excellence through STEWARDSHIP

GUIDE FOR

Incident Response OF Biotechnology-Derived Plant Products

DISCLAIMER

The Incident Response Guide for Biotechnology-Derived Plant Products ("Guide") is solely an educational tool and is guidance to assist users in developing and implementing their own organization-specific process for managing incidents with plant biotechnology products.

The Guide is flexible, and its application will differ according to the size, nature, and complexity of the organization and products involved. The Guide is representative and not exhaustive. It is the responsibility of any user of this Guide to consider that user's specific circumstances (1) when developing an incident-response process specific to its organization, and (2) in meeting any applicable legal requirements.

This Guide is not, and should not be used as, a substitute for (1) a user's own individual understanding of its legal requirements, (2) consultation by a user with its legal counsel and other advisors, or (3) direct contact with appropriate regulatory agencies.

The Guide does not define or create legal rights or obligations, and Excellence Through Stewardship (ETS) specifically disclaims any such rights or obligations. ETS and its members do not make any warranties or representations, either express or implied, with respect to the accuracy or completeness of the information contained in this Guide, or the sufficiency of the general procedures and processes contained herein to eliminate risk inherent in the referenced operations or processes; nor do they assume any liability of any kind whatsoever resulting from the use of or reliance upon any information, procedures, conclusions, or opinions contained in this Guide. ETS assumes no responsibility to update this Guide.

November 2008; Revised February 2019; Revised 2024

Excellence Through Stewardship 1201 New York Ave NW Suite 1300, Washington, DC 20005

CONTENTS

Introduction

This Guide is designed to provide information for the efficient management and successful resolution of incidents involving biotechnology-derived plant products. Potential incidents can occur at any stage of the product life cycle. Therefore, an organization should have processes, procedures, and resources in place to respond to potential incidents involving such products during each stage of the product life-cycle (Figure 1).

Figure 1 - Biotechnology Plant Product Lifecycle

Potential Incidents

Examples of potential incidents that may occur throughout the product life cycle could include:

- Unintended/unauthorized release of propagative plant materials into the environment;
- Unexpected/unauthorized third-party intervention (e.g., destruction or theft of material);
- Unintended harvest/shipment/sale of unauthorized material;
- Planting at unauthorized areas;
- Loss of unauthorized material during transit/shipping;
- Detection of biotechnology-derived plant materials/events where not authorized (e.g., in commercial grain flow); or Traits at unauthorized levels;
- Publishing of unexpected research study findings, scientific literature, or media coverage impacting a product/event;
- Non-compliance with regulations and/or permits.

By anticipating the types of potential incidents that may occur, an organization can prepare and establish response teams, processes, procedures, and tools specific to such types of incidents. For example, if an organization is involved in conducting confined field research trials it would be useful for the organization to have a defined process in place for reporting an unauthorized release to the relevant government authorities, when appropriate, and having reporting tools and contact lists readily available.

Importance of Incident Response Planning

Proactive planning and preparation are important to the successful resolution of an incident. When designing, developing, and implementing an incident response process and procedure, an organization should consider contingencies for incident management based on the different stages of the product life cycle. Some planning and preparation activities include:

- Process to define scope of activities involved in a potential incident (e.g., lab only vs. field release of regulated biotechnology-derived plant material);
- Proactive establishment of relationships with key stakeholders and contact list of key external stakeholders that could potentially be impacted by an incident (organization should consider establishing a primary person responsible for the line of contact to each external stakeholder group);
- Evaluation of Potential for material to enter commodity/trade channels inadvertently, and where the product may be found (one country vs. several);
- Understanding of the diverse laws and regulations in the respective countries of activity;
- Knowledge of the escalation potential of an incident from the farm level to global trade (Figure 2) and through potential media coverage of an incident.

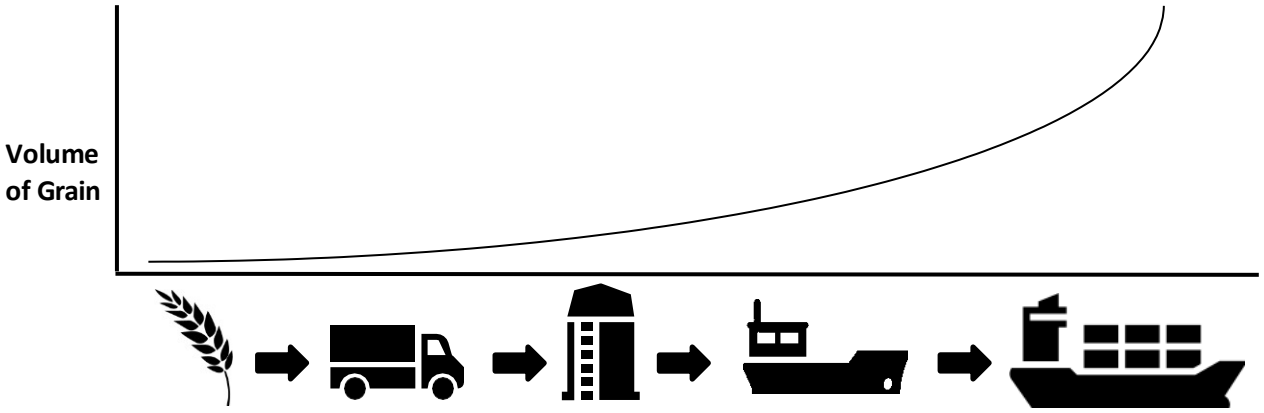


Figure 2: Escalation potential of unauthorized seed material in grain channels. Generally, the volume of grain involved tends to increase exponentially as storage and shipment progresses from farm through subsequent channels.

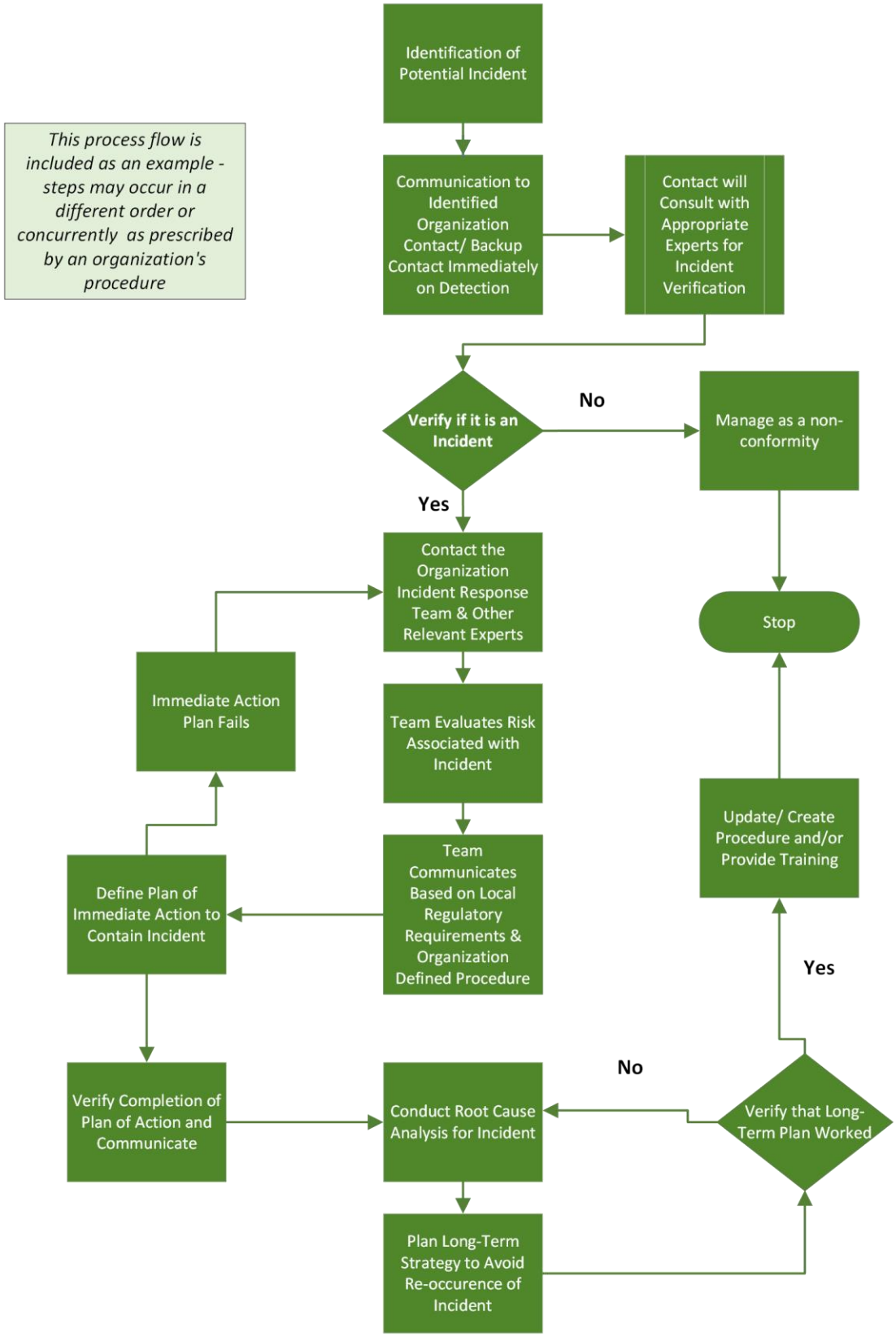
Quick action is a key element necessary to prevent escalation of incidents when grain and shipment in commodity channels are involved.

Incident Response Process

An organization should have an incident response process in place that is designed for its respective operations and activities. This includes defining and establishing:

- **Roles and accountabilities** for incident response, including response team leadership and experts:
    - Functional Experts could include: Regulatory Compliance, Legal, Seeds Stewardship, Analytics/Quality Control (QC) Testing, Stakeholder Relations, and Communication.
    - Operational Experts could be included representing functions responsible for the activities throughout the product life cycle including Research and Development, Breeding, Commercial Operations, and Supply Chain.
- **Process flow** (Figure 3) for incident response and an **escalation process** which includes response triggers that define appropriate reactions to specified types of incidents.
- **Communication networks** for dissemination of information internally and externally. This may include **stakeholder maps** to facilitate timely inclusion of key parties.
- **Documentation requirements**, as appropriate and as determined by legal counsel.
- Ongoing **training programs** that facilitate awareness of an organization's incident response processes and procedures.

Figure 3 – **Sample** Incident Response Process Flow



Elements of Incident Response Process

There are six basic elements of a typical incident response process (Figure 4). Each organization should define and implement an incident response process to meet their needs in a timely and effective manner to manage and resolve an incident. These elements may be conducted in whatever order outlined by an organization's incident response process. Note that some of these elements and associated activities may be conducted concurrently.

Quick and immediate actions within these elements may be needed to prevent further escalation of the incident.

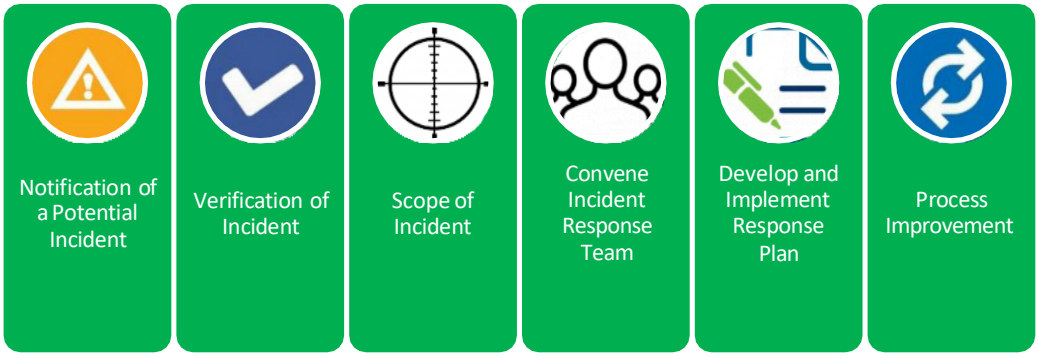


Figure 4: Basic Elements of a Typical Incident Response Process

Notification of Potential Incident

The person who initially identifies or suspects a potential incident should quickly outline the circumstances so that it can swiftly and accurately be escalated to appropriate experts and managers within the organization, and then managed according to the subsequent steps in the process. A basic potential incident response form or format should be available to collect information as appropriate and in accordance with the organization's procedures.

Potential incidents may also be identified by external sources (e.g., auditors, consultants, cooperators). As feasible, there should be response procedures established with these external sources for prompt notification of an incident to the organization. Organizational personnel should be designated and trained to react appropriately, taking information from these external sources as described below.

The list below provides examples of the information to consider collecting when notified of a potential incident:

- Name and contact information for person notifying of the potential incident and personnel receiving the notification
- Time, date, and location of potential incident
- Name and contact information of the internal and/or external people involved

- Description of incident
    - Events leading up to the potential incident
    - Type of material involved (e.g., crop, status)
    - Where is the material? Is it under your control?
    - Which step in the product life cycle
    - Any associated factors or circumstances
    - Potential indirect effects (e.g., Health, Safety, Environment)
- Immediate actions requested or taken
- Proposed next steps including who was/will be contacted within the organization (including local and global relevant experts)

This preliminary report is important to the successful management of a potential incident. It may initially be a verbal report to a supervisor or other manager.

Verification of Incident

Initial notification of a potential incident should be communicated to the appropriate internal contact(s) (e.g., Stewardship, Regulatory, Quality, Regulatory Compliance, Stakeholder Relations, and/or Legal), who should confirm whether there has been an incident that warrants escalation to an incident response team and should review the nature of the incident. For example:

- Trade Disruptions
- Loss of Confinement/Containment
- Unauthorized Release
- Vandalism
- Weather-Related Disruption

Immediate action may be needed to prevent further escalation.

At this point it is critical to verify that the information provided is factual. Note that a key decision is needed - either escalate further to an Incident Response Team or manage as a non-conformity[1] according to internal procedures. Criteria may be established in order to assist the responsible parties in making this determination. Examples of potential non-conformities rather than incidents:

- Unauthorized material spilled in a contained environment (greenhouse, lab)
- Mislabeled material in the laboratory
- Unauthorized access to a containment facility
- Equipment clean out at a confined field trial site not documented

[1] A non-conformity, or non-conformance, is the nonfulfillment of a requirement.

Scope the Incident

Once an incident has been verified, the (initial) Incident Response Team should rapidly determine the potential impact and magnitude of the incident. In addition to material related consequences, the potential regulatory implications, regulatory obligations, and liability/litigation risks should be evaluated. Considerations could include applicable government regulations, permit conditions, contracts, and legal agreements.

This is the start of what may be a long and more comprehensive process to understand the full consequences of the incident. However, this initial evaluation should be fast, extensive, and accurate, so that subsequent immediate actions are as effective as possible. This will assist in ensuring that internal and external response mechanisms can be initiated with appropriate information communicated to key stakeholders.

This initial evaluation should comprise the following details:

- Clear definition of the incident
- Initial quantification
- Determine whether actions could be taken to safely and immediately confine all material involved
- Definition of potential impacts
- Equipment and facility considerations
- Logistics and transportation considerations
- Downstream secondary and tertiary parties and activities
- Identification of potential legal requirements (e.g., reporting obligations)
- Scenario analysis of actions and consequences
- Identification of stakeholder (regulators, customers, grain trade, food chain, etc.)
- Review of relevant agreements and potential insurance coverage under applicable policies

Convene Full Incident Response Team

The response-team structure and membership will depend upon the initial evaluation of the scope, the potential impact of the incident, and the expertise needed to manage the incident. The response team leader should have the expertise, time, and resources to manage the incident in an expedient manner. Sub-teams, with local or global focus, may also be needed for major incidents so that specific external stakeholder needs are covered once agreed to by the Incident Response Team (e.g., government staff, industry trade partners, distributors, local or international media). It is important to have clarity on roles and accountabilities, as well as transparency and coordination across sub-teams.

Develop and Implement the Response Plan

Clear analysis with timely and effective response can lead to successful resolution of an incident. A dedicated response team should focus on resolving the incident. Response activities should consider the framework of stakeholder commitments, regulatory requirements, contractual obligations, and other legal requirements that may include confidentiality responsibilities. Efforts should be undertaken to maintain customer, trade, and public confidence.

Members of the Incident Response Team should develop a response plan and implement remedial actions. The response plan should identify the actions to be taken, the persons accountable for the actions, when the actions should be completed, and when the overall plan should be considered complete. The response plan will need continuous updating as new facts emerge and should be transparent as a working tool to all team members. Generally, it is most effective for one team member to own the plan, to emphasize and monitor consistency and accuracy. This person or another designated team member should monitor the ongoing resolution process.

Stakeholders should be identified and appropriately informed of an incident and any potential impacts on them. Communications should take place within the relevant regulatory and legal framework and according to the organization's procedures. Incoming questions should be adequately addressed by informed expert staff.

Process Improvement

At an appropriate phase in managing the incident, it may be necessary to conduct an internal investigation and to recommend process improvements that could be made to help reduce the likelihood of similar future incidents. This investigation can be based on the incident response plan and may be supported by a root cause analysis. Corrective actions should be reviewed for effectiveness after an appropriate time.

A review of the organization's incident response process and procedures should also occur in a timely manner following an incident. Any necessary process improvements and training should be implemented to correct identified deficiencies.

Summary

Incidents should be dealt with quickly and effectively to minimize impact on the organization and its stakeholders. Preparedness followed by directed and effective response is important to successful incident management, together with the implementation of corrective and/or improvement actions that can help reduce the likelihood of a reoccurrence. Prompt and thoughtful response actions will help to maintain strong stakeholder relations.