Ultimate Security

www.TerminuSys.com info@TerminuSys.com

Terminus System Comprehensive ISMS Implementation Model

Secure Your Business. Optimize Your Resources. Achieve Excellence.

Why Ultimate Security?

Our comprehensive and agile Information Security Management System model is designed to ***maximize organizational benefits*** while ***minimizing resource expenditure***—including time, budget, and human effort. By ***strategically aligning the ISMS with your business objectives***, ***it unlocks the full potential of your organization's security***.

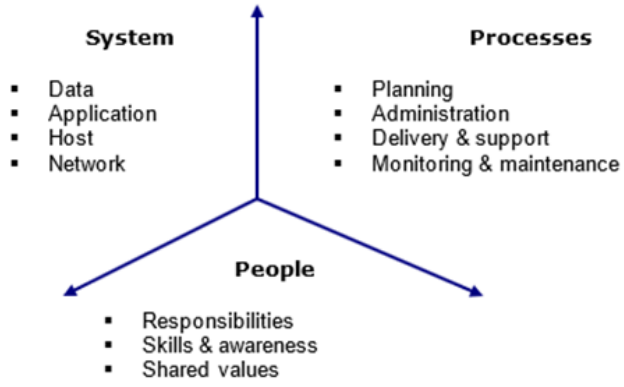
Ultimate Security defines clear information security objectives, identifies key challenges and drivers, and provides a structured roadmap to assess, prepare, and successfully implement an effective ISMS.

Ultimate Security stands out by:

translating everyday business language into actionable security measures

This unique feature allows users to communicate their security needs in familiar terms, ensuring a seamless and stress-free experience. With ***Ultimate Security***, achieving your security goals has never been easier.

Using this model, we examine the security status of the organization in the following areas:



Our model helps organizations:

- Strengthen organizational resilience against cyber threats
- Align security investments with business objectives
- Reduce financial and operational risk exposure
- Improve governance and regulatory compliance
- Optimize security spending through risk-based prioritization
- Enhance operational efficiency and process integrity
- Establish measurable and sustainable security performance

"Ultimate Security: Where Business Meets Security."

Ultimate Security

www.TerminuSys.com info@TerminuSys.com

Features

Ultimate Security is characterized by four core features:

1. **Process-Oriented**
   Unlike generic approaches, this model integrates directly with business processes. This connection:
   - Facilitates measuring the effectiveness of security measures
   - Enhances personnel engagement by linking their daily activities to ISMS objectives
   - Reduces process risks, improving business operations
2. **Excerpt-Oriented**
   Applying the Pareto principle, Ultimate Security focuses on the 20% of processes that generate 80% of the potential benefits. While all processes are considered, priority is given to key areas, making implementation faster, cost-effective, and impactful.
3. **Profit-Oriented**
   Ultimate Security emphasizes tangible business value, addressing common misconceptions:
   - ISMS as a prestige or certification exercise
   - ISMS without practical benefits

   By focusing on the improvement of key business processes, Ultimate Security ensures that ISMS implementation delivers measurable organizational benefits.
4. **Cycle-Oriented**
   Following a cyclical improvement philosophy (Deming's PDCA approach), ISMS implementation is iterative. Each cycle:
   - Reviews organizational status
   - Analyzes results from the previous cycle
   - Develops a new plan for security improvement

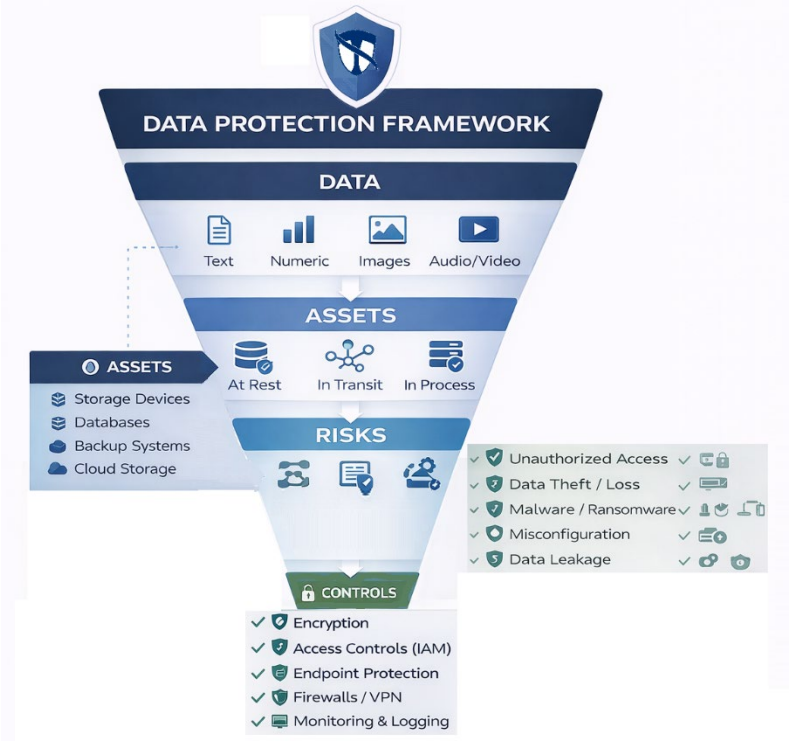
   This approach ensures continuous enhancement of security aligned with evolving

Philosophy of Ultimate Security

At the core of our model is a simple principle: **protect your most valuable asset—data—while maximizing business value**.
We consider all forms of data—digital, physical, and human knowledge—and address their full lifecycle:

- **At Rest:** Stored on devices, servers, or cloud
- **In Transit:** Moving across networks, applications, or cloud services
- **In Process:** Actively used in systems, applications, or cloud compute

Our approach is **risk-driven and benefit-focused**, applying the right controls to ensure confidentiality, integrity, and availability without overcomplicating implementation.



Why It Works:

- **Holistic:** Covers people, processes, and systems
- **Practical:** Focuses on key areas that deliver maximum impact
- **Agile:** Adapts to organizational needs and resources
- **Value-Oriented:** Aligns information security with business goals

How It's Applied

Now, the important question is "What controls should we use for our case"?
To answer this question and design RTP (Risk Treatment Plan), this model is using all possible tools and facilities, including:

- Security Domains → define scope (WHAT to secure)
- Security Principles → define behavior (HOW to think)
- Framework / Standards → define requirements / specifications (WHAT must exist)
- Guidance / Baselines → define configuration (HOW to configure)
- Best Practices → enforce protection (HOW to implement)
- Models → ensure operation (HOW to operate daily)

We integrate **security domains, principles, frameworks, guidance, and best practices** to create a tailored security program that is measurable, sustainable, and continuously improving.

Ultimate Security

www.TerminuSys.com info@TerminuSys.com

It covers everything in information security including:

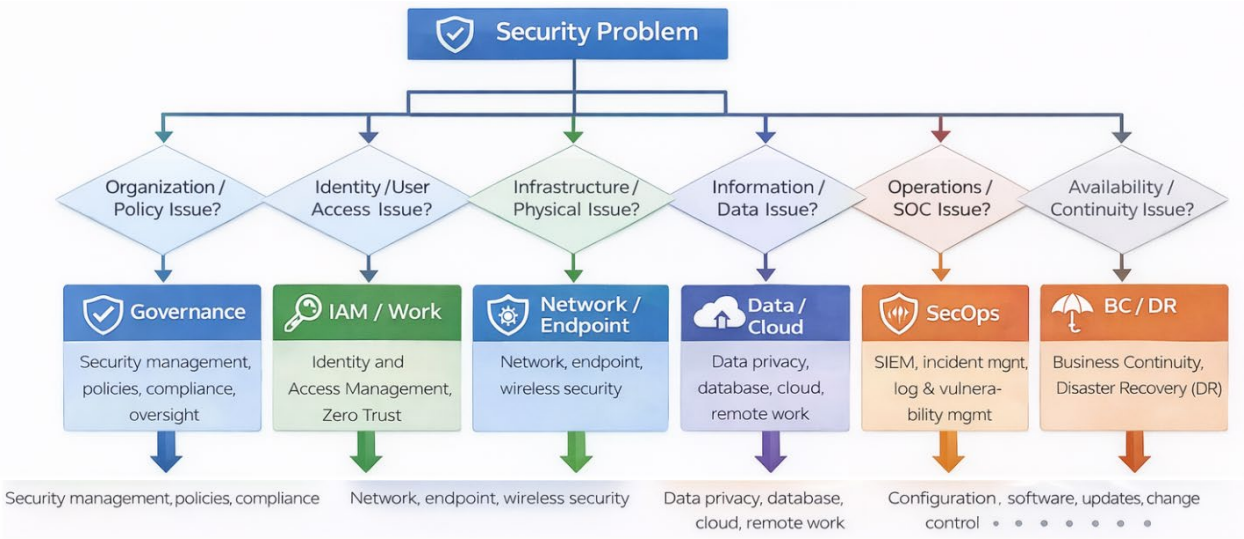
- ***27 Security Domains***
- ***16 Security Principles***
- ***85 Security Standards***
- ***45 Security Frameworks***
- ***30 Security Guidance***
- ***And Best Practices***

And much more …

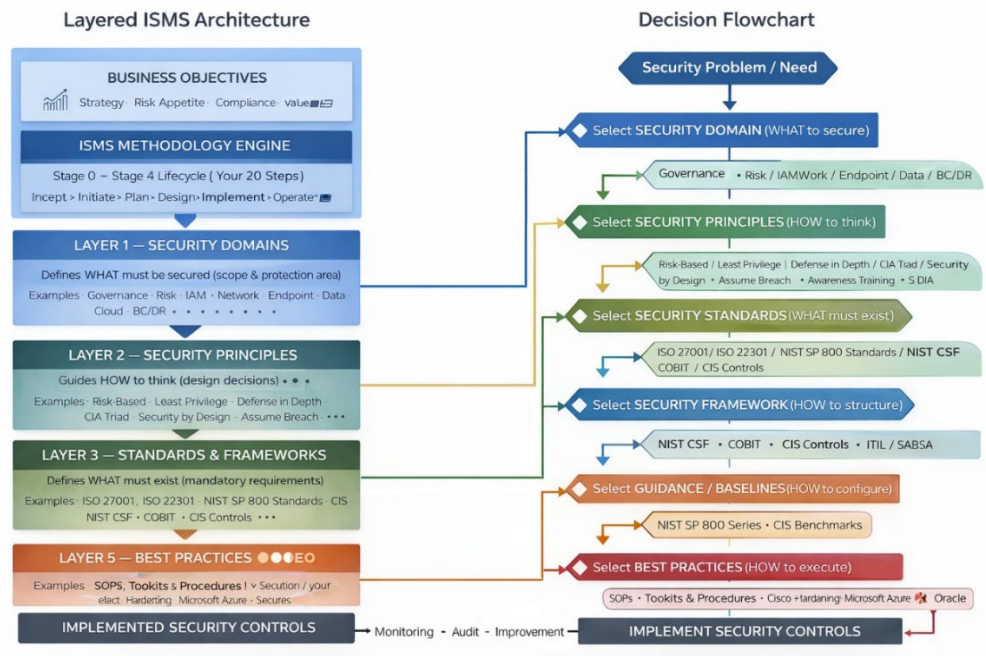
Within Ultimate Security, security implementation follows a structured decision chain that transforms business intent into operational protection. Starting from the **business need**, the 20-step ISMS process defines a systematic path for implementation.

"Speak Business. Think Security."

This process determines the appropriate **security domains** that define the scope of protection.



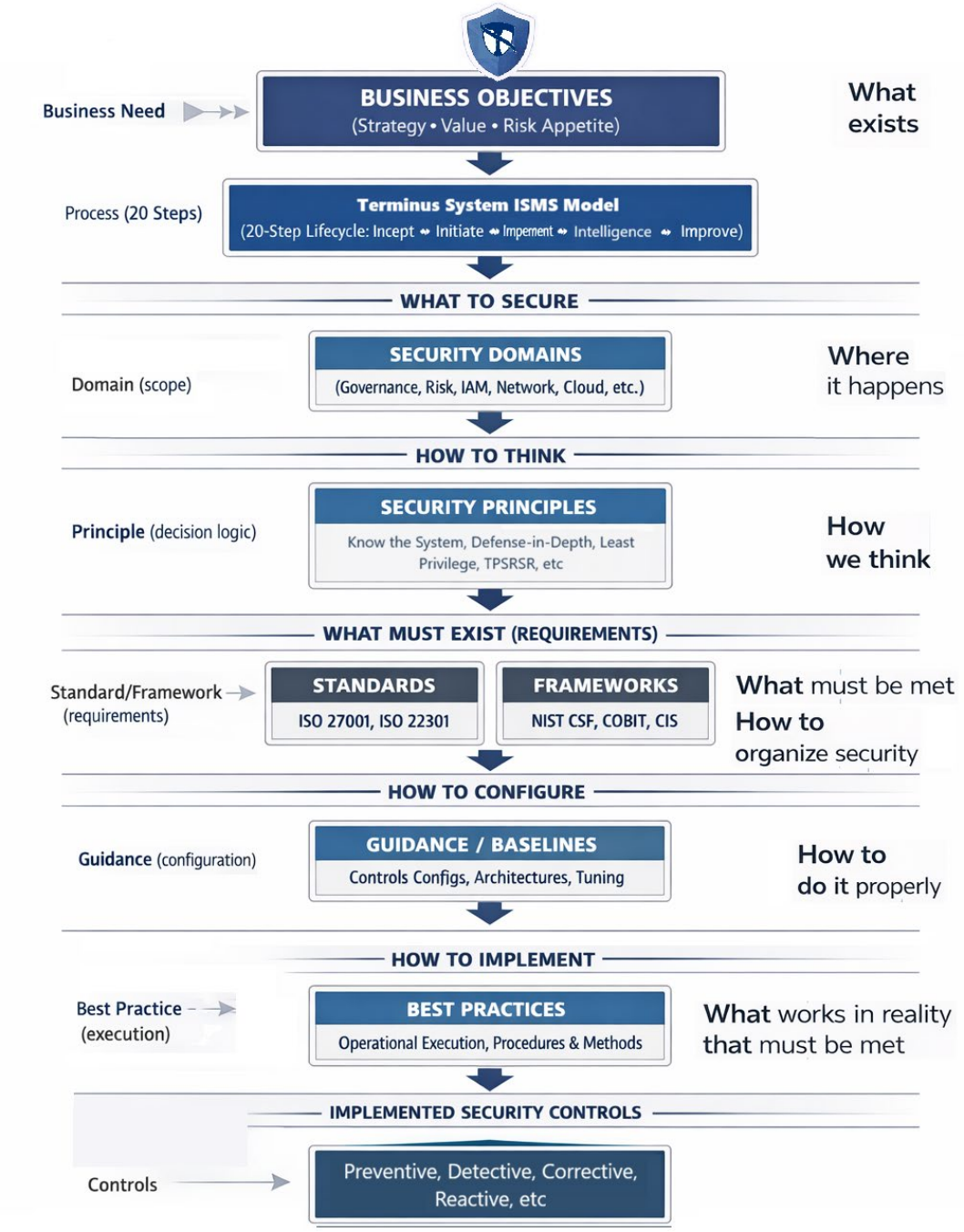
Each domain applies one or more **security principles** that provide decision logic and guide design choices. These principles and domains are then translated into formal **standards and frameworks**—such as ISO/IEC 27001 or NIST Cybersecurity Framework—which define required controls and compliance expectations. From these requirements, organizations derive **guidance and baselines** that specify technical configurations and architectural settings. Each guidance baseline can generate multiple **best practices** that define operational procedures and execution methods, ultimately resulting in implemented security controls.



The relationships between these elements are dynamic and many-to-many: a single domain may relate to multiple principles and multiple frameworks or standards; one principle may map to several guidance or baseline configurations; a framework can also produce multiple guidance sources; and each guidance baseline may lead to several best practices.

This layered and interconnected structure ensures flexibility, consistency, and alignment between business objectives, risk management decisions, and practical security implementation.

www.TerminuSys.com info@TerminuSys.com



The 20-Step Journey to Security Excellence

Our model is a **multi-layered, end-to-end framework** based on **PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize)**, aligned with the **Deming Cycle**, and covering all approaches to information security management. It consists of **1 primary stage** (2 phases, 7 steps) and **4 main stages** (6 phases, 20 steps). Each step contains key activities to ensure practical, measurable results.

Stage 0 – Inception

Purpose: Establish a solid foundation before starting the ISMS project. Ensures business justification, project readiness, and organizational alignment.
Outcome: Comprehensive technical and financial proposal.

Phase 0.1 – Security Justification

Determines the necessity, urgency, and business value of improving security.

- **Step 0.1.1 – Executive Security Posture Assessment**: Evaluate current security status across domains.
- **Step 0.1.2 – Total Loss Estimator**: Estimate potential financial losses from security gaps.
- **Step 0.1.3 – Implementation Urgency**: Assess urgency and prioritize improvements.

Phase 0.2 – Engagement Preparation

Prepares the organization for project execution by defining scope, boundaries, and readiness.

- **Step 0.2.1 – Project Definition**: Define high-level objectives and alignment with business priorities.
- **Step 0.2.2 – Boundary Definition**: Determine project scope and limits.
- **Step 0.2.3 – Security Domains Posture Assessment**: Evaluate in-depth status of targeted security domains.
- **Step 0.2.4 – Readiness Assessment**: Confirm organization's readiness to undertake ISMS implementation.

Stage 1 – Initiation

Phase 1 – Prepare

Establishes foundational understanding of the organization and assets.

- **Step 1 – Setup**: Assess readiness, challenges, and information availability.
- **Step 2 – Business Cognition**: Map organizational structure, goals, strategies, and obligations.
- **Step 3 – Asset Inventory**: Identify all assets (information, hardware, software, human resources, infrastructure, intangible).
- **Step 4 – Business Processes Management**: Document, map, and analyze all business processes.

Phase 2 – Plan

Designs the project blueprint, defines boundaries, and evaluates assets and gaps.

- **Step 5 – Project Plan**: Allocate resources, define tasks, timing, and deliverables.
- **Step 6 – Scope Definition**: Determine project scope, stakeholders, and interdependencies.
- **Step 7 – Gap Analysis**: Identify gaps between current and target security states.
- **Step 8 – Asset Evaluation**: Quantify asset value and role in achieving business goals.

Stage 2 – Implementation

Phase 3 – Design

Sets the framework for ISMS deployment, ensuring alignment with organizational goals.

- **Step 9 – Risk Assessment**: Identify, analyze, and evaluate risks to assets.
- **Step 10 – Risk Treatment**: Define solutions and mitigation plans for unacceptable risks.
- **Step 11 – Security Strategic Plan**: Develop long-term strategy and objectives.
- **Step 12 – Security Policy Development**: Establish policies, procedures, and technical guidelines.
- **Step 13 – Training & Awareness**: Define role-based training and awareness programs.
- **Step 14 – Business Continuity & Disaster Recovery Plan**: Identify critical services, recovery objectives, and DR strategy.

Phase 4 – Implement

Executes security solutions and manages deployment.

- **Step 15 – Implementation Planning**: Plan rollout of technical and organizational controls.
- **Step 16 – Implementation Management**: Oversee execution and ensure compliance with strategic plan.

Stage 3 – Intelligence

Phase 5 – Operate

Monitors and manages security operations.

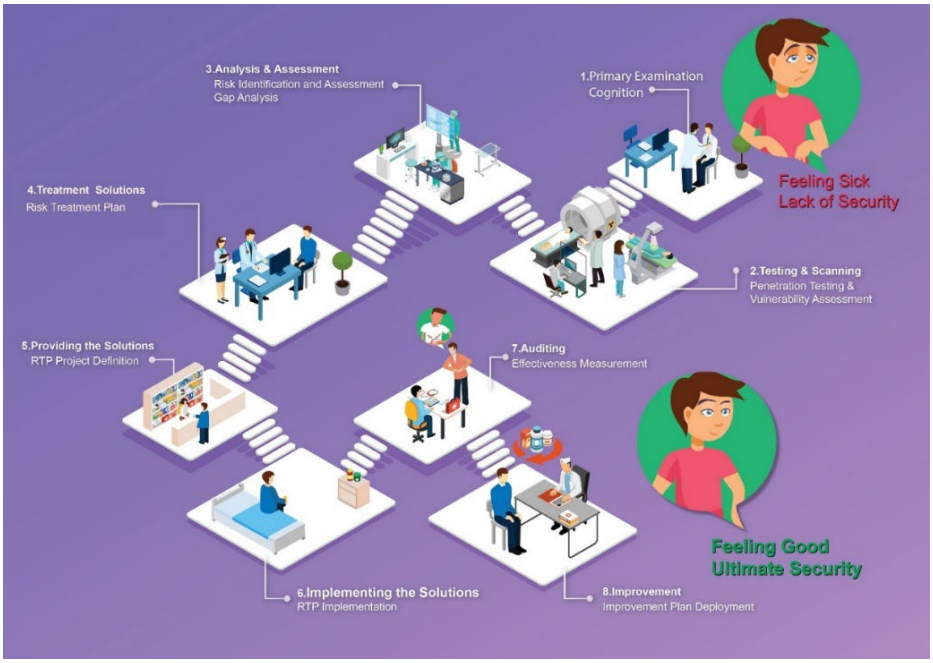
- **Step 17 – Operation Management**: Maintain security controls, monitor performance, and respond to incidents.

Stage 4 – Improvement

Phase 6 – Optimize

Continuously evaluates and enhances the ISMS.

- **Step 18 – Audit**: Evaluate compliance, performance, and effectiveness.
- **Step 19 – Review**: Review metrics, incidents, and lessons learned.
- **Step 20 – Improvement Management**: Implement corrective actions and optimize security posture.



Why Choose Terminus System?

Because Ultimate Security model is:

- ✓ **Comprehensive** — Covers all security domains, principles, standards, frameworks, best practices
- ✓ **Agile** — Adapts to your organization's capacity and resources
- ✓ **Efficient** — 20-80 principle ensures maximum ROI
- ✓ **Business-Aligned** — Profit-oriented, value-driven approach
- ✓ **Proven** — Based on international best practices and standards
- ✓ **Continuous** — Built on the Deming cycle for ongoing improvement
- ✓ **Risk-Focused** — Addresses data at rest, in transit, and in process

Key Deliverables You Receive

Ultimate Security produces comprehensive implementation outputs, including:

- Security posture and maturity assessments
- Risk and impact analysis reports
- Security strategy and roadmap
- Policies, procedures, and governance framework
- Implementation plans and control architecture
- Operational monitoring and audit reports

- Continuous improvement plans

Who Benefits

- Enterprise organizations
- Government agencies
- Financial institutions
- Technology companies
- Critical infrastructure providers
- Regulated industries

Transform Your Security Posture Today

"Achieve Security Goals Effortlessly with Ultimate Security."

Move from security as a cost center to security as a business enabler. Our model provides the roadmap, tools, and framework to achieve information security excellence while optimizing your resource investment.

"AI-Powered Security for the Modern Business."

Contact Terminus System to begin your ISMS journey.

Unlocking the Full Potential of Your Organization's Security