|  |  |
| --- | --- |
|  | **I-ISMS Revision** 1 |

**NP Factory, Ltd.**

**Plant floor**

**Industrial Information Security Management System**

Metrics and Measurements

Nathan Pocock

https://our.intranet/path/to/document.docx

|  |  |
| --- | --- |
| **I-ISMS Revision** 1 (43) | **Industrial Information Security Management System**  Metrics and Measurements  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**KPI**

PRIVATE

|  |  |
| --- | --- |
| Do - 06 -- Metrics And Measurements.Docx  Version: 1 Revision 43  Pages: 1 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\Do - 06 -- Metrics and Measurements.docx  Keywords: key performance indicator, quality, measure, metric, analytic, report, status, performance  Last Saved by Nathan Pocock on 9/20/2016 10:37 AM |
|  | **NP Factory, Ltd.**  [Company Address]  Plant floor  I-ISMS  704-491-5840  Manager Pocock |

Executive Summary

A template for defining the key performance indicators for measuring the success and overall performance of the I-ISMS and all implemented controls and systems.

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 19-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Instructions 1](#_Toc462131179)

[2 Introduction 1](#_Toc462131180)

[1.1 Five I-ISMS processes to monitor 1](#_Toc462131181)

[1.2 Purpose 1](#_Toc462131182)

[1.3 Responsibilities 1](#_Toc462131183)

[1.4 What will be monitored 1](#_Toc462131184)

[1.5 Data collection methods 1](#_Toc462131185)

[1.6 Evaluating efficiency 1](#_Toc462131186)

[3 Measurements and Metrics 1](#_Toc462131187)

Figures

Figure 1 I-ISMS Measurements and Metrics Table 1

# 

# Instructions

This document describes how you are going to evaluate the overall status of your industrial information system management system.

**IMPORTANT**: This document describes actual work that you (or somebody) will need to do in order to collect the metrics needed to determine how good (or bad) your implementation is operating. Therefore, it is essential that you create a version of this document that is realistic to your environment and needs.

To complete this document, do the following:

1. Open the document’s properties and modify all metadata to make the document yours!
2. Review all sections of the document and revise where necessary
3. To add more rows, simply copy an empty-row and then paste for each new row needed
4. Hit CTRL+A and then press F9 to update all fields, references, and table of contents etc.

Lastly, delete this page and then save the document.

# Introduction

The I-ISMS implementation exists to protect computer systems and networked industrial devices/machines from falling victim to cyber-attacks or other security-related breaches.

## Five I-ISMS processes to monitor

The following I-ISMS processes shall be measured:

* Business Alignment
* Risk Management
* Compliance to the I-ISMS Policy
* Awareness
* Internal Auditing

## Purpose

Measuring the effectiveness of the program and the controls put in place is essential to measure success, or more importantly to determine if there are weaknesses that must be resolved.

## Responsibilities

The principal engineer and cheerleader is responsible for the initial creation and then the collection of performance data. Specific duties may be delegated as necessary.

## What will be monitored

The following will be monitored:

* Operations (internal audits, training, etc.)
* Security controls (locks, logins, etc.)
* Systems (infrastructure, hardening, policies, etc.)
* Computer systems and networked industrial devices
* Issues detected/raised/avoided

## Data collection methods

Performance data will be collected using a variety of methods, including:

* Interviewing personnel
* Reviewing system logs
* Reviewing documentation
* Measuring up/down time of systems and processes

## Evaluating efficiency

To calculate efficiency, an initial set of targets must be defined and an initial collection of baseline obtained.

# Measurements and Metrics [[1]](#footnote-1)

The following table contains the measurements and metrics that will be used for this IISMS. Complete the entries in the right-column as appropriate.

* **Target** What you are hoping to find; the goals you seek to achieve
* **Finding** What you have actually found
* **Action Plans** How you will resolve

Figure 1 I-ISMS Measurements and Metrics Table

| Measurement | Targets | Findings | Action Plan |
| --- | --- | --- | --- |
| BUSINESS ALIGNMENT | | | |
| % of strategic goals and requirements of I-ISMS policy and company/IT strategic goals/decisions  Method/sources:  Review business strategic decision as they relate to production and verify appropriate risks are assessed and security-related issues are reviewed and approved by management/ | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| % of changes made to the I-ISMS policy as mandated/requested by management review.  Method/sources:  Review decisions made and count the actions requested. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Method/sources:  … | **Target:** …  **Finding:** …  **Action Plans:** … | | |
|  | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Method/sources:  … | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Method/sources:  … | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| RISK MANAGEMENT | | | |
| % of the production floor processes covered by the I-ISMS risk management process.  Method/sources:  Interviews with plant-floor management, supervisors, and personnel | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Number of approved risk treatment plans actually being implemented compared the last risk assessment.  Method/sources:  Correlate with previous risk assessment reports. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Are changes to the production processes along with technology being addressed by the risk management processes?  Method/sources:  Interview personnel and compare to risk assessment reports. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| % of factory-floor/production budget being used to manage risk management processes.  Method/sources:  Correlate total man-hours spent on risk assessment compared to the total budget, also compare to the sub-budget allocated to technology. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| # of new threats identified compared to previous risk assessment.  Method/sources:  Compare the # new risks added to the previous reports. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Level of satisfaction with the risk assessment action items as they relate to the wellbeing of the business and safety of personnel.  Method/sources:  Interviews and/or self-assessment surveys. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Method/sources:  … | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| COMPLIANCE WITH I-ISMS (OTHER REGULATIONS?) | | | |
| # of non-compliance issues found and subsequent costs over the year  Method/sources:  Review annual internal audit reports and any external audits (if applicable). | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Time between the identification of a non-compliance till when the issue was completely resolved.  Method/sources:  Correlate the date/time of the finding to the date/time of the final sign-off. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Costs for fixing non-compliance issues with regulatory requirements (if any).  Method/sources:  Review costs as found in budgeting system. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Method/sources:  … | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| AWARENESS | | | |
| % of personnel completed awareness training  Method/sources:  Review personnel records. Interview personnel. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| # of specialized awareness training programs  Method/sources:  Review awareness training guides. Interview HR. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Time spent by employees in security awareness training over the course of a year.  Method/sources:  Review HR records. Interview personnel. Self-assessment surveys. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| % if retention of awareness information  Method/sources:  Interview personnel. Conduct surveys with questions. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Method/sources:  … | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| INTERNAL AUDITING | | | |
| % of industrial processes included in audit  Method/sources:  Correlate the # of observed/known processes to the internal audit reports. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| % of computer systems and networked industrial devices/machines included in audit  Method/sources:  Correlate the # of observed/known systems/devices to the internal audit reports. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| # of issues found that require an action plan  Method/sources:  Review audit findings. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Amount of resources allocated to address findings (e.g. time, money, manpower, etc.)  Method/sources:  Compare total # of resources and budgets to the assessment action items. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Extent of changes implemented within the I-ISMS as a result of internal audits.  Method/sources:  Review audit reports and action items list. Compare costs with last year. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Extent of changes implemented on computer systems and/or networked industrial devices/machines as a result of internal audits  Method/sources:  Review audit reports and action items list. Compare costs with last year. | **Target:** …  **Finding:** …  **Action Plans:** … | | |
| Method/sources:  … | **Target:** …  **Finding:** …  **Action Plans:** … | | |

1. Table based on examples found in *Measuring ISO 27001 ISMS Processes* (Johnson, 2014) [↑](#footnote-ref-1)