# CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

## Using Standards to Build an Information Security Program

**Key Message**: Business leaders can use international standards to create a business- and risk-based information security program.

**Executive Summary**

Information security internal standards have been broadly reviewed, vetted, and adopted by a wide range of organizations. Business leaders should consider using these with confidence as a trusted source for building and sustaining their information security program. Not only are these standards process- and risk-based, but they also can be used to benchmark an organization's practices with its peers and market leaders.

This effort requires the involvement of a multi-disciplinary team with an enterprise perspective and needs to be managed just like any other key business project.

In this podcast, Bill Wilson, technical manager of CERT's Survivable Enterprise Management Team, discusses how business leaders can use the leading international standards for information security to jump-start an effective information security program.

---

**PART 1: AN INTRODUCTION TO THE LEADING STANDARDS: ISO 17799 AND ISO 27001**

**What Are the Leading Standards for Information Security?**

ISO/IEC 17799: Code of Practice for Information Security Management

ISO/IEC 27001: Requirements for an Information Security Management System

ISO 17799 describes security practice principles and guidelines in the following 11 categories, starting with an introduction to risk assessment and treatment:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

ISO 17799 can be thought of as a handbook of controls.

ISO 27001 is organized and structured around a plan, do, check, act (PDCA) cycle, which is fairly standard for any process-based improvement program.

**What Are the Benefits of Using These Standards?**

ISO 17799 and 27001

- are international standards
- describe a common language that has been widely adopted over the past 15 years or so
- have been proven and tested by organizations and security practitioners
- provide a recipe that can serve as an excellent starting point for building an effective security program
- can be used to benchmark your organization's program against others
- can be used to evaluate your supply chain partners' security
- provide a broad, international community of practice to draw from
- can be used as a basis for information security audits and certification

---

## PART 2: GETTING STARTED

### What NOT to Do

Do not jump into practice implementation (the Do part of Plan, Do, Check, Act) without sufficient planning.

Selection of security controls needs to be risk-based, in the context of the organization's business objectives and the overall information security management system (27001).

### First Steps to Take

- Start with 27001, not 17799.
- Make sure there is executive-level sponsorship, as a standards-based security program takes time and long-term care, feeding, and investment.
- Be clear about scope:
    - Will the information security management system (ISMS) be for the entire organization or initially for selected business units, as a pilot or trial?
    - What assets (systems and business processes) are included? Excluded?
- Treat this effort as a legitimate project with the same oversight as other projects.

### Should I Tackle This In-House or Outsource It?

It is essential to put any security program in a business context, and this is sometimes difficult when using third parties.

Conversely, there are many experienced service providers that are familiar with these standards and how best to implement them.

When using outside parties, you need to adopt a collaborative approach and stay actively involved.

When tackling this type of project in-house, it helps to be familiar with process-based improvement approaches such as those described in ISO 9001 and the SEI's Capability Maturity Model.

Apply the same rigor and thinking as you would use for any make-or-buy decision.

---

## PART 3: IMPLEMENTATION CHALLENGES, BARRIERS, & KEY ROLES

### The Need to Use a Process- and Risk-Based Approach

To be successful, an ISMS requires a process-based approach driven by risk assessment and risk management, and closing the gap between your current and desired state.

The results of ongoing risk assessment determine which practices to implement. Results and the decisions based on these need to be defensible. For example:

- We've looked at our critical business processes.
- We've determined which assets are critical.
- We've identified relevant risks to those assets.
- We've identified required mitigation steps or risk treatment options.
- We've used risk treatment options to drive the selection of controls.

To be compliant with 27001, you need to be able to answer the question, "Did the risk assessment result in decisions and plans that effectively address the high-priority risks?"

In other words, "I've followed the steps advocated in the standard, and I've produced results that tie back to my business needs and the organization's assets."

**The Devil Is in the Details**

There is always competition for senior managers' attention and for investment dollars.

ISO 27001 and 17799 describe what needs to be done, not how.

The program requires supporting processes, practices, and tools to be successfully implemented. Some organizations struggle with pulling this together and may lose their collective will over the long term.

Also, organizations may opt to select specific controls or technologies without thinking things through from a big-picture perspective.

And the big-picture perspective is essential: A standards-based security program can turn out to be a much larger undertaking than originally planned if you don't do your homework.

Unfortunately, many organizations bury such a program in their IT or security organizations, even though business knowledge, context, and buy-in are essential.

**Some Key Roles**

A designated project manager is critical to ensure any standards-based security effort is treated as an organizational project using the same planning, requirements, reporting structure, tools, and approaches as other projects.

Someone needs to have the responsibility for communication: outreach and building awareness for the project and the changes that will result from its implementation, describing the:

- ISMS process background
- Preparation for what is to come
- Information required to conduct the project
- Level of involvement required from various organizations such as business units and human resources

Other roles that may be involved include external and internal audit (for certification).

---

**PART 4: SUSTAINING A STANDARDS-BASED SECURITY PROGRAM**

**Tying the Security Program to Compliance**

Often, a security program is sustained as a key contributor to regulatory and other types of compliance.

Leaders need to recognize that 27001 and 17799 represent a starting point; there are likely other security requirements to fulfill that are not addressed by these standards.

- The ISMS Plan, Do, Check, Act approach will support including these additional requirements.

If I adopt these standards, will I keep myself and my organization out of the headlines?

- 27001 represents a significant starting point and first effort, but day-to-day operational action is key, as is making sure that the right people are in the right place at the right time for implementing effective controls tied to risk.
- As risk changes, operational, management, and technical controls also need to change. Having the discipline to review and update controls in a timely manner based on change is key.

## Future Plans for the 27000 Standards Series

- 27001: Information security management system, as described in Part 1
- 27002: New designation for ISO 17799 (to make the 2700x numbering consistent)
- 27003: Implementation guidelines, intended to address more of the how rather than the what
- 27004: Metrics and measurement
- 27005: Information security risk management
- 27006: Guide for accredited certification bodies on formal ISMS certification processes

**Resources**

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). Information technology - Security techniques - Code of practice for information security management. ISO/IEC 17799:2005(E), Second edition, June 15, 2005.

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC 27001:2005(E), First edition, October 15, 2005.

---