation procedures, however, do not include a control to follow-up on reconciling items and to obtain independent review of the reconciliation procedures. This results in the controls not being suitably designed to achieve the control objective, "Controls should provide reasonable assurance that all output is complete and accurate."

### (Opinion paragraph)

In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Loan Servicer's controls that had been placed in operation as of June 30, 20X1. Also, in our opinion, except for the deficiency in the design of the controls and its effects on the related control objective referred to in the preceding paragraph, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

---

# Qualified Reports

---

## Disclosure of a significant deficiency in the operation of the service organization's controls

### (Explanatory paragraph preceding the opinion paragraph)

As discussed in the accompanying description and in our description of the tests of operating effectiveness, XYZ Trust Department reconciles security positions with outside custodians on a daily basis through a tape-to-tape computer matching process. Any out-of-balance situations are to be researched and cleared within three days. Items not cleared within three days require supervisory approval in accordance with company policy. Our tests of operating effectiveness, however, noted that out-of-balance situations unresolved after three days generally were not being approved in accordance with company policy. This results in the nonachievement of the control objective, "Controls provide reasonable assurance that investment purchases and sales are recorded completely, accurately, and timely."

### (Opinion paragraph)

In our opinion, except for the deficiency in operating effectiveness and the nonachievement of the related control objective noted in the preceding paragraph, the controls that were tested, as described in our description of the tests of operating effectiveness, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in our description of those tests were achieved during the period from January 1, 20XX to December 31, 20XX.

---

# New Standards

---

- ▶ Current – Several standards for service organization reporting
  - ▶ SAS 70, Section 5970, etc
  
- ▶ Future – Two substantially equivalent standards that replace SAS 70
  - ▶ Global – ISAE 3402, Assurance Reports on Controls at a Third Party Service Organization
  - ▶ US – Statement on Standards for Attestation Engagements (SSAE) Reporting on Controls at a Service Organization
  
- ▶ Drivers for change
  - ▶ Globalization of business process outsourcing
  - ▶ Need for common global standard
  - ▶ Need for increased emphasis on service organization rather than the auditor

---

# Similarities Between ISAE 3402/SSAE 16 & SAS 70

---

- ▶ Major elements of SAS 70 adopted by the IAASB
  - ▶ Type 1 and Type 2 reports (now Type A and Type B)
  - ▶ Description of controls prepared by service organization
  - ▶ List of controls specified and tested
  - ▶ Provision for carve-out and inclusive sub-servicers
  - ▶ Use of internal audit is permitted

---

# Differences Between ISAE 3402/SSAE 16 & SAS 70

---

- ▶ Change to an attestation standard
  - ▶ Service organization attests to the existence and operating effectiveness of controls in the report
  - ▶ Auditor opines on the subject matter supporting the assertions
- ▶ Service auditor required to assess the reasonableness of management's criteria used to develop the control objectives and controls
  - ▶ Criteria must be specific, measurable, and relevant to users' intended reliance on the report

---

# SSAE 16 vs. ISAE 3402...which is preferable?

---

- ▶ ISAE 3402
  - ▶ Communicates a sensitivity to international customers
  - ▶ Non-US user entities and auditors are likely to be familiar with this standard
  
- ▶ SSAE 16
  - ▶ Perceived as the direct replacement of SAS 70
  - ▶ US user entities and auditors will be most familiar with this standard
  - ▶ Based very closely on ISAE 3402 – AICPA was to make them as similar as possible

# Service Auditors' Responsibilities

---

- ▶ Report complete and accurate description of the system/processes under examination

## Unchanged from current standard

- ▶ Opinion on fairness of management's description of the system (formerly controls)
- ▶ Opinion as to suitability of the design and operating effectiveness of controls to achieve the control objectives
- ▶ Perform tests of controls and present an opinion on operating effectiveness

## Changes in new standard

- ▶ Standard moves from an audit standard to an assurance/attestation standard
- ▶ Additional considerations on using the work of internal audit
- ▶ Requires description of the internal auditor's work

# Service Organization's Responsibilities

---

- ▶ Report complete and accurate description of the system/processes under examination

## Unchanged from current standard

- ▶ Specifying the control objectives
- ▶ Designing, implementing and maintaining controls
- ▶ Complementary user entity controls (a.k.a., user control considerations)
- ▶ Other aspects of control environment, risk assessment, information and communications, control activities and monitoring

## Changes in new standard

- ▶ Describing services provided including classes of transactions processed
- ▶ Describing procedures by which the services are provided
- ▶ Management provides a written assertion that is included as part of the published report

---

# Sub-Service Organizations

---

- ▶ Subservice organizations can still be treated under the carve-out or inclusive method
- ▶ Change: inclusive subservicer will need to provide management a separate management assertion report
  - ▶ May be difficult to obtain
  - ▶ Alternatives to an inclusive report
    - ▶ Provide subservicer's report directly to your clients
    - ▶ Report on controls over subservicers that have been implemented

***Early communication with sub-servicers is critical***

Sadagopan Raghavan T

Manager – IT Risk & Assurance  
Ernst & Young

Oval Office, 18 iLabs Centre, Hitech City, Madhapur, Hyderabad, Andhra  
Pradesh 500 081, India

Direct: +91 40 6736 2292 | Mobile: +91 900 076 6979 and +91 984 029 6979 |  
Office: +91 40 6736 2000 | Fax: +91 40 6736 2200 |  
sadagopan.raghavan@in.ey.com

Website: [www.ey.com/india](http://www.ey.com/india)