CONTROL SELF-ASSESSMENT
Good Practice Note

Prepared by: CGIAR Internal Audit Unit

Table of Contents

FOREWORD

What is a GPN

A Good Practice Note (GPN) is a document themed around a specific risk or control-related area.

It is developed by the CGIAR IAU with contributions of subject-matter specialists, leveraging knowledge accumulated within the CGIAR System and reflecting good practices suggested by professional bodies or standard setters, and implemented by Centers and/or other external organizations.

GPNs aim to summarize, circulate and promote existing knowledge around the System and can be used to benchmark existing arrangements against good practices and to improve knowledge, processes and operations at Center and System levels.

What it is not

GPNs are not and should not be interpreted as minimum standards, policies, guidelines or requirements, as practices mentioned in the GPN may not be relevant to or applicable in all Centers.

1. INTRODUCTION

CGIAR Centers have a wide geographical footprint with their head offices, regional and country offices distributed across the globe. This creates a challenge of ensuring that the regional and country offices are working towards the same mission and objectives. Tools supporting alignment of a Center's operations may include an organizational strategy and common processes/controls frameworks to be followed by the region and country office staff.

Generally, the Centers will have existing organizational arrangements for local management and for headquarters' oversight of regional and country office activities. These vary from Center to Center— some have adopted a centralized approach where all decision-making responsibilities lie with the HQ, while others have a more decentralized structure, empowering the regional or country offices to make operational decisions. An important aspect, regardless of the arrangement, is the ability of the HQ to oversee and monitor these operations.

1.1 Main risks arising from poor oversight of field offices

#	COSO Category	Potential Risks
1.	Strategic Risks	• Field office strategies, operational decisions and resource allocation may not be aligned with an approved corporate strategy • Reputation risk stemming from misalignment
2.	Compliance Risks	Failure to comply with: • Hosting agreements requirements • Country laws and regulations • Policies and procedures of the Center and/or of the hosting institution • Donor conditions
3.	Operational Risks	• Inefficiencies and ineffectiveness of the internal control system at field offices • Fraud risks
4.	Reporting Risks	Inaccurate or incomplete reporting by field office

The extent of any oversight and monitoring activities depends on the level of resources available for them. The key objective of this Good Practice Note is to describe recognized practices on how to perform oversight of country offices using a Control Self-Assessment (CSA) which can be one of the most efficient ways to monitor remote activities.

1.2 Potential benefits of implementing a Control Self-Assessment

- Management can utilize CSAs to clarify business objectives and to identify and deal with the risks to achieving these objectives. It creates a clear line of accountability for controls, and a reinforced governance regime. It leads to a better understanding of business operations (by both management and operational staff).
- It improves the internal control environment of an organization by:
  o Increasing awareness of organizational objectives and the role of internal control in achieving goals and objectives
  o Motivating personnel to carefully design and implement control processes and continually improve operating control processes
- A well-designed CSA helps management to reduce the costs of oversight activities while expanding their coverage.
- An effective and efficient CSA can assist in limiting extensive audit testing for internal auditors. Internal audit performs various types of audits, such as country office audits or process audits. Internal auditors can utilize CSA programs for gathering relevant information about risks and controls; for focusing audit work on high risk and unusual areas, and to forge greater collaboration with operating managers and work teams.
- CSA may help to reduce the risk of fraud (by examining data that may flag unusual patterns of transactions).

2. STANDARDS AND APPROACHES

2.1 About Internal Control

The Institute of Internal Auditors (IIA) standards for Professional Practice in Internal Auditing defines control as "*any action taken by management to enhance the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.*"

The primary objectives of internal controls are to ensure:

- The reliability and integrity of information
- Compliance with policies, plans, procedures, laws, regulations and contracts
- The safeguarding of assets
- The economical and efficient use of resources
- The accomplishment of established objectives and goals for operations or programs.

2.2 The COSO Framework

Under the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, internal control is defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

COSO identifies five components of internal control that need to be in place and integrated to ensure the achievement of each of these three objectives:

A) Control environment
The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance.

B) Risk assessment
Involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives, and forming the basis for determining how risks will be managed.

C) Control activities

The actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities.

D) Information and communication

Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information.

E) Monitoring activities

Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning.

These five components operate together in an integrated manner to reduce, to an acceptable level, the risk of not achieving objectives.

A direct relationship exists between the three objectives, the five components of internal control, and the organizational structure of the entity (the operating units, legal entities, and other). The relationship can be depicted in the form of a cube (see *Figure 1* on the right).

Everyone in an organization has some responsibility for internal control.

Figure 1: COSO cube

More and more organizations are adopting the Three Lines of Defense (or Three Lines of Assurance) model to bring clarity to specific roles and responsibilities for internal controls.

Its underlying premise is that, under the oversight and direction of senior management and board of trustees, three separate groups (or lines of defense) within an organization are necessary for effective management of risk and control. The responsibilities of each of the groups (or "lines") are:

A) Own and manage risk and control (front line operating management).
B) Monitor risk and control in support of management (risk, control, and compliance functions put in place by management).
C) Provide independent assurance to the board and senior management concerning the effectiveness of management of risk and control (internal audit).

Figure 2: The Three Lines of Defense Model

The first line of defense lies with business and process owners, while the third line lies with Internal Audit. In between the two, the second line of defense pertains to monitoring activities (the fifth component of the COSO framework) of risk and control, put in place by management which are then reviewed by Internal Auditors.

Management needs to have an efficient second line of defense, which a Control Self-Assessment process can help develop. Control Self-Assessments is a systematic and iterative process whereby management periodically validates the operating effectiveness of the company's key controls instead of solely relying on internal or external auditors to make such an assessment.

2.3 What is a Control Self-Assessment?

The concept of Control Self-Assessment (CSA) was developed by Bruce Mc Cuaig in 1987 for Gulf Canada, where he was an auditor at the time. In his paper, "Auditing Assurance, CSA" (1998), he defines CSA as *"any activity where the people responsible for a business area, task or objective, using some demonstrable approach, analyze the status of control and risk to provide additional assurance related to the achievement of one or more business objectives."* This definition still holds true today. The Institute of Internal Auditors (IIA) defines CSA as "*a process through which internal control effectiveness is examined and assessed… to provide reasonable assurance that all business objectives will be met*", while the PricewaterhouseCoopers defines it as *"an effective approach to identifying and managing areas of risk exposure, as well as highlighting potential opportunities."*

As its name indicates, CSA is not an independent assessment. Rather, it is done by process owners and managers to assess whether internal controls in business areas under their responsibility are effective and, in turn, have and provide assurance that business objectives are being met. Often, CSAs are led by someone experienced in internal controls and risk and control concepts. The data produced from this exercise gives management a comprehensive view of its operations from bottom-up. The power of self-assessment lies in its ability to provide information that would not otherwise be easily

obtainable, through the participation of employees who know, better than anyone, what is helping them or stopping them from getting their work done. It is a valuable tool in performing oversight, especially for international organizations such as the CGIAR System where operations are distributed globally. In analyzing the information gathered from different locations, it is often found that some issues repeat themselves, which could be used by management to drive change across the organization.

2.4 Possible Involvement of Internal Audit

The Internal Audit's involvement in CSA exercise can be significant and may involve sponsoring, designing, implementing and, in effect, managing the CSA process - conducting CSA training, orchestrating the participation of key management and staff, and scribing and reporting CSA outcomes. In other CSA exercises, the Internal Audit's involvement may be minimal, serving as an interested party and consultant to the whole process and as an ultimate verifier of the evaluations produced by the teams. In most exercises, the Internal Audit's involvement will be somewhere between these two extremes.

Whatever the role, Internal Audit maintains professional independence and objectivity. Internal Audit contributes expertise in relation to the assessment, implementation and effectiveness of internal controls, similar to other auditing techniques. Management remains responsible for the effective operation of internal controls and for considering and making decisions based on advice received from a CSA report. However, whether a CSA exercise has been conducted independently of the Internal Audit or there was minimal involvement, it is desirable for the Internal Auditor to review outcomes of the CSA, as a means of helping to validate the risk assessments and proposed action plans and to help ensure that Internal Audit remains up to date with the risk profile of the area or function concerned.

2.5 Challenges and constraints

Before developing a CSA methodology, it is important for an organization to have a business plan with a clear set of objectives, usually documented in an organizational strategy. Ultimately, the purpose of a CSA is to see whether an organization can achieve its objectives, by checking how strong its internal controls framework is. So, while internal controls are critical in any organization, their strength cannot be properly gauged if business objectives are not there or are not clearly communicated to all involved.
Once objectives have been set, some of the challenges that may be experienced when developing a CSA are:

A) *Management buy-in or support*
Tone from the top is important. If there is no support from management, the implementation of CSAs (or any initiative for that matter) will not take off. Participants would also likely view activities related to CSAs as trivial and a waste of time. Management should be given a clear understanding of the benefits of CSAs and how this could help the organization. Management involvement throughout the development process of the CSA as well as its roll-out would also ensure the right level of response from process owners.

B) ***Educating respondents on risk and control concepts***

Participants should be able to understand risk and control concepts. Otherwise, CSAs produced might be irrelevant, too detailed, or too high-level. At the start of the CSA implementation, a training on how to properly conduct this exercise should be given to participants.

C) ***Ensuring timely completion and submission of the self-evaluations***

Despite there being management buy-in and participants being supportive of the CSAs, timeliness may still be an issue especially where other more pressing matters are at hand. At worst, the CSA is continually delayed and end up not being done at all. A way to address this is to include CSA exercises as part of deliverables of regional or country offices and business units, in the same way as they are required to report on their research activities or finances.

D) ***The assessments produced may be inaccurate or fraudulent***

Given that the nature of a CSA is that it is a self-test, there is a chance for the information provided in the CSAs to be incorrect, whether by mistake or deliberately. This may depend on the environment and culture of an organization and/or an office. This should be considered when choosing a CSA approach to be used. For example, if experience has shown the likelihood of fraudulent activities to be a prevalent ina country office, then perhaps a workshop approach would be best, and should be facilitated by someone not directly connected with the office but is familiar with its internal controls framework, such as an Internal Auditor. Validation procedures are usually done after a CSA exercise; however, the depth of validation may depend on several factors. This is further discussed in the Good Practices section, under reporting.

3. GOOD PRACTICES

3.1 Summary

Once the challenges and constraints have been considered, a CSA can be developed. Whether the CSA approach is a facilitated workshop, a structured questionnaire, a management-produced analysis, or a combination of these, the basic premise remains the same, as follows:

Plan	Design	Execute	Report
• Evaluate organization's objectives • Gather preliminary information • Determine CSA scope • Determine CSA approach • Create timeline, allocate resources	• Select participants • Communicate • Design the workshop / design questions for survey	• Conduct workshop / send out questionnaire	• Validate the results • Analyze results and document into a formal report • Monitor action plans

The good practices are summarized below:

A) *Plan*
- The CSA exercise is led by a person trained and experienced in internal controls system design.
- CSA objectives and scope are clearly set.
- The appropriate CSA approach is determined based on information gathered.
- A schedule is prepared, identifying projected timeline for each CSA activity and milestone.
- Adequate investment of time and resources are identified and provided for CSA exercise.

B) *Design*
- Participants selected should be those who can provide relevant information regarding the scope.
- The design of the CSA (questions for surveys, starting point and objective of discussion for workshops) is planned and discussed with management beforehand.
- Tools and resources are prepared prior to the CSA exercise.
- In a questionnaire approach, the questions should both provide information on the process or business area being assessed, as well as test for the existence of key controls.

C) *Execute*
- The CSA objectives, purpose and process are communicated to appropriate levels of management and to participants.
- Participants are aware of risk and control concepts and understand expectations from them in the CSA.
- In a questionnaire approach, the deadline to respond is communicated properly to participants.

- In a workshop approach, information captured during the discussion is summarized and confirmed by participants.

D) *Report*
- The information received from the workshop/questionnaire is examined as to its validity.
- After validation, the results of the CSA are analyzed and reported.
- Any action plans identified during the CSA exercise are included in the report.
- The implementation of action plans is monitored periodically.

3.2 Planning the CSA

To begin with, management involvement and buy-in should be secured. As previously discussed, management sets the tone determining how useful the CSA will be and how well it will be received by process owners. The benefits of the CSA should be communicated to management and they should be involved in its implementation as much as possible. It is important for management to be aware that they are not control specialists and may not be able to identify weaknesses in the control framework.

Accountability is also one of the keys to the success of a CSA. It should be clearly defined who owns the process and who is accountable for it. Process owners are management and staff who are directly involved with or affected by a particular process under examination, who know them best and are critical to the implementation of appropriate controls.

The CSA activities are usually owned and led by management. An organization's Internal Auditor may provide assistance by initiating the activity but the ownership of the CSA should eventually be handed over to management following the second line of defense model (see page 5). An organization may choose to hire a consultant with CSA expertise to lead the CSA activities, or identify a CSA Coordinator from within the organization, such as a risk manager or a compliance manager. Whoever fills up this role, it is important that he/she has a full grasp of internal controls. The CSA Coordinator would manage the implementation of the CSA, from getting the buy-in of management to reporting on the CSA outcomes. It also involves conducting CSA trainings, ensuring participants have a good understanding of risk and control concepts, as well as of expectations from them in the CSA exercises.

In CSA planning, it is integral to visualize what the final product is expected to look like. In such a way, CSA objectives can clearly be identified which gives the CSA exercise a structure on how it will be performed. CSA objectives should be defined based on organization's priorities, and in alignment with the organization strategy or business plan. Management input should be sought as this further clarifies broad objectives. Management would also be able to identify major concerns that a CSA can focus on.

The scope of the CSA should also be clearly defined. This begins with a defined CSA objective/s. Management needs to factor in the country offices and processes which they consider as high risk areas requiring regular monitoring. For example, if the CSA objective is to have more transparency in regional and country office operations, scoping may begin with identifying risk areas in the region and country office.

The size of regional and country operations varies. The following is a list of areas that can be considered when developing a CSA scope:

- Governance and legal
  - o Hosting arrangements
  - o Compliance with statutory requirements
  - o Updates on the country strategic plan and
  - o Risk management
- Resource Mobilization
- Proposal development
- Grant & Project Management
- Research & Intellectual Property
  - o Publications and reviews
  - o Compliance with IP principles
- Partner management
- Finance management
  - o Cash management (cash-in-bank, petty cash, revolving fund)
  - o Payroll
  - o Advances (travel and loan)
  - o Consultancy expenses
  - o Receivables
  - o Statutory payments
  - o Overall expenditure
- Procurement
- Asset Management
- Human Resources
- Information Technology
- Monitoring and Evaluation
- Safety & Security
- Fraud

Information gathering activities need to be performed to determine the scope. To do so, the CSA Coordinator may conduct preliminary interviews with process owners, and review reference documents such as policies and procedures, risk assessments, internal and external audit reports, and others.

While gathering information, the CSA Coordinator should also understand the environment and culture of an organization to determine the best approach to use in the CSA exercise. For example, if the intended participants are globally distributed and bringing them together to have a workshop would delay the CSA or end up being too costly, then a questionnaire may be a better approach. The following will help determine the appropriate CSA approach:

- CSA objectives
- Organization objectives
- Organization, region/country office culture

- Risk assessment
- Geographic distribution
- Capability in respect of facilitating a workshop
- Technology available
- Budget and resources
- Timing and staff availability.

3.3 CSA approach

The two primary forms of CSA are: facilitated workshops and structured questionnaires. An organization may also have a management-produced analysis, such as an internal controls analysis done through interviews, document reviews and validations. A combination of these approaches may also be performed.

Facilitated workshops are more frequently used by organizations. In this approach, work teams from which internal control information is gathered are formed. A facilitator, trained in internal controls system designs, guides the workshop. Through a facilitated workshop, information can be obtained in a shorter amount of time.

Questionnaires or surveys are often used where there are numerous respondents, or if respondents are too widely dispersed to be readily brought together for a workshop. Questionnaires are also preferred if the culture of the organization might hinder open, candid discussions in workshop settings or if management desires to minimize the initial time spent and cost incurred in gathering the information.

Once a CSA approach is determined, it is easier to understand how much time is needed as well as the resources required to complete a CSA exercise. A schedule should be prepared, defining CSA milestones, activities and its projected dates. Among the key milestones are the completion of the following:

- An agreed plan and budget
- Any preliminary training required for participants
- The design of the CSA exercise
- Execution of the CSA exercise
- Reporting on the results
- Follow up/action planning.

The associated costs and resources needed should also be identified. This puts in detail the investment needed in implementing a successful CSA. The time and resources needed largely depend on the CSA approach chosen. For example, the number of hours needed from participants for a workshop differs from what is required in completing questionnaires. Workshops may be done in a classroom format (include travel-related costs) or through webcasts. Questionnaires, although generally less costly, may require a longer turnaround time than a workshop.

3.4 Design and Execute the CSA

The design of the CSA depends on the objective, scope and approach determined during the planning phase. Input from management should be sought in designing the CSA, so that any concerns and issues are included and answered during the assessment.

Participants selected should be those who can provide relevant information regarding the scope, such as process owners or members of management. They should then be informed beforehand of the CSA objectives and scope, and be given a clear understanding of expectation from them in the CSA exercise.

3.4.1 Facilitated workshops

The work groups in a workshop should be carefully composed so that they are not too large that participants' inputs are not heard, or too small that it might as well have been an interview. The grouping of participants should be made in a way that allows for a candid and open discussion.

The CSA Coordinator should make sure to obtain commitment from the participants. This may be as simple as sending an invit so that participants are aware of the date and length of time required, as well as ensuring that their schedule is allotted for the workshop. The CSA Coordinator may further impress on the participants that management supports the activity and communicate to them about the benefits of the CSA.

Additionally, the CSA Coordinator should let participants know the expectations from them as this encourages them to prepare and refresh their knowledge on the subject matter to be discussed in the workshop. If possible, the materials to read regarding CSA concepts should be given to them in advance, as well as any policies, procedures or any other reference documents available. This helps ensure that participants are empowered with the basic knowledge needed in the workshop and can participate more. This also helps establish one of the CSA Coordinator's responsibilities: to ensure that participants are aware of risk and control concepts.

In a workshop approach, the role of a workshop facilitator is usually filled by a CSA Coordinator. One of the challenges is to establish an environment in which participants feel free to disagree, try out new ideas, discuss their own experiences and propose solutions, conclusions or strategies. The facilitator stimulates and guides the discussion. His/her role is to:

- Keep the discussion moving, ask questions, provoke different views, promote a lively exchange of ideas
- Ensure the discussion stays on-topic
- Get as many of the participants involved in the discussion as possible
- Provide facts, policies, laws as needed (or from other participants).

The facilitator should ensure, beforehand, how the outputs of the discussion will be recorded. This may be done through unsophisticated methods such as noting them on a whiteboard, on flipcharts, post-its (usually noted by participants and pasted on the board), drawings, sketches and others. The best way to preserve these outputs (or 'artefacts') is to take photographs as paper is easily lost and

can be cumbersome, especially if there are many artefacts to be expected through numerous workshops. More sophisticated methods of recording may also be used, such as the use of a voice or video recorder. Just remember to obtain consent from participants. Also, consider the culture of the organization or office, whether the use of recording devices would hinder participation.

The starting point of the workshop could be any of the following. Since they are all intended to arrive at the same outcome, none are inherently preferable:

- Business objectives – the discussion begins with identifying the business objectives and the best ways to accomplish these objectives to ensure that the best control techniques have been selected and that these techniques are working to reduce the residual risk to a minimum.
- Business risks – focuses on identifying and managing risks. It evaluates the mitigating actions addressing key business risks to identify any significant risks for corrective action.
- Internal controls – focuses on how well the controls in place are working. The main aim is to produce a gap analysis between how controls are working and how management intended these controls to work.
- Business processes – examines the activities performed within selected processes. The main aim is to evaluate, update, and/or streamline selected processes.

At the end of the workshop, the conclusion or ideas from each group are usually reported to the full group. This is to ensure that the facilitator could accurately capture the points discussed. This also gives the participants additional time to review and raise any other concerns that were not raised before.
Additionally, if the purpose of the workshop is to get action plans for any weaknesses noted, ensure that these are captured correctly by obtaining confirmation from participants.

3.4.2 Questionnaires

As for the workshop approach, the CSA Coordinator should also take steps to obtain a commitment from respondents. Prior to sending the questionnaire, let them know about the CSA activity and that a questionnaire will be sent out to them at a certain date. In this announcement, note that the activity is supported by management. Also, include the purpose of the CSA, how their responses are going to be used, and how such activity will benefit them. Expectations from them should be clear, as well as the timeline—when they will receive the questionnaire, when their responses will be due, and when reporting will be done.

In creating the questionnaire, the content should specify the internal control objectives for the areas included in the CSA scope. Questions should be designed to test for the existence of key controls, but also provide information on the process or business area being assessed. The following seven steps will help in designing a questionnaire:

Step 1: Decide what information is required. The starting point should be the CSA objective/s and the business area in-scope. List all key controls that should be in place, but also consider the culture and environment of the organization to assess which controls are, at a minimum, expected to be in place.

Input from management must be sought so that main concerns are included in the set of questions, as well as any issues flagged while planning the CSA.

Step 2: Make a rough listing of the questions. The aim is to be as comprehensive as possible in the listing and not to worry about the phrasing of the questions.

Step 3: Refine the question phrasing. Here, the questions are developed to the point where they make sense and will generate an appropriate response.

Step 4: Develop the response format. This could be a pre-coded list of answers or it could be open-ended to collect verbatim comments.

Step 5: Put the questionnaires into an appropriate sequence. This brings logic and flow to the questions.

Step 6: Finalize the layout of the questionnaire. Include clear instructions, an introduction and expectations from the respondent.

Step 7: Choose the Best Delivery Method. Questionnaires can be delivered over the computer (through emails or web surveys), in person, or on the phone. Face-to-face can be expensive but will generate the fullest responses. Web surveys or emails can be cost-effective but inconsistent with response rates. Telephone can be expensive, but will often generate high response rates and will allow for follow-up questions to enhance findings. If there are many respondents, email or web surveys are likely to be the best option, however deadlines should be clearly set in the questionnaire. Reminders before the deadline should be sent to the respondents, as well as follow-ups in case of any delays.

An additional step is to test the questionnaire. In a pilot, the aim is to make sure that the questionnaire works. Time and money can preclude a proper pilot so, at the very least, it should be tested on one or two colleagues for sense, flow and clarity of instructions. In theory, the questionnaire should be piloted using the method that will be used. The whole purpose of the test is to find out if changes are needed so that final revisions can be made.

Below are some additional tips in constructing questionnaires:

- Include simple instructions on how to complete the questionnaire. If the question requires a rating, define the rating system.
- Use plain language. Be direct and avoid jargons as much as possible. Include definitions if needed.
- Be brief. Focus on 'need to know' and minimize 'nice to know'.
- Put the most important questions first. Respondents may get fatigued by later questions.
- Ask questions one at a time.

If the questionnaire is in the form of document attachment, ensure that the file is protected so that respondents cannot inadvertently change or remove any of the questions or the pre-coded responses. Make sure to specify the expected date of completion. Send out reminders as well before it is due, particularly if the questionnaires were sent out months earlier.

Upon sending out the questionnaire, reiterate the expectations from the respondents as well as the expected turnaround time for them to complete the questionnaire. If the turnaround time is a month or longer, it is best to send out a reminder prior to its due date.

3.4.3 Combination approach

This format tends to be launched via an initial workshop approach followed in future periods by a questionnaire for subsequent CSA exercises, with a further workshop if a new activity or major trigger event occurs. A hybrid approach can often be successful in maintaining momentum/keeping the process alive over time without overburdening the participants.

3.4.4 Reporting

Upon completion of the workshops or questionnaires, the CSA Coordinator must first examine and assess whether the information is valid. This, however, does not mean that an audit should be conducted. The extent of the validation depends on the consistency of the testimonies from one participant to the other and whether information received is complete. Where necessary, the validation may include making additional inquiries with managers/staff, the use of follow-up questionnaires, or gathering supporting documents. Once this is done, a report on the CSA should be prepared.

The report should summarize the results of the CSA and provide a coherent, integrated view of the operational risks and existence of controls to manage them. The more the individual components of the framework provide consistent indicators of where the risks of the organization lie and the likelihood of events and their severity, the more effective will be the design and the operation of the overall control framework.

There is no prescribed format for reporting CSA results since this depends on the objectives of a CSA and its intended use. However, its contents may highlight or include the following:

- Emerging issues or trends
- Areas in need of improved controls / with control gaps
- Clusters/concentration of risks
- Duplication of controls or over-control.

Another way to interpret and report the CSA results is to map them against a maturity model. Below is an example of a maturity model that can be used to determine the strength of internal control frameworks based on CSA results.

Maturity level of internal control frameworks			
Level 1	Level 2	Level 3	Level 4
Informal or ad hoc	**Standard**	**Managed and monitored**	**Optimized**
Control activities fragmented Control activities may be managed in "silo" situations Control activities dependent upon individual heroics Inadequate documentation and reporting methods Inadequate monitoring methods	Control awareness exists Control activities designed Control activities in place Some documentation and reporting methodology exists Automated tools and other control measures may exist, but are not necessarily integrated within all functions or consistently used Accountability and performance monitoring requires improvement	Key Performance Indicators (KPI) are defined for monitoring effectiveness Well-understood chains of accountability exist A formal controls framework exists Automated tools and other control measures are consistently used to generate more standardized assessments	Highly-automated control infrastructure is in place and consistently used Benchmarking, best practices and continuous improvement elements incorporated into monitoring efforts Real-time monitoring

3.4.5 Action plans and recommendations

Action plans and recommendations should be included in the CSA report, if the intention of the CSA exercise is to improve and strengthen the organization's control framework. Action plans may also have been identified in a workshop approach, which should then be included in the CSA report.

Action plans are those that the process owners have already identified or agreed with during the CSA exercise. Recommendations come from the CSA Coordinator or in consultation with the Internal Auditor (if the Internal Auditor is not the CSA Coordinator). Recommendations need to be agreed with management and process owners for their proper implementation. In documenting the action plans and/or recommendations, the expected due date should be included and a responsible person.

To ensure that the action plans and/or recommendations are properly implemented, monitoring activities should be in place. The CSA Coordinator follows-up with the management on the status of implementation prior to the next CSA exercise. An organization may also have a mid-year status update, wherein process owners can inform management of any issues with regard the

implementation of the action plans/recommendations, any additional resources needed, or whether there is a need to adjust the due dates.

Tools can be used to monitor action plans. Some organizations invest in the use of automated tools such as keeping a controls database and recording the results of a CSA exercise, any action plans, their due dates and responsible person.

3.5 Good practice in CGIAR

There are examples within CGIAR where CSAs were successfully used or are being implemented. A CSA approach used in WorldFish is described in the Appendix A.

At the time of writing of this GPN, 3 Centers in Americas, CIP, CIAT and IFPRI were implementing CSA approach to monitor their field offices' compliance with the Centers' policies and procedures.

4. ROLES AND RESPONSIBILITIES

The main players in the successful implementation of CSAs are: Management Team, a Steering Committee, a CSA Coordinator, and the process owners.

A) **The Management Team** (MT) is responsible for**:**
- Establishing and overseeing overall internal control framework of the organization
- Developing the organization's strategy and key business objectives
- Recommending CSA methodology changes
- Recommending scoping decisions
- Monitoring and overseeing execution of CSA program against the agreed milestones.

B) **A Steering Committee** (SC) that would be taking on the last three bullet points listed above, may also be formed. The membership of the SC includes:
- Key process owners
- Internal Audit
- CSA Coordinator.

C) **The CSA Coordinator** (CSAC) is responsible for:
- Planning and leading the CSA exercise
- Reporting the results of the CSA exercise
- Delivering trainings as required
- Ensuring the completion of each CSA milestone
- Monitoring and reporting progress of action plan implementation.

The CSAC must be well-versed in internal control designs, as such this role may be taken up by an organization's internal auditor. However, an organization may also assign this role to a Risk Manager or other similar position. Alternatively, an external consultant with expertise in CSA may also be hired.

If the CSAC role is not taken up by the Internal Auditor (IA), the IA provides support and consultation to the CSAC. The IA should review outcomes of the CSA, to help validate the risk assessments and proposed action plans and to help ensure that the IA remains up to date with the risk profile of the area or function concerned.

D) **The Process Owner** (PO) is responsible for:
- Operating effective and efficient business processes
- Making necessary resources and information available to the CSAC
- Participate in the CSA exercise as a subject-matter expert on the process or business unit being assessed
- Identify risks and opportunities with current process, as well as any issues
- Identify action plans / review CSAC recommendations
- Implement CSA action plans/recommendations.

As previously described, POs are management or staff members who know best a particular process and are critical to the implementation of appropriate controls. A PO is typically a head of a function or department. For regional or country offices, these are usually the Regional Director/Coordinator or Country Director/Coordinator as this position should be aware of the whole operations in the office. However, POs may also be subject-matter experts such as project accountants, research administrators and others.

Below is a summary of the steps in a CSA, showing the parties responsible, accountable, supporting, consulting, and in need to be informed. This includes the role of the IA, supposing that he/she has not taken over the CSAC role and is only consulted.

Activity	Responsible[1]	Accountable[2]	Support[3]	Consulted[4]	Informed[5]
Identify CSA objective	CSAC	MT/SC		MT/SC, IA	PO
Identify CSA scope	CSAC	MT/SC		MT/SC, PO, IA	PO
Identify CSA approach	CSAC	MT/SC		IA	PO
Prepare work plan and budget	CSAC	MT/SC			PO
Train process owners on risk and control concepts and CSA	CSAC			MT/SC	PO
Design workshop/ questionnaire	CSAC	MT/SC			
Lead CSA exercise	CSAC		PO, MT		
Participate in CSA exercise, provide input	PO, MT				
Summarize results	CSAC		PO		PO
Identify action plans in workshop	PO, MT	MT	CSAC		
Validate and analyze results	CSAC	MT/SC	PO	IA	
Identify recommendations	CSAC	MT/SC, PO		IA	

[1] Responsible: Those who do the work to achieve the task. There is at least one role with a participation type of responsible, although others can be delegated to assist in the work required.

[2] Accountable (final approving authority): The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those responsible. In other words, an accountable must sign off (approve) work that "responsible" provides. There must be only one "accountable" specified for each task or deliverable.

[3] Support: Resources allocated to "responsible". Unlike "consulted", who may provide input to the task, "support" helps complete the task.

[4] Consulted: Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.

[5] Informed: Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

Activity	Responsible[1]	Accountable[2]	Support[3]	Consulted[4]	Informed[5]
Monitor implementation of action plans/ recommendations	CSAC		PO, MT/SC		IA
Implement action plans / recommendations	PO	MT/SC			CSAC, IA

5. BIBLIOGRAPHY AND CREDITS

This GPN was developed under the leadership of Pierre Pradal, CGIAR IAU Director, by Steve Korir and Charisse Ragasa, CGIAR IAU Internal Auditors and Madina Bazarova, CGIAR IAU Associate Director, with kind contributions from WorldFish.

It was based on the following materials:

- A perspective on Control Self-Assessment, 1998, The Institute of Internal Auditors
- Auditing Assurance, CSA, 1998, Bruce Mc Cuaig
- Control Self-Assessment, 2015, PricewaterhouseCoopers
- Controls Transformation, 2015, Deloitte
- Guidance on Monitoring Internal Control Systems, 2008, COSO
- Internal Control - Integrated Framework, Executive Summary, 2013, COSO
- International Standards for the Professional Practice of Internal Auditing (Standards), revised 2012, The Institute of Internal Auditors
- International Standard of Auditing 200 (ISA 200), 2009, The International Auditing and Assurance Standards Board
- IS Auditing Procedure, Control Risk Self-Assessment (CRSA), 2003, Information Systems Audit and Control Association (ISACA)
- Leveraging COSO Across the Three Lines of Defense, 2015, Douglas J. Anderson and Gina Eubanks, research commissioned by COSO
- The COSO Framework and SOX Compliance, 2013, J Stephen Mc Nally
- The Key Principles of Effective Questionnaire, 2006, B2B International
- The Process of Control Self-Assessment and its Use in Risk Management, 1999, L du Plessis and G. P. Grobler
- What is Effective Training?, 2003, Human Rights NGO Capacity Building Program - Iraq

APPENDIX 1: USE OF CONTROL SELF-ASSESSMENT AT WORLDFISH

The use of CSA at WorldFish was initiated by Internal Audit to obtain a baseline information on compliance with key controls by the Center's country offices. The CSA approach has been agreed with management against the following objectives:

"- To identify areas of support needed and improvements across the organization, to address any gaps systematically and efficiently as opposed to by each country office strengthening controls at a local level

- It will help management have an overview of key controls at each country level and incorporate any action stemming from the self-assessment into annual plans

- It will also give them a baseline to compare the progress to over time

- The self-assessment will increase awareness of controls expected to be in place

- It will also help Internal Audit to focus on areas of importance e.g. providing assurance over the controls that have been indicated to be in place."

Considering the time constraints and the fact that the information had to be gathered from 6 country offices, it was decided to use a self-assessment questionnaire. The questionnaire was developed by the CGIAR Internal Audit Unit based on prior knowledge, WorldFish policies and expectation for country offices, and explores compliance with key controls within 11 areas of business, including:

- Governance and legal
- Research and IP
- Finance
- HR
- Procurement
- Asset management and inventory
- IT
- Grant and project management
- Partner management
- Safety and security
- Monitoring and evaluation.

In addition, several General questions were asked to explore past and present trends e.g. increase/reduction in funding. The areas to be covered and questions to be asked were then validated with subject matter experts within WorldFish. The questions asked are listed at the end of this Appendix.

Once the questions were agreed, they were uploaded on SurveyMonkey and the link to them was sent to key contacts at the Country Offices. Considering that the questionnaire covered a wide range of topics, country management was suggested to involve staff from all the departments to complete the questionnaire. The answers solicited for the areas listed above were binary: Yes or No, so that the returned data is easy to analyze. The General questions required specific alphanumerical answers in certain format.

Once the returns from the countries were received, they were reviewed for completeness and sense checked by Internal Audit. Where needed, follow up questions were asked and responses obtained.

The information was then analyzed and results presented to WorldFish Board with suggested actions to address identified gaps and emerging risks.

To reap the benefits of the information garnered using the CSA, the Center can continue using the questionnaire, for example once a year as part of the annual planning exercise. It will allow the Center to:

- identify trends e.g. improvements or deterioration in compliance with key controls
- improve efficiency of its support activities of country offices focusing on where the biggest gaps are
- identify cross-cutting themes where institutional intervention is needed e.g. deliver training on a specific topic across country offices to build their capacity in key control implementation
- re-enforce key controls as country offices will be consistently reminded of them when completing the questionnaires
- to provide assurance to the Board of the existence and efficiency of oversight activities by continuous monitoring of compliance with key controls.

The questionnaire used at WorldFish is presented below:

Control self-assessment for country offices

1. **General information**

Area/question
Office name e.g. Bangladesh country office
Annual expenditure budget FY 2016, USD
Annual expenditure budget FY 2015, USD
Number and value of new proposals submitted FY 2016
Number and value of new proposals submitted FY 2015
Number and value of successful proposals FY 2016
Number and value of successful proposals FY 2015
Number and value of active grants as of end of June 2016
Number of staff as of end of June 2016
Number of staff joined in 2016
Number of staff left in 2016
Number of consultants deployed as in 2016
Number of vehicles as at end of June 2016
Number of vehicles as at end of June 2015
Value of assets (from the asset register)
Value of inventory (both administrative and research)
Project locations

Area/question
Organizations being hosted
Organization that hosts your office
Number of donor audits in the last year
The amount of donor disallowed expenditure in the last year
Number of fraud, grievance, whistle-blowing cases, litigations in the last year

2.   Governance & legal

Control
G1.   Is the MoU with the host government up-to-date?
G2.   Were the office legal/regulatory arrangements (e.g. tax remittance, registration, policies, contracts etc) reviewed by an independent legal expert for compliance with local legislation?
G3.   Is an up-to-date country strategic plan in place?
G4.   Was the plan approved by HQ?
G5.   Is there an up-to-date country risk register in place?
Are WorldFish policies and procedures available to all staff?

3.   Research & IP

Control
R1.   Are research activities based on an approved strategic plan and supported by a sound design?
R2.   Does technical capacity exist to deliver research activities against research commitments?
R3.   Is value of strategic partnerships to achieve research objectives regularly reviewed?
R4.   Are adequate research facilities and sites in place to achieve research objectives?
R5.   Has research ethics review been completed at project design stage where required?
R6.   Are all research activities adequately documented and research data kept in a secure central depository?
R7.   Are all research results shared or published with approval by a thematic/program lead?
R8.   Are research activities subject to a regular review by global science? When was the last review conducted?

Control
R9.   Are measures put in place to secure IP rights? Are all contracts in compliance with IP Policy?

4.   Finance

Control
F1.   Is there an up-to-date country office finance manual?
F2.   Are cash flow needs estimated monthly?
F3.   No one person that has sole access to the safe
F4.   Are cash counts conducted weekly, reconciled to cash balances in OCS and signed off by the country director (or equivalent)?
F5.   Are bank reconciliations conducted monthly and signed off by the country director (or equivalent)?
F6.   Are all budgets up-to-date in OCS?
F7.   Are budget monitoring reports produced monthly by finance and shared with budget holders?
F8.   Are reasons for underspend/overspend identified/documented and addressed?
F9.   Are revenue (pipeline) and anticipated expenditure reviewed on at least quarterly basis and any gaps identified are flagged to HQ and addressed?
F10. Is UAT analysis carried out at least quarterly and any gaps identified are flagged to HQ and addressed?
F11. Does the person who has access to cash also enter transactions in OCS?
F12. Are all transactions posted in OCS approved by a budget holder as per the delegation of authority and reviewed by finance?
F13. Are balance sheet reviews/reconciliation conducted on a monthly basis?
F14. Are financial controls subject to a regular review by HQ? When was the last review conducted?

5. HR

Control
H1. Is there an up-to-date country office HR manual?
H2. Are all new positions approved as per the delegation of authority confirming availability of budget to cover the costs?
H3. Is any conflict of interest in recruitment declared?
H4. Do all newly recruited staff attend a standard induction program?
H5. Are all staff engaged with up-to-date signed contracts?
H6. Do all staff have up-to-date job descriptions?
H7. Is an up-to-date office organogram in place?
H8. Do all staff have agreed work objectives and, learning and development plans?
H9. Do all staff have annual performance reviews?
H10. Is staff attendance tracked?
H11. Is payroll reconciled to staff attendance records and employment contracts?
H12. Is payroll month-on-month reconciliation carried out and authorized by the country director or equivalent?
H13. Do Health and Safety protocols comply with local legal requirements and applicable international regulations?
H14. Are all staff trained in Health and Safety protocols?
H15. Are HR activities subject to a regular review by HQ? When was the last review conducted?

6. Procurement

Control
P1. Is an up-to-date country office procurement policy in place?
P2. Are procurement requisitions (PR) raised for every purchase?
P3. Are PRs approved by a budget holder?

Control
P4. Is there a list of authorized vendors?
P5. Was a due diligence carried out on authorized vendors?
P6. Are quotations sought from authorized vendors?
P7. Are all exceptions from the approved procurement process authorized by HQ?
P8. Is procurement committee in place and its mandate is clear?
P9. Does the procurement committee consist of staff outside the procurement function?
P10. Are decisions to select a supplier documented and justified?
P11. Are procurement staff aware of donor procurement rules?
P12. Are all purchase orders authorized as per the delegation of authority?
P13. Are supplier invoices only paid for goods/services delivered?
P14. Are procurement activities subject to a regular review by HQ? When was the last review conducted?

7. Asset management and inventory

Control
A1. Are all assets registered in an up-to-date asset register?
A2. Are all assets tagged with irremovable/unique tag labels?
A3. Is asset count conducted at least once a year and reconciled to a previous asset count?
A4. Are asset counts conducted by staff outside asset management function?
A5. Are assets disposed of as per donor requirements?
A6. Is access to inventory restricted to an authorized person?
A7. Are periodic inventory counts carried out?
A8. Are asset controls subject to a regular review by HQ? When was the last review conducted?

8. IT

Control
I1. Is there a dedicated IT specialist in place? (Please indicate whether it's an in-house or outsourced position)
I2. Are regular meetings held to discuss IT performance, IT issues and developments with central IT team?
I3. Have policies been established covering IT Operations, IT Security and Service Management?
I4. Is the IT landscape subjected to a regular IT security review?
I5. Are regular backups performed for organization data on all computers?
I6. Are performance indicators established and monitored for the IT function?

9. Grant & project management

Control
GR1. Are all proposals recorded in OCS?
GR2. Are all proposals reviewed and signed off as per the delegation of authority?
GR3. Are all approved projects recorded in OCS?
GR4. Is proposal success/failure analyzed and learned from?
GR5. Are donor agreements signed as per the delegation of authority?
GR6. Is grant information in OCS complete?
GR7. Is compliance with donor terms and conditions monitored?
GR8. Are all donor reports submitted on-time?
GR9. Are all donor reports approved as per the delegation of authority?
GR10. Are all projects have SMART objectives and clear ToCs with specific outputs and outcomes defined?
GR11. Are all projects outputs and outcomes recorded in OCS?
GR12. Are all projects have timed implementation work plans and budgets?

Control
GR13.Are all project activities monitored against the implementation plans and budgets monthly?
GR14.Are changes to project scope and deliverables approved at appropriate level?
GR15.   Are all donor grants that expired closed in OCS within 6 months?

10. Partners

Control
PR1. Is country office partner engagement manual in place?
PR2. Are partners selected based on a competitive process? If not, is justification clearly documented?
PR3. Do all partners undergo due diligence before being engaged?
PR4. Are all partner contracts signed as per the delegation of authority?
PR5. Do partner contracts contain partnership objectives, contract amounts and budgets, reporting schedules, original donor rules, IP requirements, confidentiality clauses and right to audit?
PR6. Are partners paid only after satisfactory submission of reports and completion of deliverables?
PR7. Are partner reports reviewed by finance and projects for accuracy, completeness and compliance with partner agreement?
PR8. Are partner activities monitored on a regular basis?
PR9. Are partner payments tracked against partner reports?
PR10.   Are all partner contracts recorded in OCS?

11. Safety and security

Control
S1.   Are country office safety and security risks assessed on a regular basis?
S2.   Are safety and security procedures in place and reflect risk levels?
S3.   Are staff regularly informed of any changes in risk levels and risk environment?
S4.   Are staff trained on managing security risks and on WF security management protocols?

Control
S5. Is an up-to-date security tree in place and communicated to all staff?
S6. Has the security tree being tested?
S7. Are whereabouts of all staff being tracked and travelers get an up-to-date information on the security risks?
S8. Are all safety and security incidents reported to HQ and responded to?

12. Monitoring and evaluation

Control
M1. Are project activities monitored against outputs and outcomes on a regular basis?
M2. Are the results of the monitoring recorded, reported and any gaps are addressed?
M3. Is monitoring conducted based on accurate and complete project data?
M4. Are long-term projects evaluated to understand/correct their progress and outcomes?