

Best Security Practices for SCADA Systems Utilizing the COSO Framework

matrix



ISS Solutions for Security Best Practices for SCADA Systems.
Utilizing the Committee of Sponsoring Organizations of the Treadway Committee (COSO) framework.

Recognizing the need for definitive guidance on enterprise risk management, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiated a project to develop a conceptually sound framework providing integrated principles, common terminology and practical implementation guidance supporting entities' programs to develop or benchmark their enterprise risk management processes. A related objective is for this resulting framework to serve as a common basis for managements, directors, regulators, academics and others to better understand enterprise risk management, its benefits and limitations, and to effectively communicate about enterprise risk management issues.

The underlying premise of enterprise risk management is that every entity, whether for-profit, not-for-profit, or a governmental body, exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management provides a framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

Source: COSO

Section One: Internal Environment

Management sets a philosophy regarding risk and establishes a risk appetite. The internal environment sets the foundation for how risk and control are viewed and addressed by an entity's people. The core of any business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.

Source: COSO

Section Elements	ISS Program Phases	ISS Solutions to Achieve COSO Compliance
<ul style="list-style-type: none"> • Risk Management Philosophy • Risk Culture • Board of Directors • Integrity and Ethical Values • Commitment to Competence • Management's Philosophy and Operating Style • Risk Appetite • Organizational Structure • Assignment of Authority and Responsibility • Human Resource Policies and Practices 	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Collaborative Business Case Assessment • Security Strategy Workshops • Policy Gap Analysis • Best Practices for SCADA systems • Security Awareness Program • Documentation

Section Two: Objective Setting

Objectives must exist before management can identify events potentially affecting their achievement. Enterprise risk management ensures that management has a process in place to set objectives and that the chosen objectives support and align with the entity's mission/vision and are consistent with the entity's risk appetite.

Section Elements	ISS Program Phases	ISS Solutions to Achieve COSO Compliance
<ul style="list-style-type: none"> • Objectives • Selected Objectives • Risk Appetite • Risk Tolerance 	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Collaborative Business Case Assessment • Security Strategy Workshops • Policy Design • Best Practices for SCADA systems • Policy Compliance Program • Documentation

Section Three: Event Identification

Potential events that might have an impact on the entity must be identified. Event identification includes identifying factors – internal and external – that influence how potential events may affect strategy implementation and achievement of objectives. It includes distinguishing between potential events that represent risks, those representing opportunities and those that may be both. Management identifies interrelationships between potential events and may categorize events in order to create and reinforce a common risk language across the entity and form a basis for considering events from a portfolio perspective.

Section Elements	ISS Program Phases	ISS Solutions to Achieve COSO Compliance
<ul style="list-style-type: none"> • Events • Factors Influencing Strategy and Objectives • Methodologies and Techniques • Event Interdependencies • Event Categories • Risks and Opportunities 	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy Design • Best Practices for SCADA systems • QuickStart Program • Gap Analysis • Security Awareness Program • Documentation

Section Four: Risk Assessment

Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible results may be associated with a potential event, and management needs to consider them together.

Section Elements	ISS Program Phases	ISS Solutions to Achieve COSO Compliance
<ul style="list-style-type: none"> • Inherent and Residual Risk • Likelihood and Impact • Methodologies and Techniques • Correlation 	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Information, Policy, Application and Vulnerability Security Assessments • Business Risk Assessment • Gap Analysis • Penetration Test • Incident Response Testing

Section Five: Risk Response

Management selects an approach or set of actions to align assessed risks with the entity's risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.

Section Elements	ISS Program Phases	ISS Solutions to Achieve COSO Compliance
<ul style="list-style-type: none"> Identify Risk Responses Evaluate Possible Risk Responses Select Responses Portfolio View 	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> Policy Design Best Practices for SCADA systems QuickStart Program Gap Analysis Security Awareness Program Documentation

Section Six: Control Activities

Policies and procedures are established and executed to help ensure that the risk responses management selected are effectively carried out.

Section Elements	ISS Program Phases	ISS Solutions to Achieve COSO Compliance
<ul style="list-style-type: none"> Integration with Risk Response Types of Control Activities General Controls Application Controls Entity Specific 	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> Policy Design Best Practices for SCADA systems Incident Response Plan Security Awareness Program Security Strategy Workshop Documentation

Section Seven: Information and Communication

Relevant information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing and responding to risk. Effective communication also must occur in a broader sense, flowing down, across and up the entity. Personnel need to receive clear communications regarding their role and responsibilities.

Section Elements	ISS Program Phases	ISS Solutions to Achieve COSO Compliance
<ul style="list-style-type: none"> Information Strategic and Integrated Systems Communication 	Deploy and Educate	Professional Security Services (PSS): <ul style="list-style-type: none"> Policy Design Best Practices for SCADA systems Incident Response Plan Security Awareness Program Security Strategy Workshop Documentation X-Force® Education Services

Section Eight: Monitoring

Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible results may be associated with a potential event, and management needs to consider them together.

Section Elements	ISS Program Phases	ISS Solutions to Achieve COSO Compliance
<ul style="list-style-type: none">• Separate Evaluations• Ongoing Evaluations	Manage and Support	Managed Services: <ul style="list-style-type: none">• Managed Protection Services• Managed Firewall Service• Managed Intrusion Detection and Prevention Services• Vulnerability Management• Customer Portal

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236 2600

REGIONAL HEADQUARTERS

Australasia

Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838 1555
Fax: +61 (0)7 3832 4756
e-mail: aus-info@iss.net
Support e-mail: support@iss.net

Asia Pacific

Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: sales@isskk.co.jp
Support e-mail: support@isskk.co.jp

Europe, Middle East and Africa

Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: 404 236 2790
Fax: 404 236 2629
e-mail: isslatam@iss.net