Center for International Trade & Security

School of Public & International Affairs

UNIVERSITY OF GEORGIA

Nuclear Security Culture As a Tool to Address Insider Threat

Dr. Igor Khripunov

at

The IAEA International Conference on Physical Protection,
13-17 November 2017, Vienna, Austria

Overview

- **Insider threat and the role of Nuclear Security Culture (NSC)**
- **IAEA NSC Model and assessment methodology**
- **Selection of characteristics and culture indicators relevant to addressing insider threat**
- **Conduct of NSC self-assessment focusing on insider threat**
- **Conclusion: a systemic and comprehensive methodology in the context of overall organizational culture**

Insider Threat: Definition

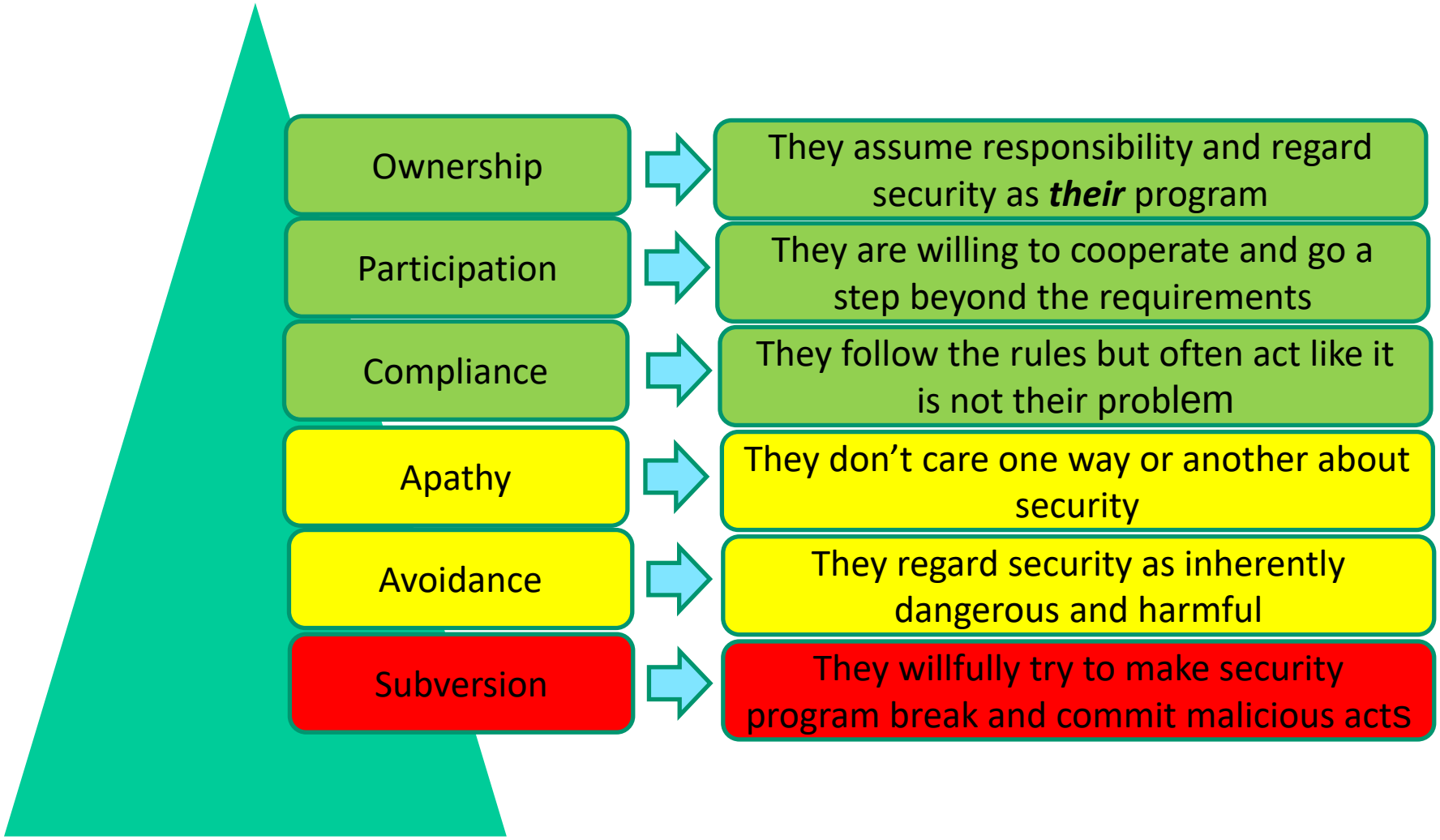
- ***Insider is defined as one or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so***

  Source: Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities" (INFCIRC/225/Rev.5) IAEA Nuclear Security Series No. 13, 2011

- Insider adversaries possess a ***unique set of attributes*** that give them advantages over outsiders, including:
  - ***Access:*** physical access, remote computer access, and access to or knowledge of sensitive information.
  - ***Authority:*** authority to conduct operations in the performance or their assigned duties and to direct other employees.
  - ***Knowledge:*** expert knowledge of the facility or its systems, including knowledge enabling to bypass or defeat dedicated physical protection elements.

Attitudes Toward Security Among Personnel

Center for International Trade & Security
School of Public & International Affairs
UNIVERSITY OF GEORGIA



Security Culture as a Tool to Address Insider Threat

Center for International Trade & Security
School of Public & International Affairs
UNIVERSITY OF GEORGIA

"…an absence of ***security culture***, security awareness and trustworthiness programs may be favorable or conducive to insider threat attempts to perform malicious acts," p.6

"Implementing a strong security awareness program for staff and contractors contributes to an ongoing ***security culture*** within the organization," p.12

"…security awareness programs should be developed in a coordinated manner with safety awareness programs in order to establish ***effective and complementary safety and security culture***," p.13

"…good relations among workers and between management and workers should be given due consideration and should be part of ***the security culture***," p.13

Source: "Preventive and Protective Measures Against Insider Threat: Implementing Guide, IAEA Nuclear Security Series No. 8, 2008

IAEA Nuclear Security Series and Nuclear Security Culture

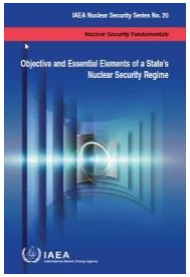
Center for International Trade & Security
School of Public & International Affairs
UNIVERSITY OF GEORGIA

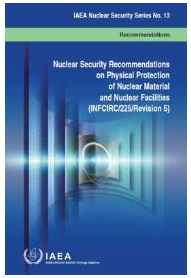
Fundamentals

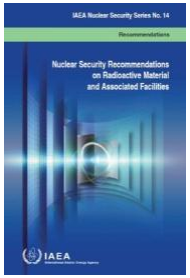
Recommendations

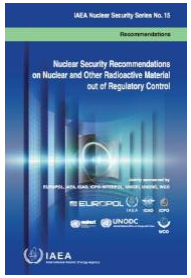
Implementing Guides

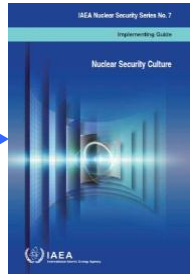
Technical Guidance







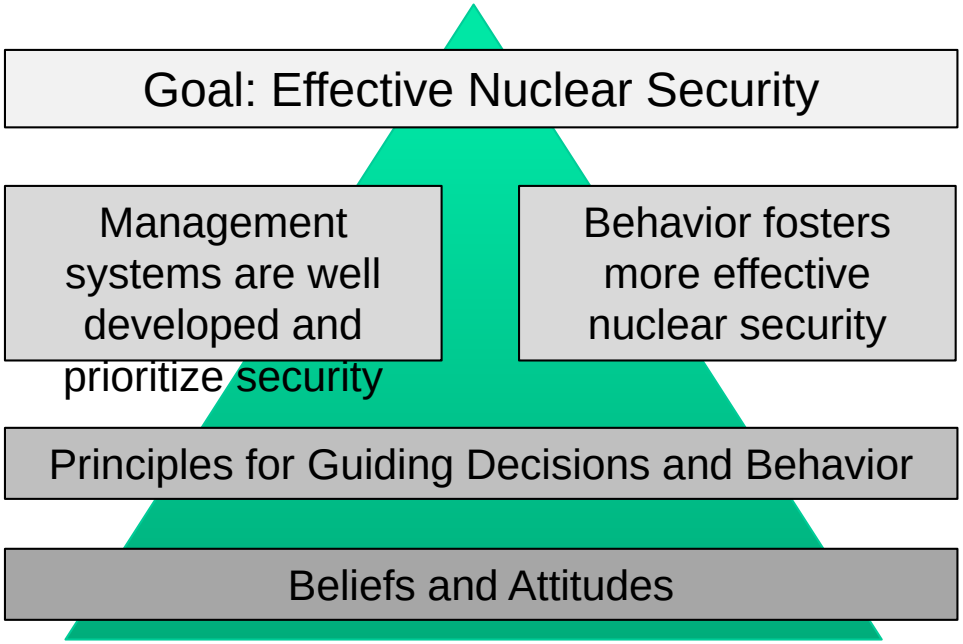




Draft Technical Guidance on NSC Self-Assessment to be released in 2017

Draft Technical Guidance on NSC Enhancement to be released in 2018-2019

IAEA Model of Nuclear Security Culture



- In September 2008, the IAEA released a guidance in its Nuclear Security Series (No.7) under the title "Nuclear Security Culture: Implementing Guide." The guidance defines the concept, model, characteristics, and indicators of nuclear security culture while also describing the roles and responsibilities of institutions and individuals.

IAEA Model of Nuclear Security Culture

GOAL: EFFECTIVE NUCLEAR SECURITY

LEADERSHIP BEHAVIOR

(a) Expectations
(b) Use of authority
(c) Decision making
(d) Management oversight
(e) Involvement of staff
(f) Effective communications
(g) Improving performance
(h) Motivation

MANAGEMENT SYSTEMS

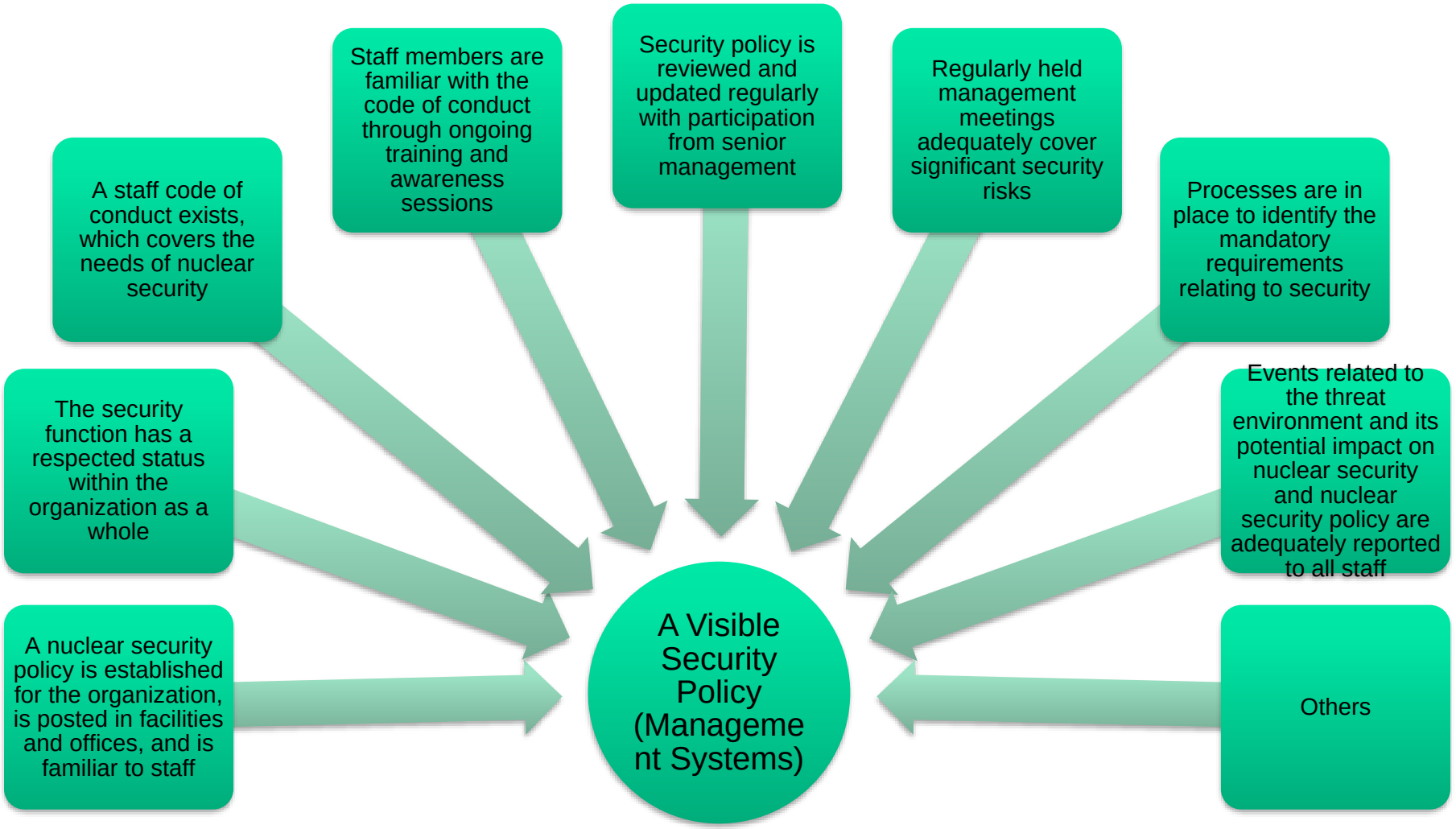
(a) Visible security policy
(b) Clear roles and responsibilities
(c) Performance measurement
(d) Work environment
(e) Training and qualification
(f) Work management
(g) Information security
(h) Operation and maintenance
(i) Continual determination of trustworthiness
(j) Quality assurance
(k) Change management
(l) Feedback process
(m) Contingency plans and drills
(n) Self-assessment
(o) Interface with the regulatory
(p) Coordination with off-site organizations
(q) Record keeping

PERSONNEL BEHAVIOR

(a) Professional conduct
(b) Personal accountability
(c) Adherence to procedures
(d) Teamwork and cooperation
(e) Vigilance

- 30 observable characteristics are illustrated by culture indicators
- Culture indicators are listed in relevant IAEA publications on nuclear security culture.
- Users of security culture methodology can use indicators as they are, modify them or develop their own consistent with specific security requirements

Sample of Characteristic-Indicator Package



Samples of Culture Indicators for Characteristics Relevant to Insider Threat Prevention and Protection

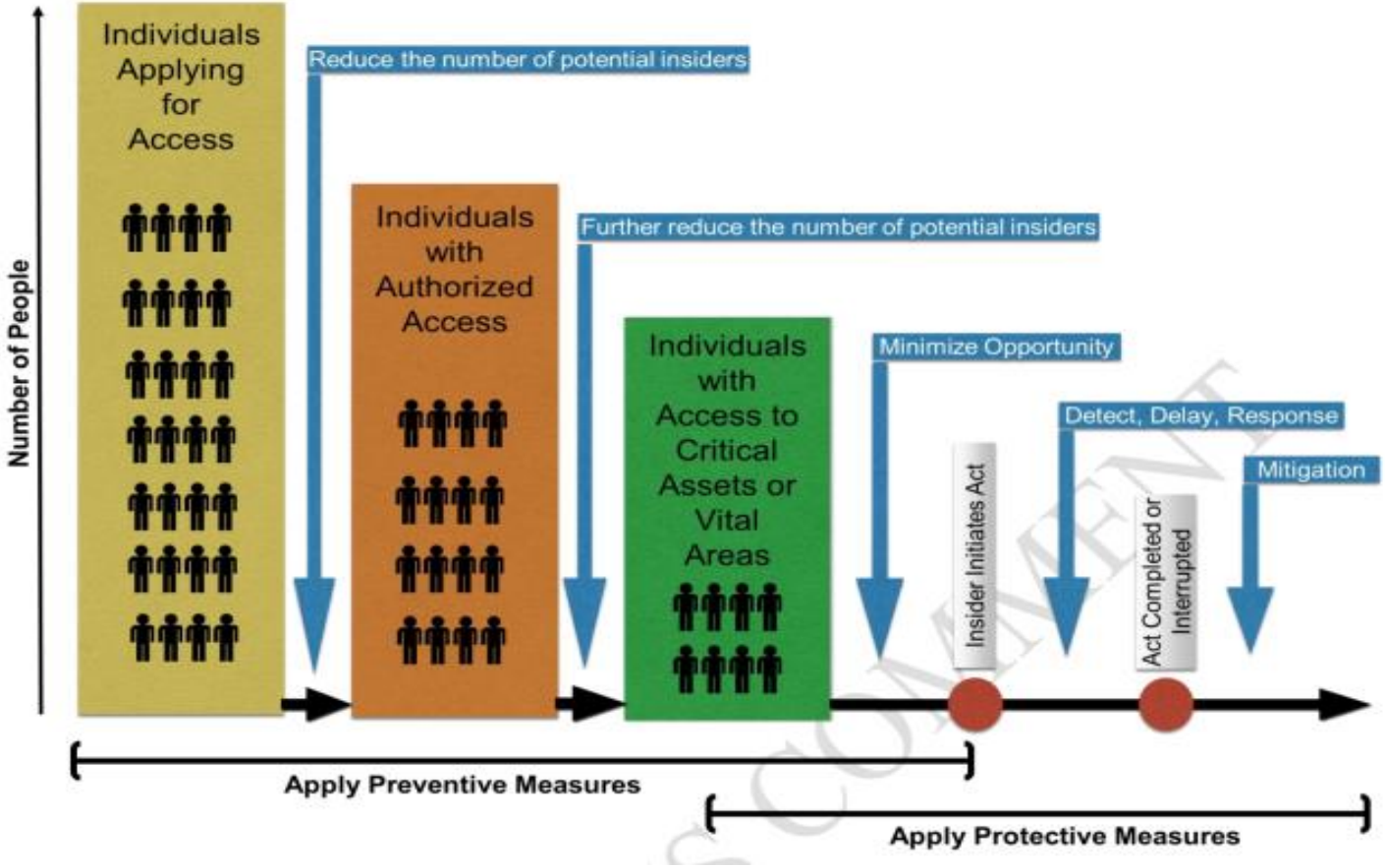
Center for International Trade & Security
School of Public & International Affairs
UNIVERSITY OF GEORGIA

Continuous Determination of Trustworthiness	Work Environment	Adherence to Procedures
• **The process of background checks is periodically reviewed** • **Screening processes are matched to the risks and threats associated with specific roles and responsibilities** • **Real or apparent failures of the screening process are appropriately investigated and adjudicated** • **Leaders provide support and resources for effective implementation of trustworthiness programs.** • **Staff is aware of and understand the importance of trustworthiness determination**	• Management show that professional capabilities and experience are the most valuable assets • Managers make themselves approachable and call for effective two-way communication • Dissenting views, diverse perspectives and robust discussion are appreciated • Security is considered a respectable career-enhancing profession • Performance-improvement processes encourage staff to offer innovate ideas	• Personnel understand potential consequences of noncompliance • Instructions on security are easy to follow because they are clear, up to date, easily available and user friendly • Leaders lead by example and—as is expected from all staff—adhere to policies and procedures in their personal conduct • The organization actively and systematically monitors security performance through multiple means

Samples of Culture Indicators for Characteristics Relevant to Insider Threat Prevention and Protection (cont.)

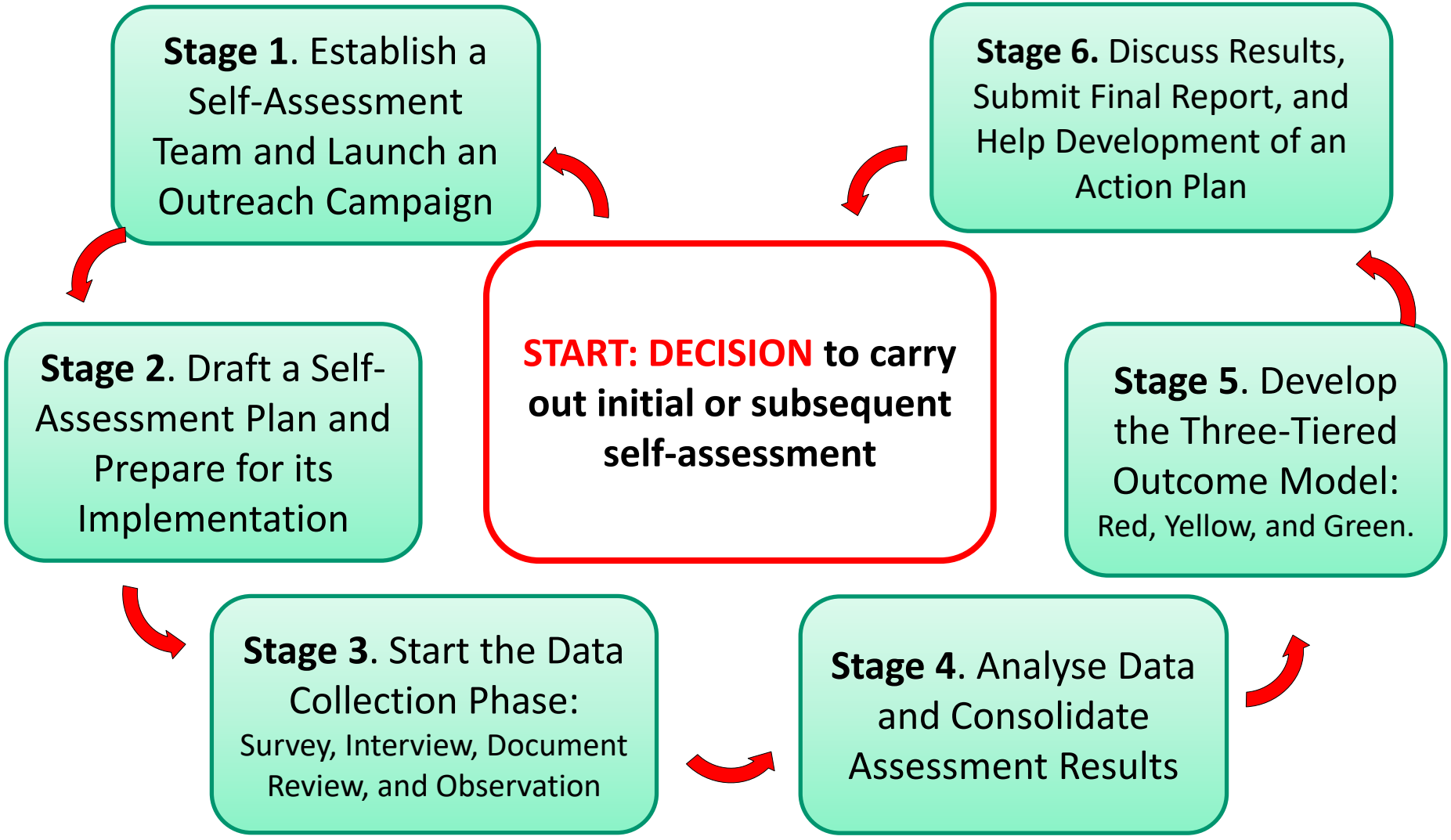
Training and Qualifications	Vigilance	Personal Accountability
• **Training materials include good practices and lessons learned from security breaches** • **Training programs at the organization address security-conscious behavior as a key element of professionalism** • **Systems are in place to ensure procedures and practices learned in training are applied in practice** • **Security awareness training instructs all staff on proper workplace security as well as requirements for reporting security violations**	• Personnel notice and question unusual behavior and incidents and report them to management as soon as possible using the established procedures • Personnel seek guidance when they are unsure of the security significance stemming from unusual events, observations or incidents • Personnel are aware of a potential insider threat and its consequences • A policy prohibiting harassment and retaliation for raising nuclear security concerns is enforced	• Personal accountability is clearly defined in appropriate policies and procedures • Personnel consider themselves responsible for security at the organization • Personnel understand how their specific tasks support the nuclear security system • Behavior that enhances security culture is reinforced by peers

Steps for preventive and protective measures against potential insiders



IAEA Self-Assessment Methodology: Multi-Stage Process

Center for International Trade & Security
School of Public & International Affairs
UNIVERSITY OF GEORGIA



Conclusion

- The value of security culture self-assessment as a tool to address insider threat is in its systemic and comprehensive nature in the context of overall organizational culture
- A wide campaign to promote security culture and its assessment is applicable to the entire workforce and can potentially deter malicious acts:
  - Relevant information and skills regarding threats and increased visibility of security (briefings, training, general meetings, social media, special events, others)
  - Leadership involvement and personnel commitments
  - Regularly held self-assessments and discussion of final reports
  - Enhancement plans as an integral part of overall management policy
  - Effective supplement to conventional classroom training.
- Like other methods, this approach is far from being perfect, but it is multifunctional and can effectively support other currently applied methods and compensate for their possible limitations.

Thank you for your attention!

Questions?