COSO 2013 Mapping Tool

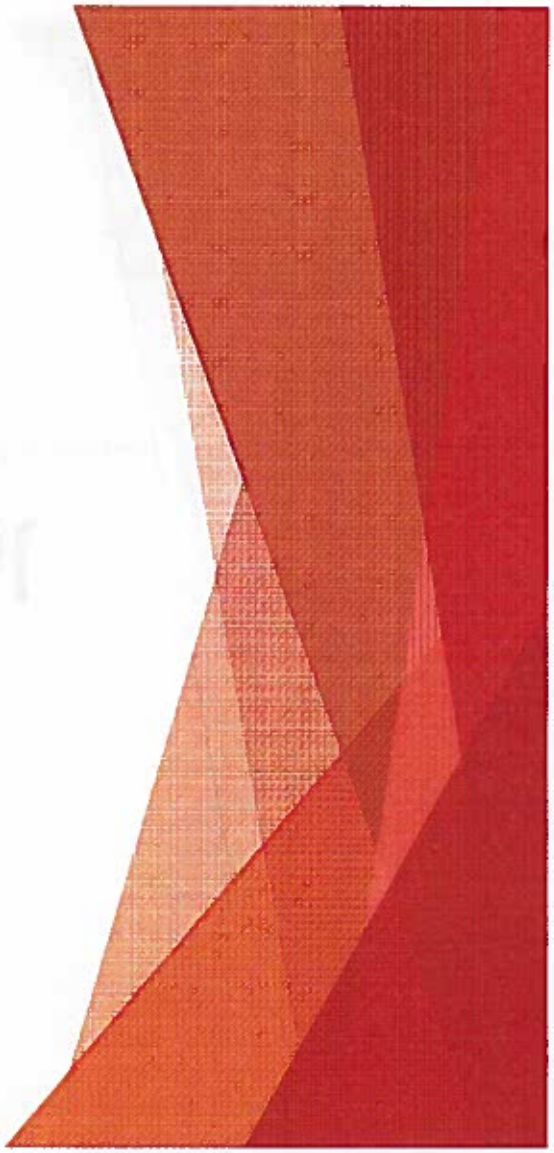
Presented By: Jeff Digman, Director of Internal Controls and Andrew Lawler, Associate Accountant

NYSIF Internal Control Department

April 28, 2016

This COSO 2013 mapping tool template demonstrates how NYSIF incorporated the COSO 2013 framework into our existing internal control documentation. We included sample responses from a fictional ITS department.

Agencies may modify the tool to incorporate their own internal control review processes.



Principle Evaluation – Control Environment

Principle 1: Demonstrates Commitment to Integrity and Ethical Values

–The organization demonstrates a commitment to integrity and ethical values.

Point of Focus

1 Sets the Tone at the Top – The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.

2 Establishes Standards of Conduct – The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the organization and by outsourced service providers and business partners.

3 Evaluates Adherence to Standards of Conduct – Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.

4 Addresses Deviations in a Timely Manner – Deviations of the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.

Summary of Controls Aligned to Principle 1

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Control Number	Major Function Name	RISK	Control Objective	CONTROL ACTIVITY DESCRIPTION	Objective Met? (Yes/No)	Applicable COSO Component					FREQUENCY	CONTROL TYPE		METHOD		OWNER	Test Description	Required Documentation
						CE	RA	CA	IC	MA		PREVENT CONTROLS (p)	DETECT CONTROLS (d)	MANUAL (c)	AUTOMATED (a)			
						Triangle												
ITS - 1	Information Security	Inappropriate or unauthorized access to obtained to critical information and systems	Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication	Physical access to the computer room is restricted Access is only granted with a properly credential ID badge Computer room access is recertified every six months by the ITS Department	Yes	3		10	13	17	On-Going		✔	✔		[Position Title e.g. ISO]	[DESCRIPTION OF TEST PERFORMED]	[LISTING OF INFORMATION REQUIRED TO COMPLETE TEST]
Notes:																		

Principle 2: Exercises Oversight Responsibility

Point of Focus

1 **Establishes Oversight Responsibilities**—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.

2 **Applies Relevant Expertise**—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate actions.

3 **Operates Independently**—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.

4 **Provides Oversight for the System of Internal Control**—The board of directors retains oversight responsibility for management's design, implementation, and conduct of internal control:

– *Control Environment*—Establishing integrity and ethical values, oversight structures, authority and responsibility, expectations of competence, and accountability to the board.

Summary of Controls Aligned to Principle 2

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle 3: Establishes Structure, Authority, and Responsibility

Point of Focus

1 Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities,
2 Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.

3 Defines, Assigns, and Limits Authorities and Responsibilities — Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization:

– *Board of Directors* — Retains authority over significant decisions and reviews management's assignments and limitations of authorities and responsibilities

– *Senior Management* —Establishes directives, guidance, and control to enable management and other personnel to understand and carry out their internal control responsibilities

– *Management* —Guides and facilitates the execution of senior management directives within the entity and its subunits

– *Personnel* —Understands the entity's standard of conduct, assessed risks to objectives, and the related control activities at their respective levels of the entity, the expected information and communication flow, and monitoring activities relevant to their achievement of the objectives

– *Outsourced Service Providers* —Adheres to management's definition of the scope of authority and responsibility for all non-employees engaged

Summary of Controls Aligned to Principle 3

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle
ITS-1	Physical access to the computer room is restricted Access is only granted with a properly credential ID badge Computer room access is recertified every six months by the ITS Department	Y	N	3	ITS Management has a documented policy restricting access to the computer room. Additionally, the Department has a procedure outlining access recertification

Principle 4: Demonstrates Commitment to Competence

—The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Point of Focus

1 Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.

2 Evaluates Competence and Addresses Shortcomings—The board of directors and management evaluate competence across the organization and ir outsourced service providers in relation to established policies and practices, and acts, as necessary to address shortcomings.

3 Attracts, Develops, and Retains Individuals—The organization provides the mentoring and training needed to attract, develop, and retain sufficient an competent personnel and outsourced service providers to support the achievement of objectives.

4 Plans and Prepares for Succession—Senior management and the board of directors develop contingency plans for assignments of responsibility importa for internal control.

Summary of Controls Aligned to Principle 4

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle 5: Enforces Accountability

—The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Point of Focus

1 Enforces Accountability through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the organization and implement corrective action as necessary.

2 Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.

3 Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.

4 Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.

5 Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence and provide rewards or exercise disciplinary action as appropriate.

Summary of Controls Aligned to Principle 5

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle Evaluation – Risk Assessment

Principle 6: Specifies Suitable Objectives

—The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Point of Focus

Operations Objectives

1a Reflects Management's Choices—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.

1b Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.

1c Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.

1d Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.

External Financial Reporting Objectives

2a Complies with Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.

2b Considers Materiality—Management considers materiality in financial statement presentation.

2c Reflects Entity Activities—External reporting reflects the underlying transactions and events to show qualitative characteristics and

External Non-Financial Reporting Objectives

3a Complies with Externally Established Standards and Frameworks—Management establishes objectives consistent with laws and regulations, or standards and frameworks of recognized external organizations.

3b Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and as based on criteria established by third parties in non-financial reporting.

3c Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.

Internal Reporting Objectives

4a Reflects Management's Choices—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.

4b Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in non-financial reporting objectives and materiality within financial reporting objectives.

4c Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.

Compliance Objectives

5a Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct which the entity integrates into compliance objectives.

5b Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of compliance

Summary of Controls Aligned to Principle 6

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle 7: Identifies and Analyzes Risk

—The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining

Point of Focus

1 Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The organization identifies and assesses risks at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.

2 Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.

3 Involves Appropriate Levels of Management—The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management.

4 Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.

5 Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.

Summary of Controls Aligned to Principle 7

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle
ITS-1	Physical access to the computer room is restricted Access is only granted with a properly credential ID badge Computer room access is recertified every six months by the ITS Department	Y	N	1, 5	Identified issues (accidental or intentional) are communicated to the appropriate individuals by the ISO

Principle 8: Assesses Fraud Risk

—The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Point of Focus

1 Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.

2 Assesses Incentive and Pressures—The assessment of fraud risk considers incentives and pressures.

3 Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts.

4 Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.

Summary of Controls Aligned to Principle 8

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle 9: Identifies and Analyzes Significant Change

—The organization identifies and assesses changes that could significantly impact the system of internal control.

Point of Focus

1 Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.

2 Assesses Changes in the Business Model—The organization considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.

3 Assesses Changes in Leadership—The organization considers changes in management and respective attitudes and philosophies on the system of internal control.

Summary of Controls Aligned to Principle 9

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle Evaluation – Control Activities

Principle 10: Selects and Develops Control Activities

—The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Point of Focus

1 Integrates with Risk Assessment – Control activities help ensure that risk responses that address and mitigate risks are carried out.

2 Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.

3 Determines Relevant Business Processes—Management determines which relevant business processes require control activities.

4 Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.

5 Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.

6 Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical management selects and develops alternative control activities.

Summary of Controls Aligned to Principle 10

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle
ITS-1	Physical access to the computer room is restricted Access is only granted with a properly credential ID badge Computer room access is recertified every six months by the ITS Department	Y	N	4	Access to the computer room is restricted an electronically locked door, only badges with the proper credentials are able to ope the door. Additionally, the Department has clearly defined policy defining which employees will be given the proper access credentials

Principle 11: Selects and Develops General Controls over Technology

—The organization selects and develops general control activities over technology to support the achievement of objectives.

Point of Focus

1 Determines Dependency between the Use of Technology in Business Processes and Technology General Controls—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.

2 Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.

3 Establishes Relevant Security Management Process Control Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.

4 Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.

Summary of Controls Aligned to Principle 11

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle 12: Deploys through Policies and Procedures

The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Point of Focus

1 Establishes Policies and Procedures to Support Deployment of Management's Directives—Management establishes control activities that are built i business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.

2 Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.

3 Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.

4 Takes Corrective Action—Responsible personnel investigate and act on matters identified as a result of executing control activities.

5 Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing fo

6 Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance, and refreshes them when necessary.

Summary of Controls Aligned to Principle 12

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle Evaluation—Information and Communication

Principle 13: Uses Relevant Information

—The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Point of Focus

1 Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.

2 Captures Internal and External Sources of Data—Information systems capture internal and external sources of data.

3 Processes Relevant Data into Information—Information systems process and transform relevant data into information.

4 Maintains Quality throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, and verifiable and retained. Information is reviewed to assess its relevance in supporting the internal control components.

5 Considers Costs and Benefits—The nature, quantity, and precision of information communicated are commensurate with and support the achievement of objectives.

Summary of Controls Aligned to Principle 13

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle
ITS - 1	Physical access to the computer room is restricted Access is only granted with a properly credential ID badge Computer room access is recertified every six months by the ITS Department	Y	N	1	The Department maintains a listing of all individuals who have access to the computer room The electronic lock logs all entry attempts made on the door (name, date, and time)

Principle 14: Communicates Internally

—The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support t

Point of Focus

1 Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.

2 Communicates with the Board of Directors—Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.

3 Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

4 Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information.

Summary of Controls Aligned to Principle 14

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity ali with the Principle

Section Not Utilized

Principle 15: Communicates Externally

—The organization communicates with external parties regarding matters affecting the functioning of internal control.

Point of Focus

1 Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties including shareholders, partners, owners, regulators, customers, and financial analysts and other external parties.

2 Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.

3 Communicates with the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.

4 Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

5 Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.

Summary of Controls Aligned to Principle 15

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle

Section Not Utilized

Principle Evaluation—Monitoring Activities

Principle 16: Conducts Ongoing and/or Separate Evaluations

—The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal

Point of Focus

1 Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.

2 Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongo and separate evaluations.

3 Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.

4 Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.

5 Integrates with Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.

6 Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk.

7 Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback.

Summary of Controls Aligned to Principle 16

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with t Principle

Section Not Utilized

Principle 17: Evaluates and communicates deficiencies

—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.

Point of Focus

1 Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.

2 Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.

3 Monitors Corrective Actions—Management tracks whether deficiencies are remediated on a timely basis.

Summary of Controls Aligned to Principle 17

Identification No.	Activity Description	Functioning? (Y/N)	Major Deficiency Identified? (Y/N)	Point of Focus	Reasoning- Explain how the activity aligns with the Principle
ITS - 1	Physical access to the computer room is restricted Access is only granted with a properly credential ID badge Computer room access is recertified every six months by the ITS Department	Y	N	2	Access to the room is recertified every six months, identified issues are communicated to management and remedied Failed access attempts are communicated to management

<Department>
COSO Evaluation Summary
<YEAR> Cycle

	COSO Principle																
	Control Environment					Risk Assessment				Control Activities			Information & Communication			Monitoring Activi	
Control Number	1. Demonstrates commitment to integrity & ethical values	2. Exercises Oversight Responsibility	3. Establishes structure, authority & reportability	4. Demonstrates commitment to competence	5. Enforces accountability	6. Specifies suitable objectives	7. Identifies & analyzes risks	8. Assesses fraud risk	9. Identifies & analyzes significant changes	10. Selects & develops control activities	11. Selects & develops general controls over technology	12. Deploys through policies & procedures	13. Uses relevant information	14. Communicates internally	15. Communicates externally	16. Conducts ongoing and/or separate evaluations	17. Evaluates & communicates
XXX-##																	
Principle Present and Functioning	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No