International Organization for Standardization

Using Standards to Cost-Effectively Manage Risk

Steve O'Malley - ISO Ship & Supply Chain Security Standards Coordinator

Motivators*

- Fear
- Guilt
- Government regulation
  - Or, no choice but to do it!
- Greed – or return on investment

*RADM Norm Saunders

Motivators*

- Fear
- Guilt
- Government regulation
  - Or, no choice but to do it!
- Greed – or return on investment

IT'S ABOUT THE MONEY!

*RADM Norm Saunders

In overall risk management you cannot separate safety and security

Hindi

- सुरक्षा Safety
- सुरक्षा Security

Chinese

- 安全 Safety
- 安全 Security

Japanese

- 安全な Safe
- 安全な Secure

English

1. Freedom from risk or danger; safety.

Nor can you separate out Resiliency

Resilience: the adaptive capacity of an organization in a complex and changing environment [ISO Guide 73:2009]

- NOTE 1 Resilience is the ability of an organization to prevent or resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.

- NOTE 2 Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.

DHS defines resiliency as the ability to resist, absorb, recover from, or successfully adapt to adversity or changing conditions

BSI discusses Business Continuity, and describes processes to help businesses develop resilience and recovery strategies during challenging and exceptional circumstances

High probability of supply chain disruption from low probability threats

Ladder54.com

There's a 100 percent chance of an earthquake today. Though millions of persons may never experience an earthquake, they are very common occurrences on this planet. So today -- somewhere -- an earthquake will occur.

U.S. Department of the Interior | U.S. Geological Survey

Worldwide, each year there are about 18 earthquakes magnitude (M) 7.0 or larger.

Government Resiliency may differ from Corporate Resiliency

End goals:

- National Survival/Recovery- may include triaging - prioritization

- Corporate profitability and survival

The making of a resilient supply chain

- Redundancy (limited)
- Flexibility
- **Corporate Culture**

*Yossi Sheffi, MIT

Corporate Culture

- Continuous communications among informed workers*– (supply chain visibility, you cannot manage what you cannot see or measure)
- Distributed power to act*-- (authority and willingness)
- Passion for work*– (sees the Mega)
- Conditioned for disruption*

*Yossi Sheffi, MIT

How do international industry standards help?

- Supply Chains are international, so you need internationally accepted/understood tools
- They help establish a common understanding of expected performance
- Allow for easier substitution
- To a certain degree, conformity determination can be made by qualified 3rd parties and those costs may not be directly passed on to you

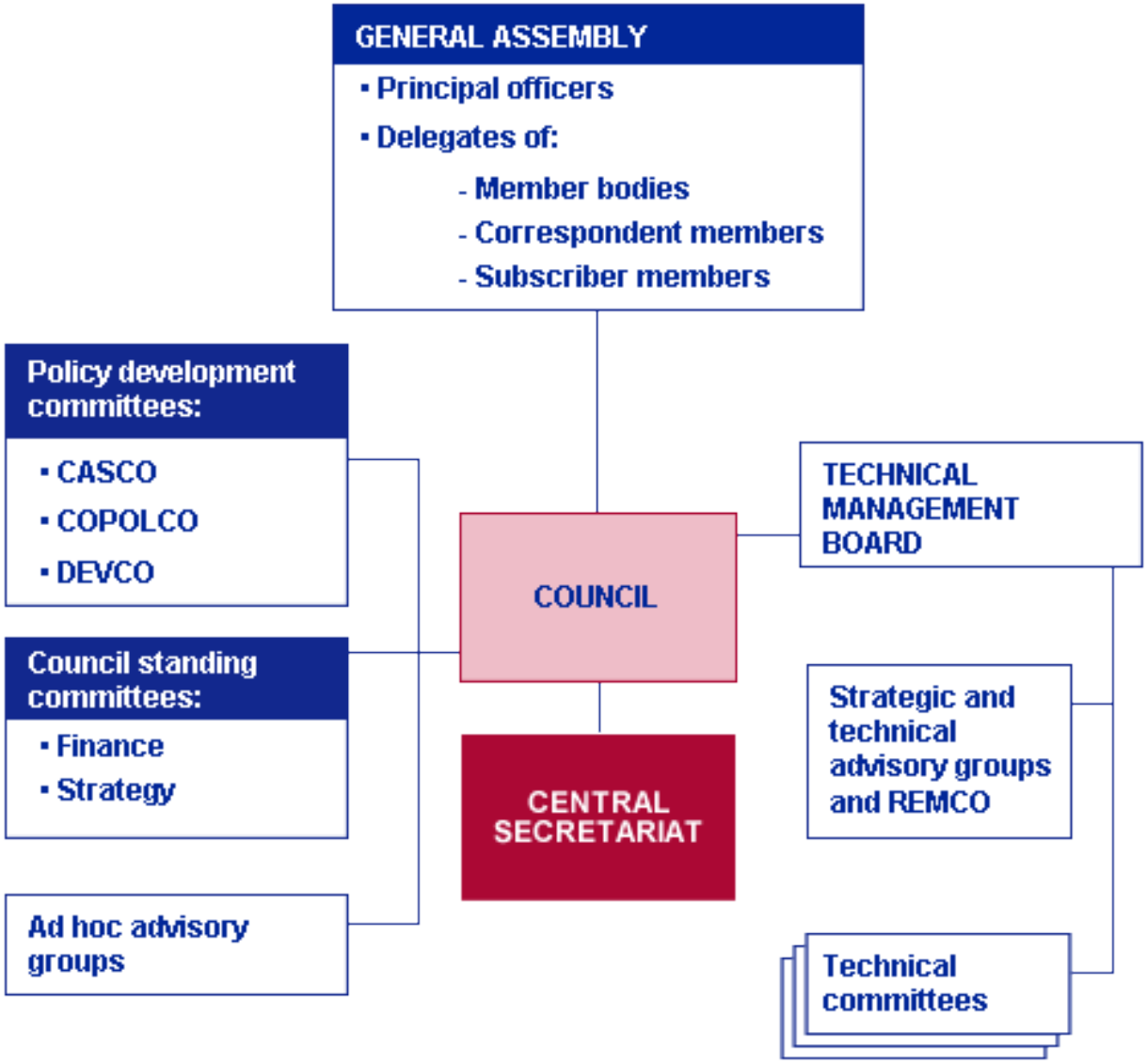
A quick overview of standards

- Types of standards-
  - Management Standards
  - Technical Standards
- Types of requirements
  - Prescriptive
  - Performance based
- Conformity
  - 1st party
  - 2nd party
  - 3rd party

Where do standards come from?

- International Standards- primarily the International Standardization Organization (ISO), International Electrotechnical Commission (IEC), and International Telecommunications Union (ITU)
- National Standards- governing body in U.S. is ANSI
- Foreign Standards- examples are BSI and CEN
- Industry specific organizations- examples are TAPA, IATA, ASIS, and others

ANSI represents the U.S. at the ISO



Two type of standards:

1. Prescriptive standards result in the measuring of things

- Height of fences
- Levels of illumination
- Size of openings
- Etc

Writer of the standard has predetermined what is adequate.

Two type of standards:

2. Performance standards require processes be developed

Within limits, the organization adopting the standard determines what is needed to meet set performance requirements based on an assessment

Better standards include the requirement to establish feed-back loops and for the user to continually assess progress and make adjustments as needed

Factors in selecting a standard

In regard to security and resilience

- What are your organization's goals?
- What are your customers' expectations of your performance?
- What are your business partners' expectations of your performance?
- What is expected of your organization by the courts and regulators?

Factors in selection of a standard

- Does the user see added value in adopting that standard
- Is it compatible with the user's industry partners
- If certification is desired, are their adequate accredited auditors available at normal rates
- Will the standard be recognized as adding value by the customers

Note: Not all users of standards seek certification

Management Standards – Truth in advertizing

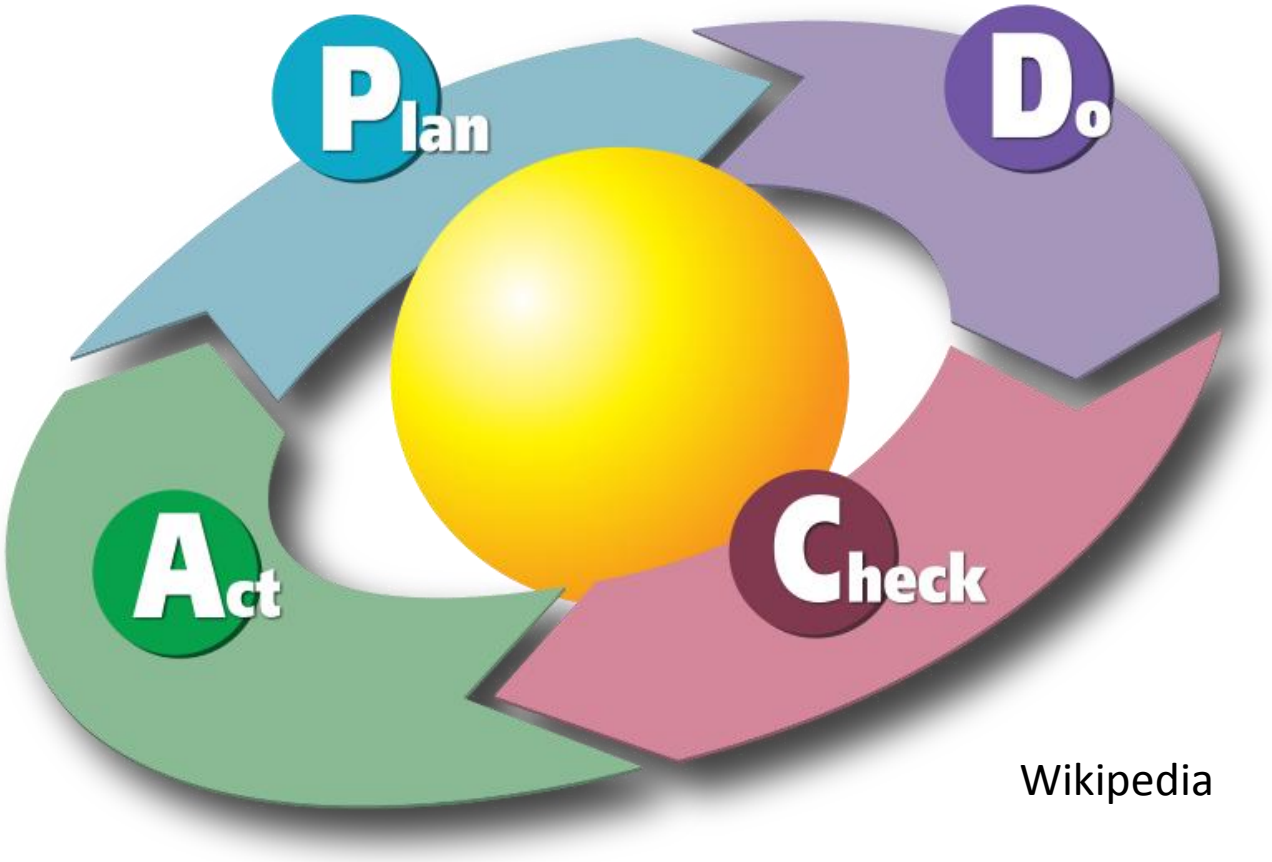
- The organization has the processes and equipment to deliver what they state in their corporate policy statements (corporate objectives)

- Better known ISO Management Standards include: ISO 9001 (Quality Management), ISO 14001 (Environmental management), and ISO 28000 (Security Management System for the Supply Chain)

ISO 28000

- Supply Chain Management Standard
  - Resiliency
  - Supply chain security (used in support of C-TPAT, Authorized Economic Programs, TAPA and others)
- The only certifiable standard (using accredited auditors)

Management is a process not a stationary target



Wikipedia

Corporate policy or objectives can include commitments to meet requirements contained in technical specifications, guides or regulations

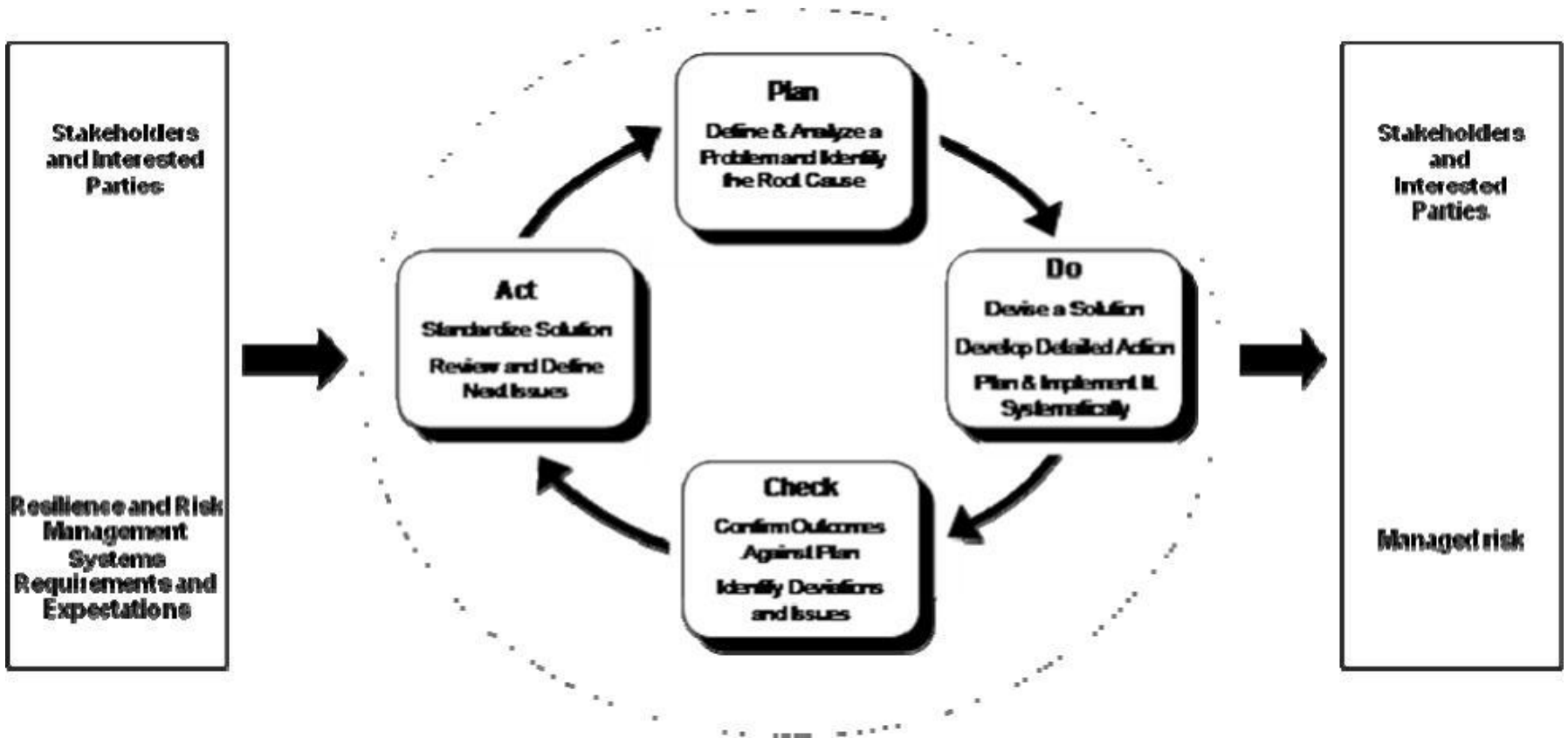
- ISO 28001 Security management systems for the supply chain -- Best practices for implementing supply chain security, assessments and plans -- Requirements and guidance
- ISO 28002 Security management systems for the supply chain - Development of resilience in the supply chain - Requirements with guidance for use
- ISO 28005 security management systems for the supply chain - Electronic port clearance (EPC) – Data Dictionary
- ISO 20585 Ships and marine technology -- Maritime port facility security assessments and security plan development
- ISO 31000:2009, Risk management – Principles and guidelines, and ISO Guide 73:2009, Risk management vocabulary

This allows for a modular approach

- Adopt a management system
- Development/identify management objectives that will add value
- Determine if 3rd party certification is an objective in the short or long term, or not at all

International Organization for Standardization

Management For Resiliency



Resiliency

- Prevent, detect/mitigate, and recover
- Supply chains are generally more complex than their operators realize
- There are aspects of your supply chain that are outside your span of control
- Resiliency requires taking a more holistic approach (discreet evaluations of site specific risks using likelihood and consequence can lead to misleading conclusions)

Risks, transnational, foreign, domestic

- Political intervention or instability
- Criminal (theft, smuggling, tampering)-(terrorism, turf battles, intimidation)
- Labor disruptions
- Business disruptions (suppliers, service providers, financial, business partners)
- Infrastructure failure (gas/electric/water, communication/Internet, transportation)
- Natural (earthquakes, storms, tsunamis, etc)
- Accidents, fires, disease
- Faulty designs/production/handling

Measures

Housed within an effective management system and based on threat assessments:

- Harden the supply chain to the extent feasible, considering; threats, economics, sphere of influence or control, cost benefits
- Improve system transparency/visibility (track, detect, react)
- Develop some limited redundancy & lots of alternative/contingency plans

Determining Conformity

- ISO 28003- Requirements for bodies providing audit and certification of supply chain security management systems

- ISO 28004- Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems

Additional guidance

- ISO 28004 now has two specialized addendums (third is in route):
  - Additional guidance for small and medium sized ports adopting ISO 28000 (approved)
  - *Additional guidance for small and mediums sized enterprises adopting ISO 28000 (being balloted)*
  - Additional guidance for organizations that which to include the requirements of ISO 28001 (security requirements for Authorized Economic Operators) as an organizational objective (approved)

Auditing

- A first party audit is the self determination of conformance by the organization itself
- A second party audit is the determination or verification of an organization's conformance to agreed criteria by another organization, agency or body which has a vested interest in the organization's operations in the supply chain
- A third party audit is a determination or verification of conformance to agreed criteria by an organization independent of all parties
- Validation and certification by government or government agency

Accredited 3rd Party

- If demonstration of compliance is sought through the third party audit process then the organization seeking certification should consider selecting a third party certification body accredited by a competent accreditation body, such as those which are members of the International Accreditation Forum Inc. (IAF) and subject to the IAF Multilateral Recognition Arrangement (MLA)

International Organization for Standardization

The Role & Objectives of IAF

The primary objective of the IAF is to develop a single, worldwide program of conformity assessment, which reduces risk for business and end users by ensuring that accredited certificates and certifications may be relied upon.

(In the United States)

ANAB is a signatory of the International Accreditation Forum (IAF) multilateral recognition arrangements for quality management systems and environmental management systems.

ANAB accredits ISO/IEC 17021 certification bodies for numerous standards including:

- ISO 9001 quality management systems
- ISO/IEC 27001 information security management systems
- ISO 22000 food safety management systems
- **ISO 28000 supply chain security management systems**
- ISO/IEC 20000-1 information technology service management systems
- ASIS SPC.1, BS 25999-2, and NFPA 16000 Private Sector Preparedness Voluntary Certification

Accredited certification bodies

Is the certification body operating under its accreditation?

- Certification bodies that are accredited by an IAF member organization may also conduct audits and issue certifications of compliance with specialized industry programs or standards that they are not accredited to certify by their accreditation body. If they are operating under their accreditation body the seal/trademark of that body will appear on the certificate of compliance – 2 such examples

Making standards work for you if you are the customer or the government

- Know what management objectives/policies that should be included
- Select standards that are readily available and can be used by all the business partners
- Determine what certifications/declarations of conformity that will be acceptable
- [If you are the government] Determine where standards can be used to meet government needs and where government needs to go it alone.

How 28000 is being used

World Customs Organization (WCO)

SAFE Framework

European Commission Authorized Economic Operator*

Customs Trade Partnership Against Terrorism

(C-TPAT)*

Singapore Secure Trade Partnership

(STP)*

Transported Assets Protection Association (TAPA)*

ISO 28000

Using ISO 28000 to manage Customs Requirements

ISO 28000 can be used to certify the AEO security requirements specified by the WCO. Although the validation of compliance remains the responsibility of the National Customs Departments, LRQA can certify ISO 28000 with the following SCOPE; **THE SCOPE of certification would read; XYZ (Activity, Location, limitations, etc) … consistent with the requirements of ABC Customs Department AEO program (Or title of program. e.g. STP)**

With this approach, certification for ISO 28000, with the above scope, establishes the internationally consistent element that all countries are looking for to progress on Mutual Recognition

Some ISO 28000 Users

- **YCH Group** the first end-to-end Supply Chain Management provider received the ISO 28000: 2007 Certification.

- **DP World was first to certify a marine terminal** and will complete ISO 28000 certifications throughout its network of 48 terminals in 31 countries worldwide by 2012. DP World is the only global marine terminal operator to have achieved simultaneous ISO 28000 certification and C-TPAT membership. Its European terminals were certified as Approved Economic Operator (AEO) by the European Union.

- **TNT Express**' Asia regional head office in Singapore is the first express integrator to achieve certification to ISO 28000.
- **YCH India** is also certified TAPA 'A-class' and ISO 28000-compliant for its security systems.
- **DB Schenker**, the world's second-largest forwarder, obtained ISO 28000 certification for its regional head office for the Asia-Pacific sector in Singapore last year, along with its local office and operations
- **Asian Terminals** (first marine terminal in Philippines),
- **CTS Logistics-China** (kitting assembly of turnkey management of consumer electronic, IT and telecommunication)
- **Banner Plasticard - Philippines** (design and printing of cards, personalization, embossing, encoding, thermal printing, wrapping crating and palletizing).

Few last words about ISO 28002- Resiliency

- Resiliency is becoming an expected corporate policy (drivers are customer demands, codes of corporate governance, obtaining finance, and others)

- Countries tend to be more accepting of standards if they had an opportunity to participate in the development and approval of the standards

This concludes my prepared remarks

- If there is time remaining let us discuss your questions and comments.

- If we are out of time, I will be staying for the entire summit and look forward to discussing the issue with you on the breaks.

Contact information

Steven O'Malley

aninso.llc@gmail.com

Tel: 425 442 7521

Thank You!