

Nuclear Security for Executive Management

CONTENTS

The WINS Academy Elective on Nuclear Security for Executive Management gives personnel with positions of executive authority—but who are not fulltime security professionals—insight into their responsibilities for nuclear security. Executive managers with responsibilities for nuclear security can be found in such departments as:

Legal and Regulatory Affairs	Engineering and Design	Information Technology
Finance and Insurance	Operations and Maintenance	Sales and Marketing
Procurement/Supply Chain	Safety and Environment	Corporate Communications
Risk Management	Human Resources	Administration

Building on the Foundation Module, this module emphasises that security, like safety, affects all parts of an organisation and is a fundamental aspect of risk management and corporate reputation. Consequently, it should be treated as a strategic operational activity that is implemented across the entire organisation.

In most cases nuclear security is a fundamental aspect of a nuclear organisation's licence to operate and subject to regulatory oversight. When it comes to addressing regulatory requirements, organisations have two approaches from which to choose:

- **The Minimalist Approach:** The organisation complies with the security regulations (it has no choice), but its policy is to do the minimum necessary at minimum cost.
- **The Proactive Approach:** The organisation believes that security, safety and environmental protection underpin effective business performance and support its strategic objectives; therefore, it manages all of these functions as effectively and efficiently as possible.

A proactive approach means that senior management view the cost of both safety and security as an investment rather than as an unavoidable regulatory overhead. Evidence suggests the most commercially successful nuclear organisations are those whose leadership commit to excellence and high safety, security and performance standards.

This module enables participants to understand:

- Some of the characteristics of excellent business, including key success factors for achieving strategic objectives and implementing new strategies.
- How to use balanced scorecards and leading and lagging indicators to measure security performance and provide assurance to the board of directors and regulator.
- How an Executive Committee for Security can contribute to the effective performance of a security programme.
- How to manage security information as part of a broader risk management process and how to build a financial model for security expenditure.
- The importance of engaging with staff and contractors so they become part of the security solution, not part of the problem.
- Some challenges that may prevent security from being managed effectively and how to resolve them.



OUTLINE

UNIT 1: SUCCESSFUL STRATEGY IMPLEMENTATION

- 1.1 Characteristics of Excellent Businesses
- 1.2 Implementing a Successful Nuclear Security Strategy: Assessment Tools

UNIT 2: INTERNAL MANAGEMENT PROCESSES AND METRICS

- 2.1 Assessing the Risks: Taking a Broader Approach to Security Risk Management
- 2.2 Board versus Executive Management Responsibilities
- 2.3 Executive Roles and Mapping Accountabilities
- 2.5 The Executive Committee for Security
- 2.6 Attributes of a Successful Security Director

UNIT 3: KEY OPERATIONAL ISSUES AND BEST PRACTICES

- 3.1 Improving the Interface between Safety, Security and Emergency Planning
- 3.2 Financial Aspects of the Security Programme
- 3.3 Managing Low Probability, High Consequence Events

UNIT 4: EMPLOYEE ENGAGEMENT AND COMMUNICATIONS

- 4.1 Preparing for a Revised Security Strategy
- 4.2 Employee Inclusion
- 4.3 Employee Induction Training and On-going Communications
- 4.4 Employee Clarification
- 4.5 Whistleblowing: Establishing Systems and Investigative Reports

UNIT 5: COMMON PROBLEMS AND SUGGESTED SOLUTIONS

- 5.1 Cognitive Blockages
- 5.2 Resource Blockages
- 5.3 Motivational Blockages
- 5.4 Political Blockages