TABLETOP EXERCISE GUIDE
SUPPLY CHAIN INTEGRITY

Abstract

This guide is based on best practices for supply chain integrity, and provides exercise scenarios focusing on prevention, protection, mitigation, response, and recovery. The exercise framework helps exercise facilitators develop and strengthen core capabilities for ensuring supply chain integrity, including operational coordination, intelligence and information sharing, operational communications, and public information. Key questions, sample objectives, and best practices are provided along with tabletop exercise scenarios, illustrating supply chain integrity threats such as tampering, theft, embargoed materials, logistics issues, and insider threats.

Analysts' Exchange Program 2019 – Physical Trade and Supply Chain Risks

CONTENTS

HOW TO USE THIS GUIDE

Stakeholders should use this guide to design a tabletop exercise to help develop an organization's capabilities to address supply chain vulnerabilities. First, participants will need to determine their objectives for each exercise based on the focus area(s) selected, such as enhanced information sharing, development of protective measures and countermeasures, and/or identification of organizational gaps. Participants will also need to define their roles and responsibilities for the exercise, to include "players" who respond to the scenario based on existing knowledge and procedures; "facilitator(s)" to guide the discussion, keep the exercise on track, and lead the final debrief; "evaluators" to collect information and decision points in order to develop the After Action Report; and possibly "observers" who watch the exercise but do not participate in response activities.

Once roles and the objective of the training are defined, facilitators should select and customize several of the example scenarios to better fit their organization's training needs. Most find it best to prepare a slide deck or other presentation tool to present the scenarios. In this document, scenarios are organized by a specific threat then further broken down into the mission areas of protection, prevention, mitigation, response, and recovery. Facilitators should select any threat(s) and the specific mission areas that fit their needs, whether it is all five mission areas or just three. If an organization would like to focus on a specific mission area, such as mitigation, facilitators can simply use only the mitigation modules from all available threats. Facilitators should also pick several discussion questions from the below section to help guide participants during the scenario.

Prior to starting the exercise, participants should agree on ground rules at the start, designed to ensure active participation, constructive comments, open dialogue, and adherence to roles and responsibilities. Also, facilitators should communicate any assumptions needed for success such as full engagement of participants for the duration of the exercise, possible time compression in a scenario, and an assumed working knowledge of existing organizational structure, policies and procedures, and planned coordination with other organizations or agencies. It is best to communicate these rules and assumptions in advance and include them in the exercise presentation.

Following the exercise, it is important for facilitators/evaluators to debrief participants and note any area identified for improvement, gaps, or best practices to be shared throughout the organization.

BACKGROUND

The Nation's public and private sectors rely on the efficiency of supply chains for the economic productivity that sustains our way of life. Efficient supply chains must be secure from, and resilient to, a variety of threats that might disrupt them.

Members of the 2019 Public-Private Analytic Exchange Program (AEP) Physical Trade and Supply Chain Risks team examined best practices to improve supply chain integrity. The extensive web of supply chains that make up the global network form a complex matrix connecting suppliers of raw materials or component parts to manufacturers or processors who in turn distribute products to wholesalers, retailers, and consumers. Stakeholders engaged in moving vital global supply chains serving the Nation, including food, pharmaceuticals, and IT supply chains, can use this guide, or personalize its content, to meet their specific exercise needs.

EXERCISE PURPOSE AND SCOPE

Use the text below to develop the exercise purpose and scope, which should be communicated to participants before the start of the exercise:

> "The purpose of this exercise is to identify and confirm roles and responsibilities to establish effective communication and information sharing practices internally within [organization] and externally among partnering agencies, as well as support on-scene operational coordination. It is a [one-day] exercise with [senior-level participants and operators]."

MISSION AREAS

Depending on the goals of the exercise planning team, the team should select different mission areas for the exercise. This guide contains scenarios designed to help bolster the following mission areas:

- Prevention
- Protection
- Mitigation
- Response
- Recovery

CAPABILITIES

Below are several core capabilities important to ensuring supply chain integrity. Organizers should select one or two areas to focus on during the tabletop exercise.

- Operational Coordination
- Intelligence and Information Sharing
- Operational Communications
- Public Information and Warning

OBJECTIVES

Facilitators should select objectives based on the goals of the supply chain stakeholder(s) participating in the exercise. The following objectives build on the core capabilities listed above:

1. Discuss existing protocols, procedures, and systems that govern the horizontal and vertical flow of information between all partners, including Federal, State, local agencies, private sector, and the public.

2. Exercise [stakeholder(s)] roles and responsibilities for receipt and dissemination of information internally, and between all partners, including Federal, State, local agencies, and private sector.

3. Identify and discuss establishment of high-level special event/on-scene incident command roles and responsibilities.

4. Discuss incorporation of [stakeholder(s)] into special event/on-scene response organization, including identification of roles and responsibilities to support multi-agency/organization response priorities.

5. Evaluate procedures and systems, including technical systems, that support internal and external communication among the incident command structure and between incident command, local Emergency Operations Centers (EOCs), and the Multi-Agency Coordination Center (MACC).

DISCUSSION QUESTIONS

Exercise facilitators should select several of the below questions to help guide discussion during the tabletop exercise. Please feel free to adapt them to fit your organization better.

1. What communication plans are in place to ensure various internal departments and external partners effectively disseminate intelligence and information amongst themselves?

2. What procedures are in place in order to maintain order and safety at the various [supply chain locations]?

    a. What additional procedures or protective measures could [supply chain stakeholder(s)] implement?

    b. How will these measures be initiated and communicated to [various stakeholder(s)' departments] and external partners?

3. What policies are in place to determine information sharing processes with supply chain operators, and to what degree (e.g., Classified, SSI, Business Confidential, etc.)?

4. What Federal and State authorities are in place to support [supply chain stakeholder(s)] integrity?

5. Are additional protective measures necessary in response to the report of [suspicious/hazardous/ criminal/terrorist] activity in the city?

    a. If so, what are some of the measures/capabilities, and how will [stakeholder(s)] communicate these measures to coordinate with external partners?

6. At this phase, how is/are [stakeholder(s)] disseminating public information?

7. How do the EOC and/or MACC receive and process information from the field?

    a. Are there tools or checklists in place to help obtain clear and concise information from the field?

8. Discuss plans/procedures to guide how system-wide protective measures should escalate based on evolving threat information.

    a. Which [supply chain stakeholder(s) positions] are involved in determining security posture in response to the threat information?

9. What messages is/are [stakeholder(s)] disseminating to the public? To operating personnel? Other employees? Customers?

10. Who is responsible for the messaging?

11. What agencies or vendors will [stakeholder(s)] need to notify and pull into the response?

12. Discuss the decision-making process, including plans, authorities, and triggers regarding system shutdown, shelter-in-place, and other appropriate actions to address public safety.

13. Discuss establishment of on-scene incident command structure.

    a. Is a unified command structure set up?

    b. What agencies would take lead authority?

    c. Where is the Incident Command Post (ICP) located? Staging area?

14. What resources can your [organization/agency] provide to assist in response to this incident, in the real world, today? Consider the actual resources and manpower capabilities that are currently present, not just a list of resources maintained or anticipated to have in the future.

    a. What resources does/do [stakeholder(s)] need from other [agencies/ organizations]?

15. What plans, policies, and procedures address communication internally, externally, and with the public?

16. What procedures exist for increasing additional preventive measures throughout the [transportation system] as the threat elevates?

17. What critical infrastructure considerations guide security and mitigation measures throughout the supply chain system? How are system components prioritized regarding protective measures?

18. What mitigation measures are in place within the [supply chain system] to ensure public safety after the event has de-escalated?

    a. What procedures exist for determining the safety and security of the system post-event?

19. What plans, policies, and procedures guide Federal, State, and local agencies and private sector roles and responsibilities?

20. What organizations have responsibility for processing and sharing the witness report with surveillance footage? Protection and processing of a crime scene?

    a. What are the capabilities of partner [agencies/organizations] to support this?

21. What procedures exist to maximize use and potential of existing video surveillance mitigation measures in place?

22. Discuss the process for sharing information, on-going response priorities, and resources needs between the field and EOCs/MACC to support Incident Action Planning for the next operational period.

a. What is required to ensure coordination and documentation of multi-agency interdependencies and priorities?

b. How will the incident transition from operational (rescue/recovery) to investigative?

c. Who is responsible for making the transition decision?

d. What roles do specific agencies play as the transition occurs?

23. Will the public information structure transition at this phase?

a. Discuss continued coordination of public information and warning messages.

EXAMPLE SCENARIOS

THREAT	INSIDER THREAT / CONSPIRACY
	Mission Area:
Prevention	Joint Intelligence Bulletin Issued: U.S. Customs and Border Protection (CBP) has issued an alert to Customs Trade Partnership Against Terrorism (CTPAT) - certified companies reporting on insider threats from shippers in [Mexico]. Narcotics including marijuana and fentanyl are being added to legitimate ground shipments from [Mexico] to the United States. Insider information on the source and destination of shipments is enabling traffickers to add narcotics to legitimate ground shipments. Key Best Practices Covered[1]: 1.2; 4.1; 5.1
Protection	CBP Alert: The shipping department at [your company] was informed of the CBP alert and instructed to take extra care in the loading and sealing of trucks and trailers bound for the United States. Due to high volumes of shipments, some trailers are being brokered from unknown sources in [Mexico]. The integrity of these containers is suspect. Key Best Practices Covered: 1.2; 2.3; 3.2
Mitigation	Seizure of shipment by U.S. Customs at the Southern border: The Corporate Security office of [your company] receives a call from CBP CTPAT Security specialist informing them that one of their shipments has been seized at the border crossing. The trailer contains a false compartment that contains a large quantity of marijuana. Key Best Practices Covered: 1.3; 4.2
Response	The seized shipment was carrying critical components, and has resulted in production delays. [Your company] tracks new shipments of critical components from loading and sealing through to delivery, resulting in substantial added cost and effort. Key Best Practices Covered: 1.3; 2.5
Recovery	The Corporate Security office of [your company] updates policy and procedures on sourcing and internal inspection during loading and sealing in order to

[1] Refer to numbered Best Practices list at end of document

prevent unlawful access to cargo during shipment. As part of the policy and procedure development, [your company] identifies practices for safeguarding sensitive information along with consequences for violations. [Your company] ensures that personnel are properly trained to conduct their insider threat program duties. A screening process for shipping contractors is also implemented.

Key Best Practices Covered: 1.1; 3.1; 3.2; 3.3; 3.4

THREAT — LOGISTICS/WAREHOUSING ISSUE

Mission Area:

Prevention

Industry groups issue checklist to review contingency plans:

Prior to storm season, the Federal Emergency Management Agency (FEMA), along with industry groups, issue a checklist to help warehouse managers review contingency plans for temperature sensitive storage. The checklist includes information on how to assess sites and identify key vulnerabilities such as power sources and suggests acquiring secondary sources such as generators.

Key Best Practices Covered: 1.2; 1.3

Protection

Vulnerability assessment conducted:

In response, [pharmaceutical company] conducts assessments on their sites and identifies five that appear to be most vulnerable. At least two sites store temperature sensitive material.

Key Best Practices Covered: 1.3; 4.2

Mitigation

Because it handles temperature sensitive inventory, and in response to previous vulnerability assessments, [pharmaceutical company] has acquired back-up generators for temporary power when the power goes out. The mitigation plan accounts for fueling sources for the temporary power and identification of these locations to local emergency managers so that access can be incorporated into appropriate route clearance plans.

In [month], a senior U.S. Army Corps of Engineer official, when asked about what was being done about the increased storm threats to power infrastructure, stated the emergency management community is urging all commercial and public components to register their critical infrastructure requirements with the local emergency management staff to better understand the immediate power needs post-event – such as medical facilities, nursing homes and shelters, plus commercial requirements.

	In [month], a trade association publishes a report that identifies best practices for community resilience involving critical power requirements relating to receiving timely information about community power restoration following disaster events, assessing situations, and reporting accurate information relating to supply chain resilience. Key Best Practices Covered: 1.2; 1.3
Response	A major storm has wiped out power to operations and storage facilities. Once the power goes out, response time is of the essence to maintain the integrity of operations, which depends on refrigeration and physical monitoring of sensitive inventory. Emergency response coordinators are called in to oversee response efforts, including operation of backup generators and continuous temperature monitoring. Medical facilities with pending or outstanding orders are briefed on status of product and response efforts, and timelines for delivery are adjusted based on response timeline. Facilities and providers depending on vaccines are notified to reach out to secondary sources in the interim. Key Best Practices Covered: 1.3; 4.2; 5.1
Recovery	The storm threatened integrity of [product name], specimens, and other components in inventory. Recovery includes some disruption to production and delay of shipments in order to divert staff to ensuring integrity of product. Existing inventory and component materials are checked for quality and efficacy, and compromised inventory is discarded. Damaged inventory is recorded and accounted for in response and recovery records. Management is briefed on status of products and lessons learned from response efforts. Procedures are adjusted based on data obtained from recovery efforts. Reserves of specimens and other components are replenished in preparation for other unforeseen events. Key Best Practices Covered:1.3; 2.5; 5.1

THREAT	THEFT OF CRITICAL/VALUABLE ITEMS IN TRANSIT *Mission Area:*
Prevention	The FBI has issued an alert about an increase in the theft of [product type] by organized criminal groups. The thefts happen after the shipments arrive at the port/airport and are placed on trucks. [Product type] seems to be specifically targeted, as thefts of other items from the same ports has not increased. There is a belief that these shipments are being specifically targeted for theft, as multiple companies have reported losses. Key Best Practices Covered: 1.2; 3.2; 3.3; 3.4; 4.1; 4.2; 5.2

Protection	A week later, [Industry Group] issues an alert indicating an increase in suspicious behavior along the East coast where trucks have been tailed after leaving gas stations along [major highway]. Key Best Practices Covered: 1.2; 3.4
Mitigation	Your operations center begins to get reports of unknown individuals loitering around trucks. Additionally, at least one truck cab has been broken into in the past week. There have been no reported thefts at this time, but drivers carrying this product have reported seeing unknown individuals loitering in the area when they stopped for gas. Several have also been approached and questioned about who they work for and what they are currently hauling. Key Best Practices Covered: 3.3; 3.4; 4.1
Response	After analyzing your own operations, you notice that there have been dozens of shipments of [product type] stolen over the past quarter. After inspecting one of the trucks carrying [product type], you find an unauthorized GPS tracking device on the shipment. It is unknown when the devices were attached, although it may be connected to the recent increase of cargo thefts. Given the scale, it could impact the delivery of the product for [key customer]'s shipment. Key Best Practices Covered: 4.1; 4.2; 5.1; 5.2
Recovery	Several months after the first unauthorized tracking device was found, a senior leader in your company hears that [competitor company] has been targeted by a similar theft ring. Knowing about the previous incident, the senior leader asks what steps have been taken to provide an early indication that shipments are going missing. Key Best Practices Covered: 5.1; 5.2

THREAT — SUBSTANDARD QUALITY INPUTS

Mission Area:

Prevention	DHS issues a report warning of an increasing trend of incidents involving overseas suppliers of critical raw material forging quality records. Market volatility, civil unrest, along with repeated mining disruptions in [Congo], the report says, have caused unanticipated short supplies and high prices of [critical material]. As a result, more raw material suppliers are delivering substitute materials to the United States. If this situation continues, it may create security vulnerabilities for the U.S. industrial base.

	In [month], an industry trade association issues a report that identifies best practices for critical manufacturers related to receiving timely information about evolving threats, assessing situations, and reporting accurate information relating to supply chain integrity. Access to this information could allow U.S. critical manufacturers and their supply chains to proactively prepare for or mitigate risks. Key Best Practices Covered: 1.2; 2.1
Protection	In [month], a senior DHS official, when asked what is being done about the increased threat, states advanced, rules-based information technologies and policies applied in CBP programs help to identify higher risk shipments and to make admissibility decisions prior to the arrival of the goods in U.S. ports. Through risk segmentation methods, shipments may be considered lower-risk, and CBP is able to focus on inspection of higher-risk shipments. Despite CBP's programs, rebel leaders in [Congo] who now control much of the world's supply of [critical material] issue a statement taking credit for controlling the natural resources and sending inferior material to the West. Similarly to previous messages released, they encourage their raw material suppliers to "keep the best material home" and ship lower quality material abroad. Key Best Practices Covered: 1.2; 5.1
Mitigation	In response to the warnings issued regarding an increase in forged quality records and substandard materials, a senior leader at the company calls a meeting with the supply chain management team. The senior executive has indicated that he would like to hear from the team what measures are being taken by the company to address this risk and what are possible additional steps which could be taken to increase the chances of identifying substandard materials coming into the company, and what additional resources would be needed to take these steps. Key Best Practices Covered: 1.1; 1.3; 2.1; 2.2; 5.1
Response	In [month] the company receives a demonstrable increase in quality issues regarding a flagship product. In one week, the internal quality assurance function is able to determine that product defects are linked to [material] provided by [vendor name] although vendor-provided quality records show materials to be within specification. This vendor has been a trusted supplier of [material] for many years without prior issues and supplies 67% of the material for the company. Quality tests of the questioned material will take approximately 3 additional days to complete. On a cable financial news segment, quality issues with [product name] are mentioned leading to a 10% decline in the company's stock price, wiping out most year-to-date gains.

After 3 days of testing it is found that the received [material] does not meet specifications and that the findings are not consistent with the quality test results provided by [vendor]. [Vendor] has no explanation for the discrepancy, and the quality issues appear to be limited to materials provided by this vendor. The relationship between your company and [vendor] are strained.

Key Best Practices Covered: 2.2; 2.3; 2.4; 2.5

Two months after the reported quality issue, it was learned by your procurement analyst that [vendor] had been acquired by a large consolidator [big company name] approximately eight months ago. Since the acquisition, [vendor] has been operating under its former name although the change of ownership has led to numerous changes in operational policy and process. Also changed was much of the management team and many of the suppliers.

Recovery

The product quality problem has led to a general decline in sales of [product name], and other related products due to damage to brand image. The stock price has also failed to recover and hovers around 10% less than what it was prior to the product quality issue.

Other suppliers have offered to meet the demand for [material] at comparable prices.

Key Best Practices Covered: 1.2; 2.2; 2.3; 2.5

THREAT

KEY MATERIALS COME FROM EMBARGOED COUNTRY

Mission Area:

Prevention

Federal agencies such as Treasury, Commerce, and State maintain several lists to assist agencies and firms in navigating the many trade-sanctioned persons and organizations. Firms can check their suppliers against these lists, and require their suppliers to disclose whether they have business with listed persons or organizations.

Key Best Practices Covered: 2.1; 2.2; 2.3; 2.5

Protection

Firms may require suppliers to undergo a screening process and provide information on their supply chain operations in order to determine the risk that items from trade-sanctioned persons and organizations may be provided. For those instances in which a critical product or service can only be obtained from a listed person or organization, a waiver process must be followed and documented.

Key Best Practices Covered: 1.2; 2.5

In [month], an industry trade association meets to highlight that supporting supply chain operations are extremely multifaceted and require a complete mapping to include 2nd and 3rd tier suppliers. Best practice indicates the first place to start is understanding your supply chain routing beyond primary suppliers. Increasingly, complex industries have been setting the requirement for firms to engage in mapping exercises which seek to understand primary suppliers' ownership structures and supply chains.

Mitigation

In [month], an industry trade association issues a report that identifies best practices for critical manufacturers which recommends ownership database tools that are good options for threat identification. The industry trade association provides extensive detail on a wide range of firms worldwide. The data is organized in a format which should simplify assessment. An initial indicator might be if your suppliers are sourcing from comprehensively sanctioned countries, namely [Iran, Syria, Cuba, North Korea, and the Crimea region]. Industry participants are directed to check their supply chain participants at the primary level, which could be subject to sanctions themselves. Failing to properly vet participants can lead to subsequent vulnerabilities.

Key Best Practices Covered: 2.5

Response

In [month], international labor rights group Do-Gooders Unite publishes a lengthy report alleging [company name] and several other competitors in the [industry] buy components from Best Components, Inc. which is owned by [Conglomerate], a company sanctioned by the U.S. Treasury. There are additional reports that in many of [Conglomerate]'s factories, workers are underage and receive substandard wages. Later that month, there are additional allegations that another charity had brought concerns about Best Components, Inc. to [company name]'s attention several years ago.

Best Components is a key supplier for a newly launched product line which is selling well. There have been no reported quality issues with the new product line or any other existing products that are made with Best Components parts. Immediately following the report's publication, several hundred Twitter users have begun calling for a boycott of all companies named by Do-Gooders Unite.

Key Best Practices Covered: 1.2; 1.3; 2.2; 5.1

Recovery

Three months later, after several protests at [company name] offices, Do-Gooders Unite begin a campaign calling for [company] to make public more information about the steps they are taking to ensure their suppliers are following safe and fair labor practices, as the group is not satisfied with the company's response thus far.

Do-Gooders' initial campaign caused a 10% drop in sales during peak times, and a build-up of inventory as new goods continue to be produced.

Key Best Practices Covered: 1.1; 1.3

THREAT MALICIOUS TAMPERING

Mission Area:

The FBI has issued a Joint Intelligence Bulletin to the U.S. private sector about Operation Anvil Ranger – a joint initiative with DHS that targets the illegal distribution of counterfeit components, including computer chips, manufactured by private entities in China. The use of counterfeit components can lead to exploitation of [devices], including unwitting surveillance. The FBI says [China] desires to conduct economic espionage on an industrial scale.

Prevention

A senior DHS official warns malware could be embedded on the chips to exfiltrate information from [devices] and result in the theft of personally identifiable information (PII) and economic data that could then be used in future cyber crimes. As the quality of counterfeit goods increases, U.S. suppliers may be challenged to tell the difference between authentic and fraudulent [components].

Key Best Practices Covered: 2.1; 2.2

Alert regarding tampered computer chips sent to private sector:

In [month], a senior FBI official, when asked about what was being done about the increased threat, stated the FBI has seized over 8,500 [components] amounting to $150 million of retail products. Ten individuals employed at Silicon Wafer Ltd, a manufacturing company in [China], have been arrested as a result of the joint initiative. FBI says this may only be the tip of the iceberg as components produced by Silicon Wafer Ltd are used in billions of devices.

Protection

Authorities from [China]'s Foreign Ministry release a statement responding to the U.S. arrests. Production at Silicon Wafer Ltd and other facilities will increase substantially by the end of the month, the statement says and [China] will not be intimidated into reducing manufacturing activity within its borders. The statement announces [China]'s desire to ramp up production to be the top producer in the world of [computer chips] by the end of the year.

In response to the statement from [China], the FBI alerts U.S. private sector partners on the Domestic Security Alliance Council (DSAC) about [China]'s provocative statement. The FBI says it wants to promote effective exchanges of information in order to prevent, detect, and investigate criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information.

	Key Best Practices Covered: 1.2; 1.3; 2.1
Mitigation	A new story identifies some [competitor company] products have been sold containing counterfeit chips dating back a year. The competitor company has issued some product recalls to remove affected product from the market. The nature and extent to which the counterfeit chips affect the product is unknown. The news story describes the potential that such counterfeits be introduced into the market to open the door for industrial espionage. Key Best Practices Covered: 2.2
Response	Tampered components identified in supply chain: [Consumer electronics company] identifies that one of its [devices] contains components tracing back to Silicon Wafer Ltd. It is estimated that these components are found within 120,000 such devices already in the hands of consumers, with another 25,000 on retail shelves. There is no conclusive evidence to show that the components contained within [consumer electronics company]'s product are or are not compromised. Moreover, it is likely that news of the company having Silicon Wafer Ltd. as a supplier will surface prior to establishment of such conclusive evidence. The company must determine next steps and time is critical. Key Best Practices Covered: 1.3; 2.2; 4.2
Recovery	Three months have elapsed since [consumer electronics company] first identified the threat posed by components sourced from Silicon Wafer Ltd. The company responded by issuing a recall of compromised product and has now recovered 80,000 devices from consumers along with 24,000 from retailers via recall. Approximately 41,000 potentially compromised devices are not accounted for. Moreover, the company must determine how to appropriately disposition recalled items. Key Best Practices Covered: 4.2

BEST PRACTICES RELATED TO ADDRESSING SUPPLY CHAIN INTEGRITY RISK

1. Identify network of subject matter experts to ensure dissemination of timely risk information and robust supply chain security measures are implemented throughout end-to-end (e2e) supply chain
    - 1.1 Internal resources including leadership to drive desired actions
    - 1.2 Identification of external resources (government, industry associations, and consultants) to provide timely intelligence and response support in the event of an emergency.
    - 1.3 Advance coordination and planning including table-top scenarios can confirm key stakeholders, roles and responsibilities.

2. Supply Chain Management
    - 2.1 Must be e2e focus that includes continual monitoring of supply chain risks and implementing actions to mitigate.
    - 2.2 As with employees, suppliers must be thoroughly vetted. (media monitoring, on-site review/inspection, use of analytics, financial health, alternate locations/sources)
    - 2.3 For outsourced portions of supply chain, security requirements must be incorporated into supplier contracts/SOWs AND (quality) inspections performed to verify continued compliance.
    - 2.4 Certifications can be effective where there is sufficient rigor, monitoring and testing to confirm continued compliance; ISO 9001 is a good start.
    - 2.5 E2e mapping of supply chain to enable targeted risk assessment

3. Insider threats /Personnel Security
    - 3.1 C-level suite commitment “Tone at the Top”. Importance of Risk management as part of the company culture
    - 3.2 Robust vetting of personnel – initial hiring, when assigned new responsibility, and periodic when in sensitive position/high risk environment
    - 3.3 Employer and supplier personnel standards of conduct
    - 3.4 Implement robust awareness and training programs to enable supply chain personnel to recognize risk and report suspicious activity and incidents

4. Cyber Security
    - 4.1 Implementation of robust security measures including access controls and network monitoring.

4.2 Physical shipments – GPS on vehicles, shipments and integrated with other data collection inputs, ...

5. Supply Chain monitoring

5.1 Risk based monitoring enables focus and additional oversight on critical aspects of the supply chain

5.2 Utilize technologies including AI, Integrated GPS, analytics and Blockchain to monitor supply chain for (integrity) risk