System and Organization Control
(SOC Reporting)

Stephen W. Minder, CPA, CIA, CISA, CFE, CGMA

Chief Executive Officer

YCN Group, LLC

steve@ycngroup.com

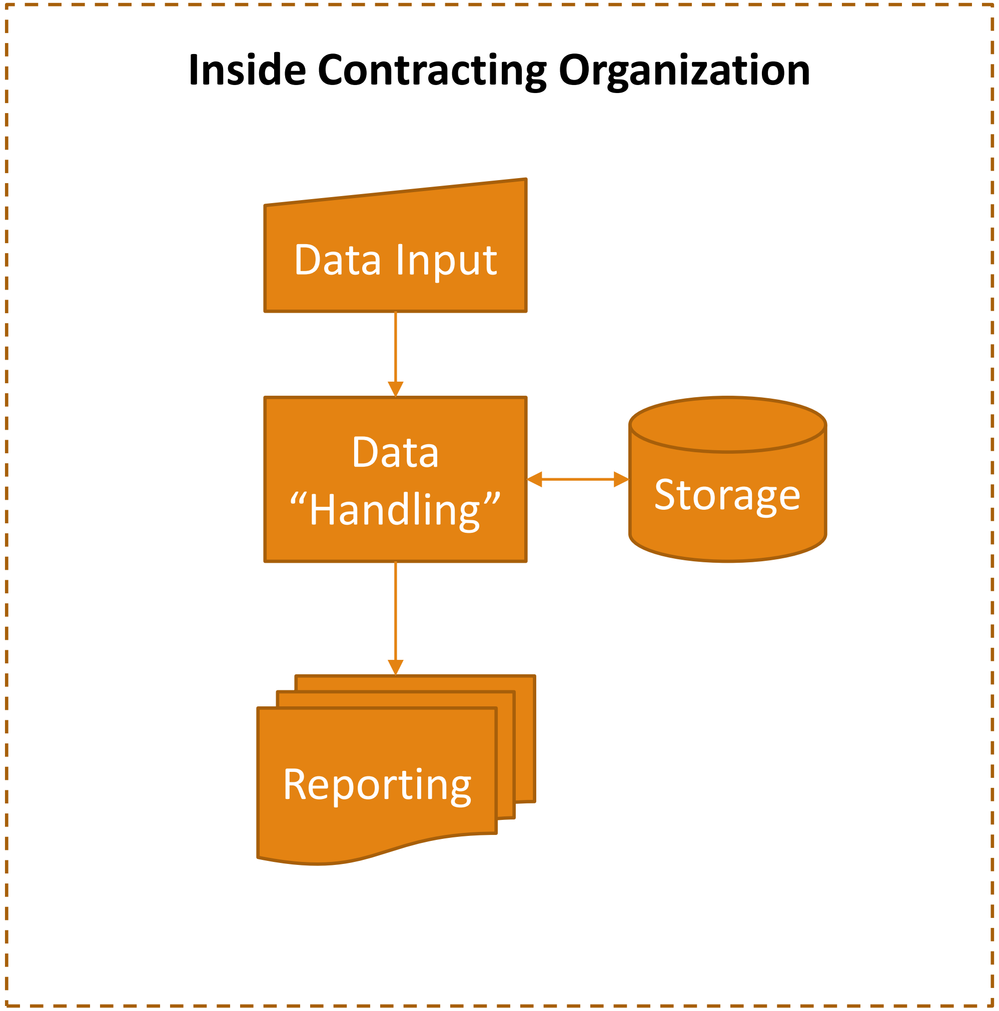
Service Organizations

An entity that **provides IT related services or processing** for clients including:

- Capture,
- Transmission,
- Editing,
- Translation,
- Storage,
- Processing,
- Analysis, or
- Reporting

of **DATA**

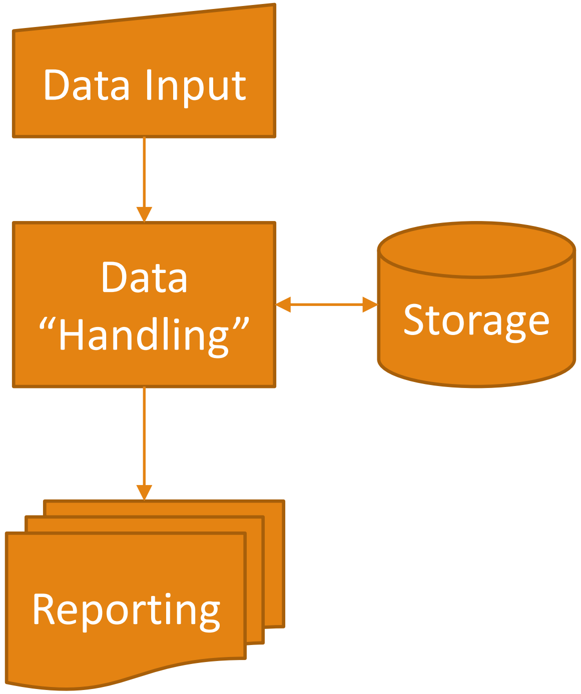
Not a Service Organization



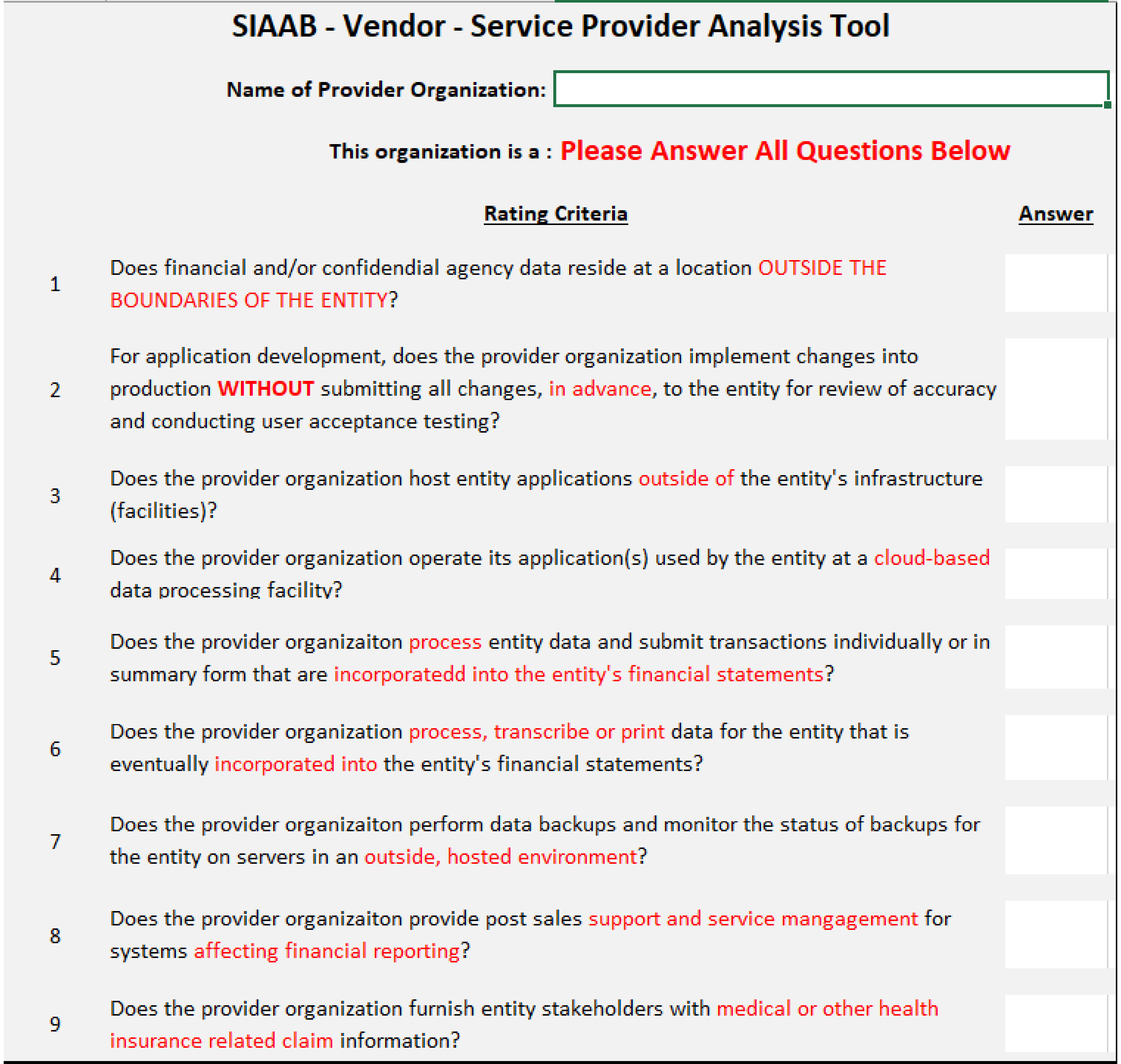
Inside Contracting Organization

Service Organization

One or more functions is accomplished under outside organization control, not within the Contracting Organization



Vendor – Service Organization Determination Tool. xlsx



SIAAB - Vendor - Service Provider Analysis Tool

Name of Provider Organization:

This organization is a : **Please Answer All Questions Below**

	Rating Criteria	**Answer**
1	Does financial and/or confidendial agency data reside at a location OUTSIDE THE BOUNDARIES OF THE ENTITY?	
2	For application development, does the provider organization implement changes into production **WITHOUT** submitting all changes, in advance, to the entity for review of accuracy and conducting user acceptance testing?	
3	Does the provider organization host entity applications outside of the entity's infrastructure (facilities)?	
4	Does the provider organization operate its application(s) used by the entity at a cloud-based data processing facility?	
5	Does the provider organizaiton process entity data and submit transactions individually or in summary form that are incorporatedd into the entity's financial statements?	
6	Does the provider organization process, transcribe or print data for the entity that is eventually incorporated into the entity's financial statements?	
7	Does the provider organizaiton perform data backups and monitor the status of backups for the entity on servers in an outside, hosted environment?	
8	Does the provider organizaiton provide post sales support and service mangagement for systems affecting financial reporting?	
9	Does the provider organization furnish entity stakeholders with medical or other health insurance related claim information?	

Background

Genesis in Financial Statement Audits where third-party processing affects the financial reporting processes.

Financial Auditing Standard AU-C 320 and AU-C 402 State:

Services provided by a service organization are relevant to the audit of a user entity's financial statements when those services and the controls over them affect the user entity's information system, including related business processes, relevant to financial reporting.

Background – cont'd

As usage of outside IT service providers, including cloud computing, software-as-a-service, etc has increased, audit requirements have evolved to include "Standardized Trust Service Categories".

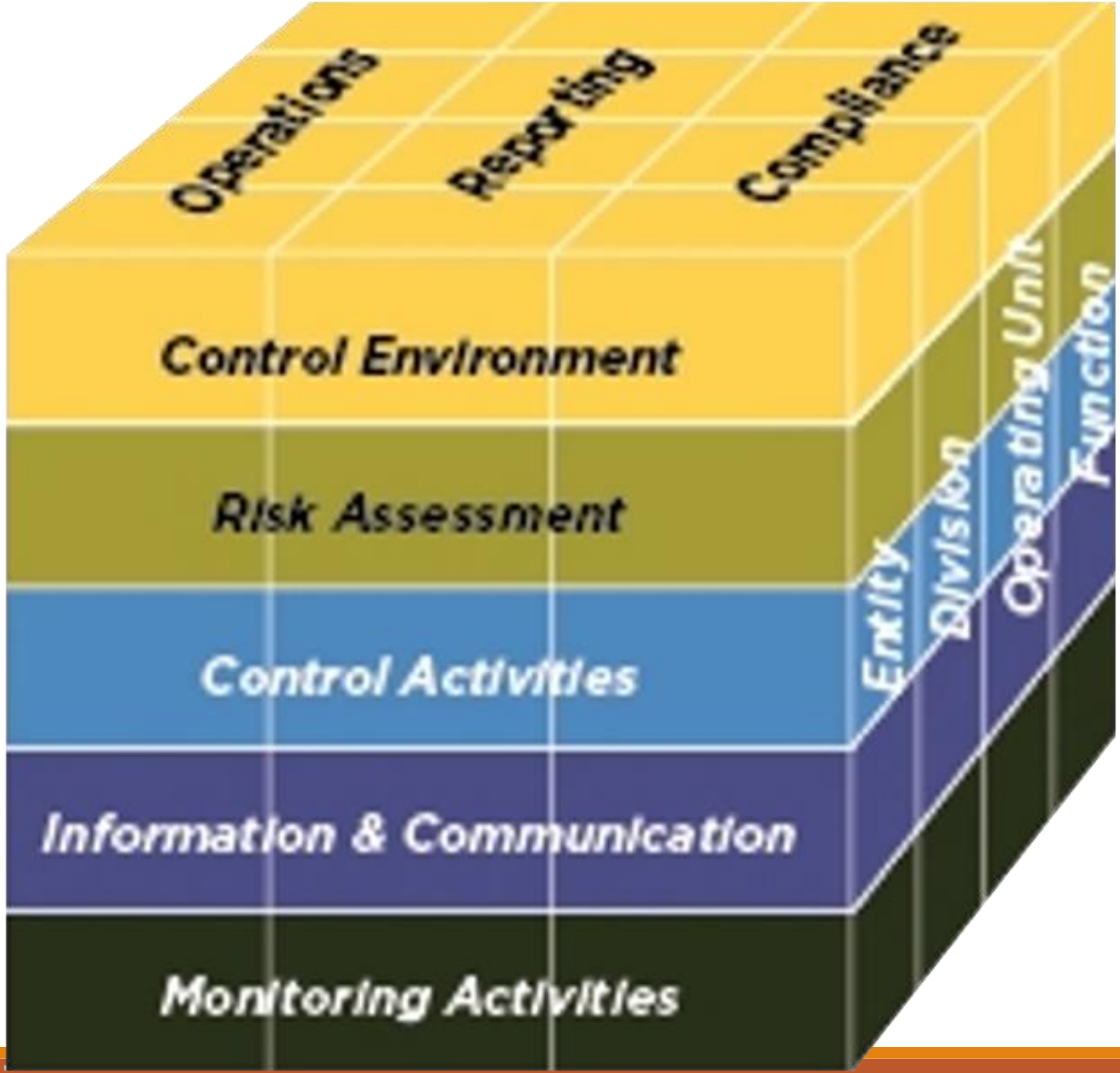
Standardized Trust Service Categories:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

Standardized Trust Service Categories

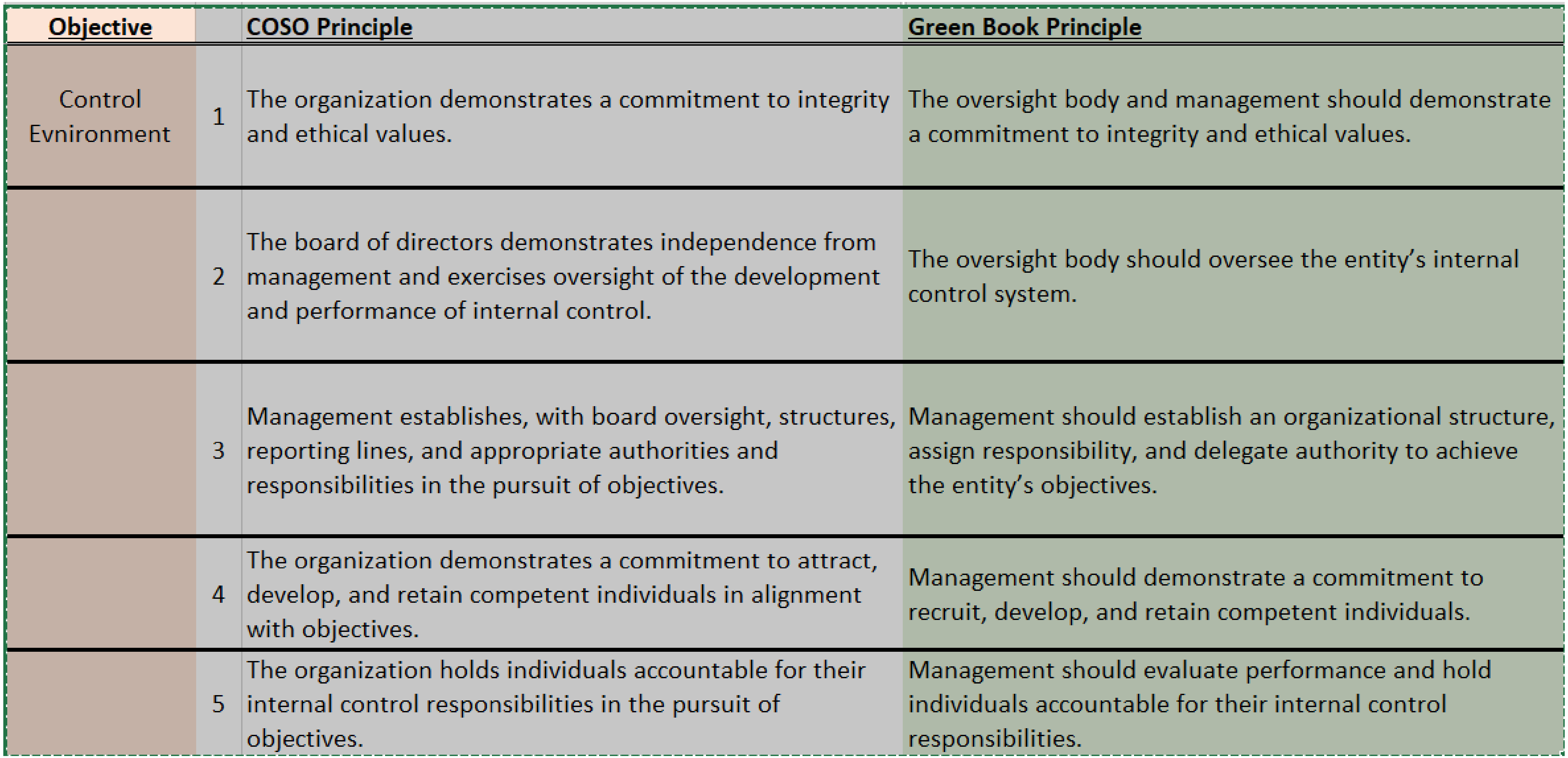
- These categories are mapped to COSO's internal control framework to evaluate how well the organization's security program meets control objectives as defined in the COSO framework

- Attainment of these COSO Control objectives are considered essential to obtain and maintain a reliable, well-controlled environment that correctly handles an organization's data in accordance with management's objectives

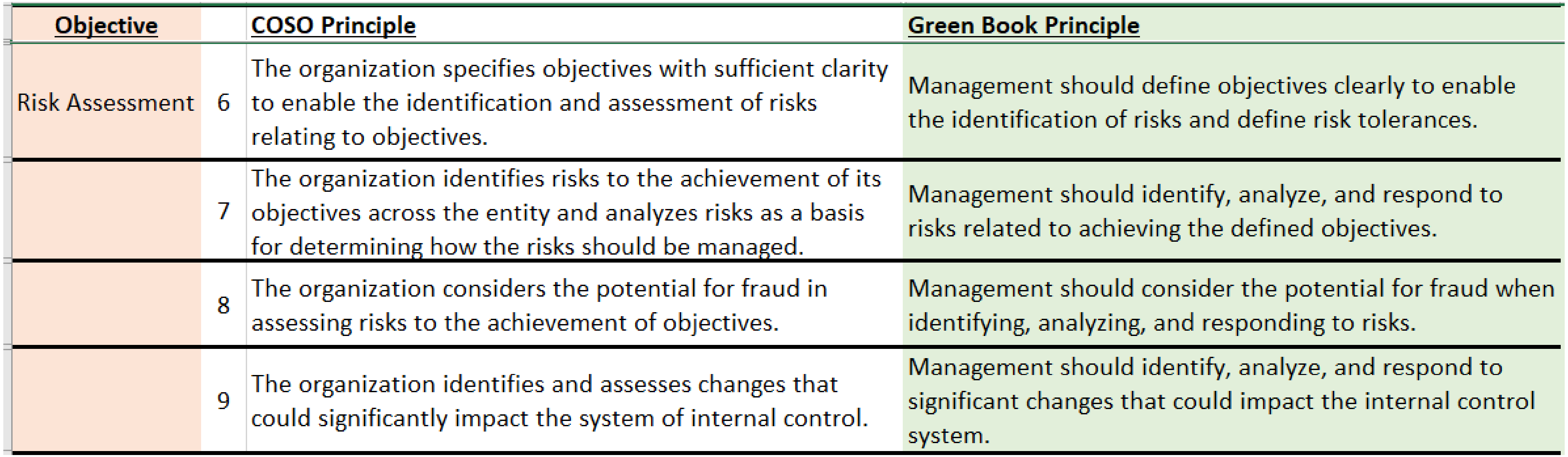

Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring Activities
Entity
Division
Operating Unit
Function

COSO Internal Control

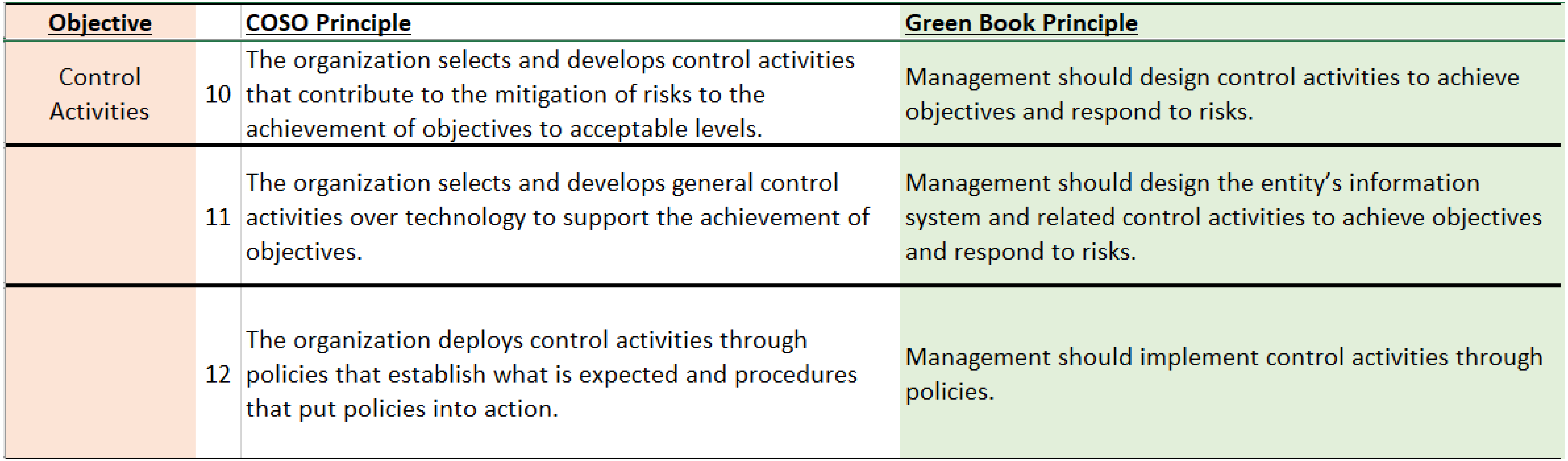
Internal Control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.



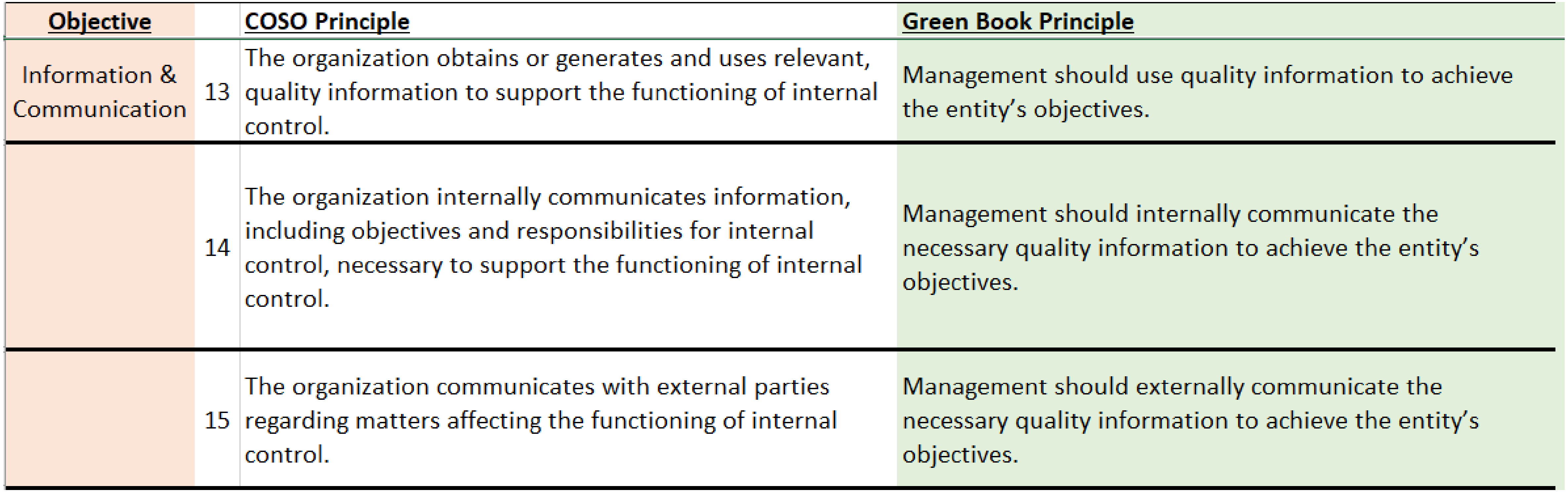
Objective		COSO Principle	Green Book Principle
Control Evnironment	1	The organization demonstrates a commitment to integrity and ethical values.	The oversight body and management should demonstrate a commitment to integrity and ethical values.
	2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The oversight body should oversee the entity's internal control system.
	3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
	4	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Management should demonstrate a commitment to recruit, develop, and retain competent individuals.
	5	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Management should evaluate performance and hold individuals accountable for their internal control responsibilities.



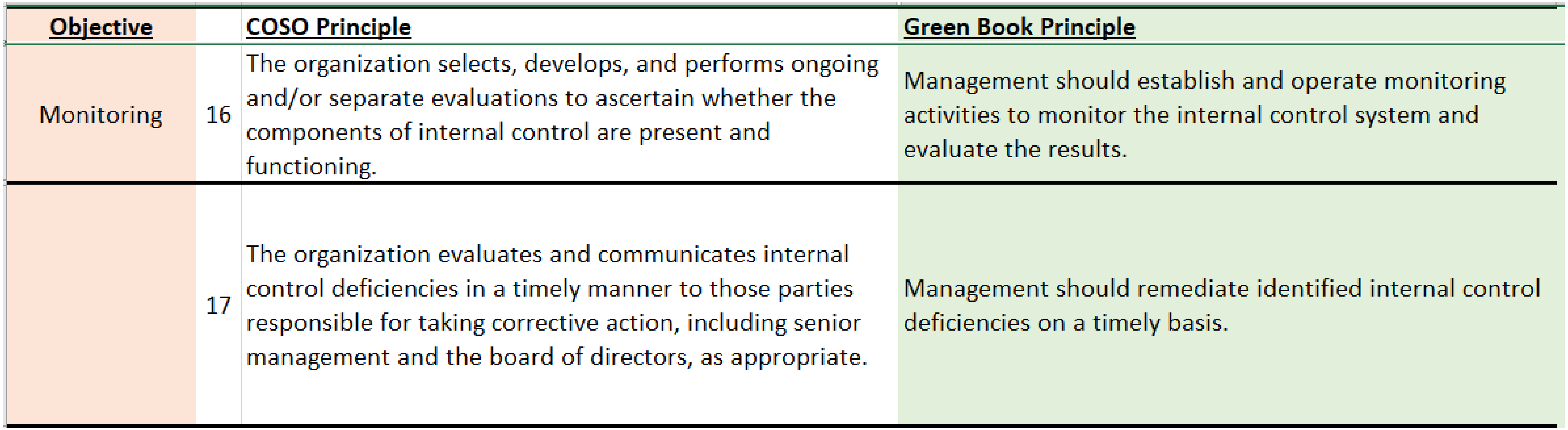
Objective		COSO Principle	Green Book Principle
Risk Assessment	6	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Management should define objectives clearly to enable the identification of risks and define risk tolerances.
	7	The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Management should identify, analyze, and respond to risks related to achieving the defined objectives.
	8	The organization considers the potential for fraud in assessing risks to the achievement of objectives.	Management should consider the potential for fraud when identifying, analyzing, and responding to risks.
	9	The organization identifies and assesses changes that could significantly impact the system of internal control.	Management should identify, analyze, and respond to significant changes that could impact the internal control system.



Objective		COSO Principle	Green Book Principle
Control Activities	10	The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Management should design control activities to achieve objectives and respond to risks.
	11	The organization selects and develops general control activities over technology to support the achievement of objectives.	Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
	12	The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	Management should implement control activities through policies.



Objective		COSO Principle	Green Book Principle
Information & Communication	13	The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.	Management should use quality information to achieve the entity’s objectives.
	14	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Management should internally communicate the necessary quality information to achieve the entity’s objectives.
	15	The organization communicates with external parties regarding matters affecting the functioning of internal control.	Management should externally communicate the necessary quality information to achieve the entity’s objectives.



Objective		COSO Principle	Green Book Principle
Monitoring	16	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
	17	The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Management should remediate identified internal control deficiencies on a timely basis.

The Need

When an outside organization (Service Provider) is performing key control functions over Contracting Organization Data, how can we know that appropriate controls and procedures are in place to safeguard the data from unauthorized or inappropriate creation, disclosure, modification, destruction, or reporting?

The Solution

- System and Organization Control (SOC) Examinations
- Performed by independent, well-trained and trusted organizations (usually CPA Firms)
- Provide written assurance
- Delineate Contracting Organization responsibilities to attain assurance

Types of SOC Reports

- **SOC 1** – Focused on Internal Controls over Financial Reporting (ICFR). Includes the Service Organization Management’s description of internal processes to address relevant controls in place
- **SOC 2** – Addresses Internal Controls for Compliance in the areas of Infrastructure, Software, People, Procedures and Data. Focus on Standardized Trust Service Categories. Unlike SOC 1, SOC 2 reports include the Service Auditor’s description and evaluation of control processes in the IT environment
- **SOC 3** - Provide a limited subset of the SOC 2 reporting process generally produced for marketing purposes to increase a potential buyer’s confidence in the Service Organization prior to establishing a contract. Often included on the Service Organization’s Website.

Types of SOC Reports

- **SOC 1** – Focused on Internal Controls over Financial Reporting (ICFR). Includes the Service Organization Management's description of internal processes to address relevant controls in place
- **SOC 2 – Addresses Internal Controls for Compliance in the areas of Infrastructure, Software, People, Procedures and Data. Focus on Standardized Trust Service Categories. Unlike SOC 1, SOC 2 reports include the Service Auditor's description and evaluation of control processes in the IT environment**
- **SOC 3** - Provide a limited subset of the SOC 2 reporting process generally produced for marketing purposes to increase a potential buyer's confidence in the Service Organization prior to establishing a contract. Often included on the Service Organization's Website.

SOC Report Testing Options

Type 1 – Tests **Design of Control** Only

A Design of Control test is an evaluation based on understanding of the control process, its timing, how it is executed and established follow-up protocols for deviations. In theory, a test of control design makes the statement that "If everything works as intended, the control objective will be met".

Type 2 – Tests both **Design of Control** and **Operating Effectiveness of the Control**

Includes the Test of Design above PLUS detailed transaction testing to determine if the control is actually working as intended.

Testing Example

An example of **test of control design** would be a description of a control requiring all expenditures to be approved by two persons authorized for that type and amount of expenditure prior to disbursement.

A **test of operating effectiveness of that control** would be to select a sample (normally a statistically valid random sample) of disbursements and verify that each expenditure was approved by two separate persons who were authorized to approve that type and amount of expenditure.

Subservice Organizations

When controls at a vendor are necessary in combination with the service organization’s controls to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria, the vendor is considered a subservice organization (AICPA)

Subservice Organizations – cont’d

A subservice organization may be a separate entity that is external to the service organization or may be a related entity, for example, a subservice organization that is a subsidiary of the same company that owns the service organization.

A vendor is considered a subservice organization ONLY IF the following apply:

- ❑ The services the vendor provides are likely to be relevant to report users’ understanding of the services organization’s system as it relates to the applicable trust services criteria.
- ❑ Controls at the vendor are necessary, in combination with the service organization’s controls, to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria.

Handling Subservice Organizations

- Carve-out Method
- Inclusive Method

Carve-out Method

Method of addressing the services a subservice organization provides in which the components of the subservice organization’s system used to provide the services to the service organization are excluded from the description of the service organization’s system and from the scope of the examination

In situations in which the subservice organization’s services and controls have a pervasive effect on the service organization’s system, management would not be able to use the carve-out method. (AICPA)

Carve-out Method

If Subservice Organization contributes to “significant” aspects of the service organization’s assurance to your organization, the best solution is to obtain a SOC 2 – type 2 report for the Subservice Organization.

Carve-out Method

When the carve-out method is used, and controls the subservice organization performs are necessary, in combination with the service organization’s controls, to provide reasonable assurance that one or more of the service organization’s service commitments and system requirements were achieved, such controls are referred to as complementary subservice organization controls (CSOCs).

Example CSOCs

- Controls relevant to the completeness and accuracy of transaction processing on behalf of the service organization
- Controls relevant to the completeness and accuracy of specified reports provided to and used by the service organization
- Logical access controls relevant to the processing performed for the service organization

Inclusive Method

Method of addressing the services a subservice organization provides in which the description of the service organization’s system includes a description of (a) the nature of the service provided by the subservice organization and (b) the components of the subservice organization’s system used to provide services to the service organization, including the subservice organization’s controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved.

Inclusive Method

Most useful when the subservice organization provide extensive services to the service organization

Review of Service Organization Report should include analysis of the extent of control and testing over subservice operations to provide assurance that overall control objectives are met

Inclusive Method

Must determine whether it will be possible to obtain:

a) an assertion from subservice organization management and

b) evidence that supports the service auditor’s opinion on the subservice organization’s description of its system and the suitability of the design and, in a type 2 examination, the operating effectiveness of the subservice organization’s controls (including written representations from management of the subservice organization).

If subservice organization management will not provide a written assertion and appropriately written representations, service organization management will be unable to use the inclusive method but may be able to use the carve-out method.

AICPA Subservice Resource

https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/infoformanagementofsvcorg.pdf

SOC Report Caution

SOC reports normally identify Complementary User Entity Controls (CUECs). CUECs are specific procedures and/or processes the Contracting Organization **MUST FOLLOW** in order to achieve the level of assurance as outlined in the SOC report.

Types of CUECs

- **Complementary** – cohesive organization controls that work in conjunction with the service organization's controls to provide assurance that objectives are met. IE. Notifying the Service Organization of Terminated Users to remove access to data

- **Compensating** – specific control procedures that address areas not fully addressed by the service organization's control environment. IE. Ensuring that data transmitted to the Service Organization from the Judicial Branch is properly encrypted using latest accepted industry standards

Recommendations

1. Evaluate all vendors using the Excel Tool entitled, "SIAAB - Vendor – Service Organization Determination Tool.xlsx"
2. For **ALL Service Organizations**:
   a. Add Contract Language specifying the Service Organization provide a SOC 2 – Type 2 report to the Contracting Organization Annually
   b. Establish calendar follow-up to verify receipt of the reports
   c. Evaluate subservice organizations to determine how to address appropriately
   d. Initiate IT and User review of SOC 2 - Type 2 report including detailed analysis of all CUECs and the Contracting Organization's handling of these requirements
   e. Document results of review including name of reviewer(s), conclusion of review, and date completed

Review of SOC 2 – type 2 reports

I. Review Report noting any weaknesses identified by the service auditor

II. Verify that the report has described relevant controls affecting services provided to your organization

III. Analyze impact of identified weaknesses on organization use of the vendor product and services

IV. Determine how subservice organizations are used by the service organization and whether appropriate assurance is provided by the inclusion method or by separate SOC 2 – Type 2 reporting

V. Review CUECs and CSOCs identified and the contracting organizations processes to comply with CUEC requirements

VI. Document Conclusions

Potential Contract Language

If applicable and requested by the ***(Contracting Organization)***, ***(Vendor)*** certifies it will undertake annual independent third-party audits performed under the AICPA's Statement on Standards for Attestation Engagements No. 18 (SSAE-18) to provide the ***(Contracting Organization)*** with a SOC 2 type 2 report covering the application(s) and services provided to the ***(Contracting Organization)***. The SOC Report information provided to ***(Contracting Organization)*** is for its own use and may not be disclosed outside the organization except to its external Certified Public Accountants (who are legally bound to maintain confidence of client data) as a part of their review of ***(Contracting Organization)*** or as otherwise required by law.

What if a Service Organization or one or more subservice organizations do not have or will not agree to provide SOC 2 Type 2 Reports?

Apply appropriate audit procedures, under right to audit clause, to obtain assurance

For Additional Assistance

Stephen W. (Steve) Minder

Chief Executive Officer

YCN Group, LLC

steve@ycngroup.com

Phone: (217) 524-6423 (office)

(217) 520-2092 (cell)

Questions?