Bureau of Customs and Border Protection
Best Practices
Of Compliant Companies

1. **Have management's commitment.** – *(Control Environment)*
   Demonstrate management's commitment to compliance.

   - Establish a statement of corporate policy that addresses Customs and Border Protection (CBP) matters.
   - Solicit a statement from the Board of Directors that assigns authority and responsibility to the customs group.

2. **State compliance and cost goals.** – *(Risk Assessment)*
   Identify and analyze relevant risk and develop internal goals to manage the risk.

   - Conduct post-entry reviews and compare these against established goals.
   - Determine how risk areas should be managed.
   - Resolve control weaknesses in a timely manner.

3. **Develop formal policies. –** *(Control Activities)*
   Develop, implement and/or modify formal policies and procedures to ensure that management's goals and objectives are met.

   - Verify the accuracy of the Internal Control Manual to ensure processes and procedures achieve prescribed goals and objectives.
   - Modify controls that are ineffective or inefficient and report to management.
   - Define accountability and controls in job descriptions.

4. **Establish training programs.** – *(Information & Communication)*
   Ensure that employees receive appropriate training and guidance to effectively discharge their responsibilities.

   - Convey pertinent information to the right people at the appropriate time.
   - Disseminate CBP information via company's communication system (i.e. intranet, bulletin board, mail).

5. **Conduct internal control reviews.** – *(Monitoring)*
   Conduct periodic process reviews to assess the performance quality of the internal controls.

   - Use external or internal audit to periodically review each business unit to confirm that corporate policies are implemented and mandate corrective action when necessary.
   - Adjust testing in response to changing risk.

6. **Create compliance group.** – *(Information & Communication)*
   Establish a customs group.

   - Foster open communication channels between all departments that may be involved in the CBP processes.
   - Establish control activities and self-testing processes to verify the accuracy of the company's internal control system since the quality of the information generated affects the ability of management to make decisions.

7. **Access executives for needed resources.** – *(Control Environment)*
   Raises the importance of the Customs group and provides adequate authority for the group to interact with other departments as needed.

   - Organize the customs group so that it is visible to top level management. (e.g. attaching to tax or legal department/division)
   - Provide an awareness of supply chain structure. Many executives know their sales figures but do they know their key import statistics and suppliers?

8. **Develop compliance requirements for suppliers.** - *(Control Activities)*
   Develop contract language on purchase agreements.

   - Develop and implement controls to help ensure that CBP transactions are valid, properly authorized and accurately processed.
   - Request suppliers provide regulatory reporting information when applicable (NAFTA, GSP, etc.).
   - Exercise reasonable care over operations performed by service providers.

9. **Establish a record-keeping program.** - *(Control Activities)*
   Establish a record-keeping program.

   - Maintain a record keeping system that forms an audit trail from production control through payment to CBP entry.
   - Provide supporting documentation for CBP transactions in a timely manner.

10. **Partner with Customs & Border Protection** *(Information & Communication)*
    Enhance partnership by:

    - Participate in voluntary CBP programs such as: C-TPAT, CSI, ISA, FAST, ACE, etc.

Italics **(indicate the Five Components of Effective Internal Control - Attached)**

The Five Components of Effective Internal Controls

The internal control process has five components:

1. Control Environment

2. Risk Assessment

3. Internal Control Activities

4. Information and Communication

5. Monitoring

Control Environment
Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels. If management views controls as unrelated to achieving its objectives, or even worse, as an obstacle, this attitude will also be communicated. Despite policies to the contrary, employees will then view internal controls as "red tape" to be "cut through" to get the job done. An effective internal control environment:

- Sets the tone of an organization influencing the control consciousness of its people
- Is an intangible factor that is the foundation for all other components of internal control, providing discipline and structure
- Describes "organizational culture"
- Includes a commitment to hire, train, and retain qualified staff
- Encompasses both technical competence and ethical commitment

Risk Assessment
A risk is anything that endangers the achievement of an objective. Always ask:
What can go wrong? What assets do we need to protect?

- Risk assessment is the process used to identify, analyze, and manage the potential risks that could hinder or prevent an organization from achieving its objectives.
- Risk increases during a time of change, for example, turnover in personnel, rapid growth, or establishment of new services.
- Other potential high risk factors include complex programs or activities, duty liability, dependence on third party service providers, and prior problems.

Internal Control Activities
Organizations establish policies and procedures so that identified risks do not prevent the organization from reaching its objectives.

- Clearly identified activities minimize risk and enhance effectiveness.
- Internal control activities are nothing more than the policies, procedures, and organizational structure of an entity.
- Controls can be either preventive, for example, requiring supervisory approval, or detective, for example, reconciling reports.
- Avoid excessive controls, which are as harmful as excessive risk and result in increased bureaucracy and reduced productivity.

Information and Communication

To be useful, information must be reliable and it must be communicated to those who need it. For example, supervisors must communicate duties and responsibilities to the employees that report to them and employees must be able to alert management to potential problems.

- Information must be communicated both within the organization and to those outside, for example, vendors, and service providers.
- Communication must be ongoing both within and between various levels and activities of the organization.

Monitoring

After implementing internal controls, organizations must monitor their effectiveness periodically to ensure that controls continue to be adequate and continue to function properly. Management must also revisit previously identified problems to ensure that they are corrected.

- Schedule monitoring on a regular basis.
- Select a sample. Review all documentation. Visit outside sites, if appropriate. Supplement sample with special tests of sensitive and problem areas.
- Monitoring is essential to verify that controls are operating properly. Reconciliation, confirmations, and exception reports can provide this type of information.