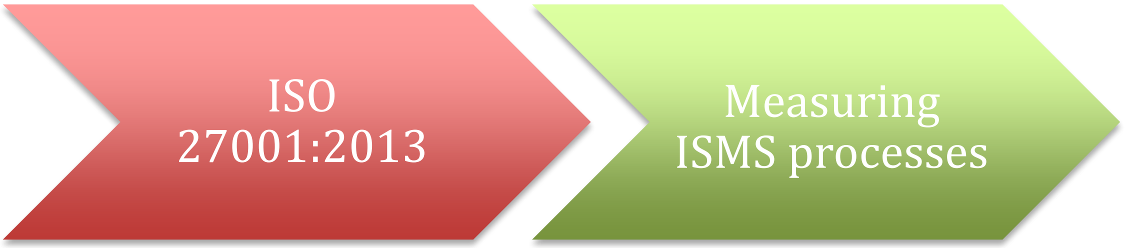

ISO 27001:2013

Measuring ISMS processes

Measuring ISO 27001 ISMS processes

By Gaffri Johnson

Senior Security Advisor

at Neupart

Introduction

During the last couple of years, interest in becoming ISO 27001 certified or the use of the ISO 27001 as a best practice framework has rapidly grown. Today, a lot of companies, government institutions and municipalities require either ISO 27001 certification or must adhere to the best practices in the standard. It's also increasingly incorporated into tender requirements or used during procurements.

The cyclic and iterative process we have come to know as PDCA or Plan-Do-Check-Act is still at the core of ISO 27001:2013 and even though it doesn't explicitly mention Plan-Do-Check-Act, it is applicable as a process framework. The following diagram illustrates how we see the link between PDCA and the ISO 27001:2013.

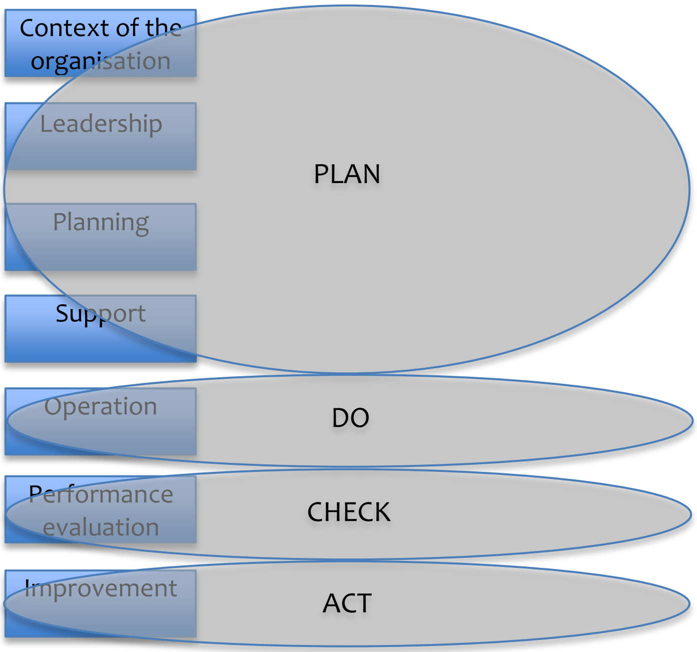

Figure 1: Link between PDCA and continuous improvement

As mentioned above, the core requirements in the ISO 27001 are mandatory processes, whereas Annex A provides suggestions for it processes and related controls.

Typically, processes are more complex to understand and time consuming to implement than the control-centric part of the ISO 27001 in annex A (ISO 27002) or other control-centric frameworks/ standards, for that matter.

ISO 27001 requires a certain level of IT governance to be in place, such as involvement from management, understanding and use of IT as a helper/enabler to achieve the business goals in an effective way. Doing that means knowing the current and emerging risks and their impact, and avoiding the worst IT-related risks. This requires a deep understanding of the organisation, business processes, IT processes, external requirements and strategic goals. That equates to a higher degree of required maturity of the organisation.

Value of an effective ISMS

Even if your organisation isn't planning to become ISO 27001 certified, having an information security governance process is essential to ensure alignment of IT processes with core business processes. This helps reduce the overall risk posture derived from this "collaboration". Some key benefits from driving an effective ISMS help encompass:

- Better IT alignment with strategic decisions.
- More ease in demonstrating the value of IT and IT security processes and related controls.
- More effective controls and better understanding of the value of those controls internally in the organisation.
- Better ability to integrate IT risk management processes with enterprise risk management processes, which over time can reduce costs and help the organisation make better strategic decisions. Examples could be software development, acquisitions or the use of outsourcing partners.
- Helps create trustworthiness amongst external parties and other key stakeholders.
- More ease in manoeuvring in an ever-changing risk and compliance landscape (technologies, threats, geo-politics, legislations, industry specific compliance, etc.).

We think it's a good move from ISO to put emphasis on the measurement part of the ISMS requirements in the new 27001 standard, as it makes it easier to operationalize the ISMS and helps build a better business case for management.

A common challenge for many organisations has been to operationalize the ISMS requirements, and decide in which processes they should embed measurement controls in order to ensure that deviations in relation to the ISMS processes are detected and addressed as part of the on-going improvement.

Choosing what to measure, setting targets and deciding how to operationalize those also poses a challenge for many organisations.

This report provides some meaningful examples on metrics along with purposes of metrics (targets). We will focus on metrics regarding the status of the ISMS and the output they generate. These are the outputs, which also feed into the reporting requirements of the ISMS.

We will not cover the measurement of implemented IT controls (e.g. ISO 27002). This is, of course, an important and integral part of running an ISMS, but is outside the scope of this paper.

So what does the ISO standard tell us about metrics and measurements requirements?

Measurement requirements are explicitly mentioned in section **9. Performance evaluation,** but the ISO standard has, purposefully, not described concrete measurement points. Deciding exactly what to measure and the critical success factors or measurements goals should be defined by your organisation and should be part of the alignment of the ISMS with business strategies and goals.

Some general thoughts on metrics

A metric can be defined as a system of measurements, for example the temperature scale Celsius provides the metric scale on which measurements can be performed. Other examples include scales such as percentages, numbers, fail/success or maturity scales such as the CMMI or Cobit maturity scale. It can even be as simple as a graduated level of satisfaction scale or colour scales.

Measuring the effectiveness of ISMS processes is measuring how well they perform against a set of predefined goals or targets such as deviations from targets in numbers or percentages or level of satisfaction. The time factor is then added to ensure comparability and to detect changes over time.

The five important ISMS processes

This white paper will focus on five core processes that must be measured in order to maintain an effective ISMS:

- IT and business alignment
- Information security risk management process
- Compliance processes
- Awareness process
- Audit processes

For each of the five ISMS processes, we will define some simple and concrete examples of measurements that you could implement in your organisation with minor customization. The overall goal is described in the beginning of each section along with examples of targets, findings and action plans.

What are the benefits of measuring?

- It provides input for better alignment with business strategy and is the basis for reporting to relevant internal and external stakeholders.
- The effectiveness of processes and IT controls are documented and success criteria are met.
- Trends that could lead to major non-conformities over time can be detected in time and dealt with (avoided or consequences reduced).
- Helps justify costs associated with the ISMS and implemented IT controls.
- Enables management oversight of our ISMS.
- Provides input as to where to improve or redesign the ISMS processes or redesign IT controls if they are over-performing, not working as intended or not addressing identified risks.

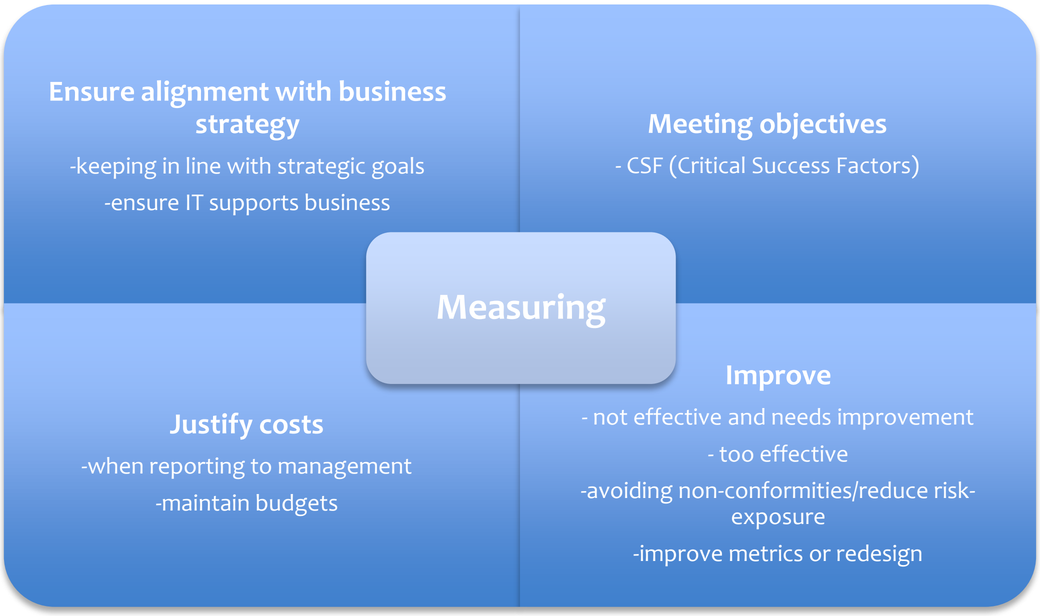
Ensure alignment with business strategy
-keeping in line with strategic goals
-ensure IT supports business
Meeting objectives
- CSF (Critical Success Factors)
Measuring
Justify costs
-when reporting to management
-maintain budgets
Improve
- not effective and needs improvement
- too effective
-avoiding non-conformities/reduce risk-exposure
-improve metrics or redesign

Figure 2: Purpose of measuring

Measurement process and basic requirements

In order to build a metric, we need to define the process including scope, ownership, targets and how the results are documented and used.

- All implemented ISMS processes and relevant IT controls should be measured in some way, whether they are grouped or measured individually.
- All measurements should have a defined purpose and output that is measurable and comparable over time. These provide indicators to the effectiveness of your ISMS processes and implemented controls.

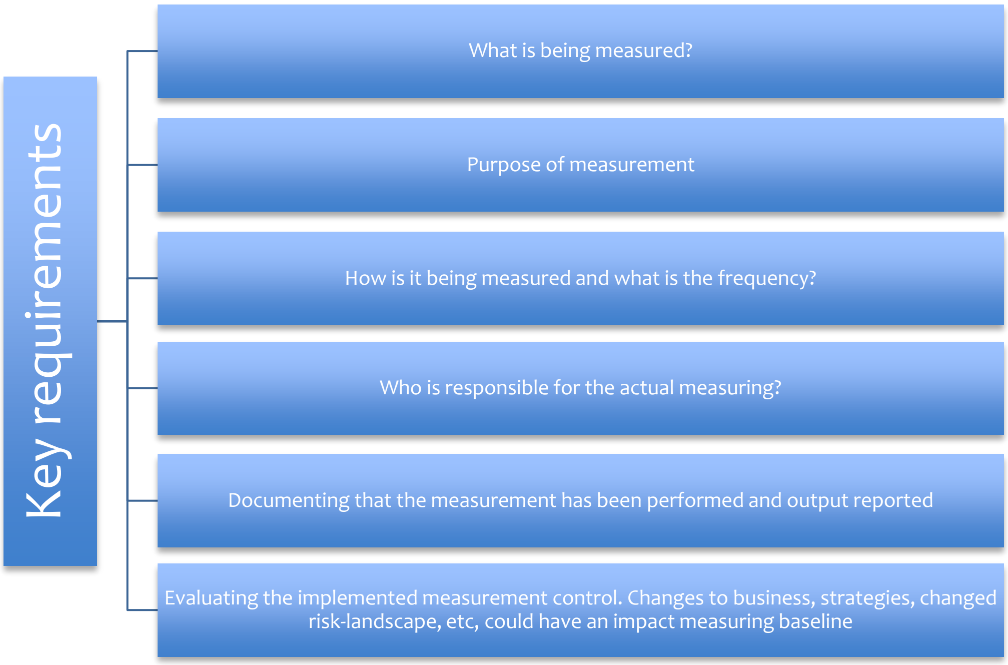
Key requirements
What is being measured?
Purpose of measurement
How is it being measured and what is the frequency?
Who is responsible for the actual measuring?
Documenting that the measurement has been performed and output reported
Evaluating the implemented measurement control. Changes to business, strategies, changed risk-landscape, etc, could have an impact measuring baseline

Figure 3: Anatomy of measurement

Suggested measurement points

The below mentioned measurement points are useful examples. **Targets, Findings** and **Action plans** vary in particular from company to company, but we have provided some examples to give an idea.

IT and business alignment

How do we ensure that the information security strategy and implemented information security processes are adequately supporting and taking into account the needs and requirements of business strategies and goals?

We can ask ourselves the following questions:

- Are the information security strategy and IT services bringing value to the business?
- Is management committed to ensuring continuous input to information security strategies and IT services?

Measurement	Targets	Findings	Action plans
% of business strategic goals and requirements supported by information security strategic goals and decisions. **Method/sources:** Review business strategic decisions and ensure that they have been risk-assessed in relation to IT and information security issues. Likewise all major information security strategic decisions should be reviewed and approved by upper management to ensure alignment with business services and strategies.	**Target** All business decisions need to be supported by IT decisions and specifically information security issues. If not relevant, this needs to be documented and approved as part of the project phase. **Finding** Our latest outsourcing and IT procurement decisions have not been aligned with our IT strategy and specifically not with information security requirements. **Action plans** Ensure that IT requirements are mandatory on the agenda and all relevant information security requirements and potential issues are identified and addressed.		

Level of business (stakeholders) satisfaction with offered information security services and internal support. Does information security bring value to the stakeholders? **Method/sources:** Data collected through interviews or survey forms sent to relevant stakeholder of each business unit, business process or similar.	**Target** Our baseline is above average e.g. high level of satisfaction with offered information security services (scale going from low over medium, high, to excellent). **Finding** Compared to last year we have increased the level of satisfaction from medium to high. **Action plans** No action plans
Percentage of executive management roles with clearly defined accountability for information security decisions. **Method/sources:** Review job roles and descriptions to ensure that responsibility and accountability has been defined and communicated.	**Target** It's important that management and, in particular, business unit owners and IT-systems owners have clearly defined roles and accountability. We are planning to increase the numbers from 50% to 80% this year and next year ensure 100% coverage. **Findings** We are on target this year with 85 % **Action plans** No action plan
% of changes to the information security strategy that is approved by management. **Method/sources:** Review current information security strategy or major information security strategic decisions and ensure that management has formally approved them.	**Target** All information security strategic decisions need to be approved by management. **Findings** Some IT-strategic decisions to outsource critical IT-systems during 2013 were not risk assessed or approved by management. **Action plans** Ensure that all major IT-strategic decisions are management approved. Establish some baseline requirements for management approval. For example: • Critical IT-services • Sensitive data? • Specific information security issues • Budgetary scope • Conflicts with business strategies

Information security risk assessment

Questions we should ask could be:

- Are the IT risk processes addressing all relevant business risks?
- Does the business feel that their risk-input is being covered?
- Is the risk management process being carried out in a structured manner?

We also need to be able to ascertain how effective we are at treating identified risks, and how our risk posture changes over time. This includes identifying changes to risk patterns.

Measurement	Targets	Findings	Action plans
% of business processes and their-services covered by the risk management process. **Method/sources:** Interviews and correlation with management.	**Target** Depending on current maturity level of an organisation it could be all or only some of the business processes/IT-services. Extending coverage could be part of a maturity process. Target this year has been 50%. **Findings** Four critical business processes have not been subjected to a BIA (40%). **Action plans** We need to find out if it's a resource problem or poor risk planning.		
Number of approved risk treatment plans actually being implemented compared to last risk assessment. **Method/sources:** Correlate with previous risk assessment reports.	**Target** We need to ensure that proposed and approved risk treatment plans are carried through and not forgotten or "saved for later". **Findings** Only 60% of the approved action plans have been implemented this year. This is a drop on 20% compared to last year. **Action plans** We need to analyse what went wrong. Is it a financial issue, lack of ownership or other factors?		

Are significant organisational or technological changes being reflected in the latest risk assessment? **Method/sources:** Interview and review of risk assessment reports.	**Target** All major technological shifts (IT-procurements, investments, outsourcing, etc.) need to be reflected in the IT-risk assessment. **Findings** Our use of cloud outsourcing services and the approval of BYOD has been included in the IT-risk assessment. **Action plans** None
% of IT budgets used to manage IT risk management processes. *This requires information security spending to be documented.* **Method/sources:** Correlate total man-hours spent on risk assessment process with total IT-budget.	**Target** Target could be just to track spending on IT-risk management processes. The metric doesn’t necessarily need to define a maximum % of IT budget or information security budget. **Findings** Budgets and time spend on the IT-risk assessment process have increased 15% since last assessment. **Action plans** Further analysis needs to be done. Causes can range from: • Changes in the methodology • Resource issues • Increase in number of identified risks (correlate with other metrics)
Number of new threats and risks identified compared to previous risk assessment. **Method/sources:** Compare total numbers of risks/vulnerabilities, and/or criticality level with previous IT-risk assessments.	**Target** We need to reduce our risk posture and ensure that prior risks and vulnerabilities don’t reoccur. **Findings** The total number of critical risks/vulnerabilities is slightly increasing, but the number of recurrent risks/vulnerabilities has decreased, which indicates that we have effectively addressed prior IT-risk assessment identified risks. **Action plans** Further analysis needs to be done. Causes can range from: • Changes in the methodology • Resource issues • Increase in number of identified risks (correlate with other metrics)

Tracking changes to risk appetite. Does it increase or decrease? Can we correlate it to strategic, organisational or financial decisions? **Method/sources:** Look at changes to risk threshold. Arguments for rejections and approvals of action plans would also be a source. Correlate that with strategy changes, technology changes, security incidents, organisational changes, etc.	**Target** Changes to risk appetite should be recorded as part of management reporting along with explanation of possible reasons. **Findings** Our risk appetite has decreased this year compared to last year. **Action Plan** Analyse why risk appetite has changed. Is this expected?
Level of satisfaction with risk outcome from business perspective. This could be the risk outcome from the BIA, vulnerability assessment or action plans. The business needs to review the quality and output of the BIA to ensure data is correct. Measurement scale: not satisfied, acceptable or very satisfied. **Method/sources:** Interviews or self-assessment questionnaire.	**Target** We need a high level of satisfaction (very satisfied) with the risk results from the BIA's and vulnerability assessments. **Findings** Input from business owners, system owners and IT operations suggest that the results were not aligned with their expectations. There were too many errors in the assessments and especially in relation to the maturity assessment of IT-controls. **Action Plan** We need to ensure that the people performing the risk assessment are adequately competent and internal review of results must be done before final reporting.

Compliance

Questions we should ask could be:

- Are we sufficiently compliant with our information security, privacy, governance and related obligations?
- Are the costs associated with achieving and maintaining compliance less than the business benefits (not just avoided penalties, but the brand value of being seen to do the right thing)?
- Are we successfully managing the risks of being caught out, for example due to non-compliance incidents, or negative compliance assessments, or failing to appreciate new or changing compliance obligations?

Effectiveness of the compliance processes can include assessing if we are addressing non-compliance issues effectively and efficiently, what financial costs are associated with driving the compliance process, the extent of management understanding, support, commitment, etc.

Measurement	Targets	Findings	Action plans
Number of non-compliance issues and derived costs per year (e.g. external requirements, policies and procedures) **Method/sources:** Reviewing end-of-year reported incidents including major external audit findings	**Target** No major non-compliance issue with either financial or image impact. **Findings** We had a data breach by our outsourcing vendor **Action plan** Review relevant IT-security processes and vendor contract.		
Time between identification of non-compliance and implementation of fixes. *Helps identify problems with the efficiency of the compliance process.* **Method/sources:** Correlate time of reported non-compliance issues of security incidents with actual implementation time.	**Target** Depending on the complexity, the issue needs to be addressed within two working days. **Findings** We had two incidents that still haven't been resolved. **Action plan** We need to evaluate the effectiveness of the internal compliance department. Do we need to restructure the process? Are there any resource constraints or internal opposition?		

Costs for fixing non-compliance issues such as administrative work in relation to fixing the problems (process optimization, procedures, policies or IT controls). **Method/sources:** Review total costs associated with fixing non-compliance with annual IT-budget.	**Target** Under normal circumstances, there is a maximum of 20% of IT-budgets allowed for addressing security related issues. **Findings** Costs relating to non-compliance issue exceed the 20% limit. This includes performing a new pen-test and reworking of policies with the assistance of external consultants. **Action plan** Has a business case and cost-benefit analysis been performed? Who has reviewed and approved the spending?
Total costs due to reputational loss, financial fines, loss of clients, etc.) Per compliance incident. **Method/sources:** Review total impact costs associated with compliance issue. *For many companies this can be hard to quantify, so often it focuses on impact on reputation and loss market edge.*	**Target** Recording the total cost and comparing this with last year. The target is not to have an increase in costs, but a decrease. **Finding** Total cost associated with this year's compliance incidents has decreased by 15 % and there was 1 less incident. **Action plan** None

Awareness

It's important to ascertain the awareness efforts are based on "real issues" identified in the organisation or current security trends that are relevant.

- How do we make sure that the awareness efforts reach the relevant stakeholders/employees?
- Have they learned something?

One the goals of awareness is to ensure that employees behave more securely and do not inadvertently expose the organisation to risks
We also need to be able to validate that the results from awareness efforts are used to improve our security posture.

Measurement	Targets	Findings	Action plans
% deviation when comparing established success factors for awareness campaigns with the results of implemented campaigns. **Method/sources:** Comparing results from awareness/training program with results of physical audits or employee quizzes/tests.	**Target** The goal was to ensure that minimum 80% completed the test/quiz following the campaign. Physical inspection of work areas shows a significant decrease in physical sensitive work paper, unlocked workstations, USB devices, etc. **Findings** Less than 60% answered correctly on the mobile device policies and use of cloud-services. During our internal audit, we discovered unlocked workstations and customer-sensitive documents lying in the printer room. **Action plan** We need to re-evaluate the way we present the message. Perhaps we can make it more story-driven and be better at using the intranet.		
Are awareness plans/strategies/sessions/courses, etc. aligned with information security risks currently of concern to the organisation? **Method/sources:** Correlate awareness/training programs and strategy with current risk posture (results from risk assessment, external requirements, security incidents, technological changes, audits, etc.).	**Target** There needs to be a direct link between focus-areas of awareness/training and current risk posture. **Findings** The awareness strategy has been arbitrarily chosen more based on security trends and media talk than actual risks relevant to the organisation. **Action plan** We need to ensure that it's derived from relevant risks to our organisation.		
% of IT users who have visited the security awareness intranet site so far this month. **Method/sources:** Document the monthly visit rate on the information security section of the intranet.	**Target** Our average visit rate must not fall below 70%. **Findings** The last update with the malware alert was seen by 90% of IT-employees. **Action plan** None		

Cost-effectiveness of the awareness and training program *E.g. can we detect a reduction in security incidents with financial impact, impact to intangibles (image/reputation).* **Method/sources:** Compare security incident before/after awareness/training efforts. This could also include physical observations of related employee behaviour, number of support calls or input from network security (IDS, IPS, content filtering or policy violations). **Other sources:** Results from audits.	**Target** We must be able to detect a reduction in security incidents following our awareness/training programs. (Awareness programs run in January and measurements in winter). **Findings** All approved follow-up plans have been implemented. **Action plan** None
Retention of key awareness messages % of employees that remember awareness messages. Can be measured by doing tests/quizzes on prior awareness campaign themes. **Method/sources:** Compare results of tests performed a short time after completion to test run after a longer period of time e.g. 2-6 month.	**Target** Success rate of 60% of employees remembering prior awareness/training themes. **Findings** The knowledge of the topics drops dramatically after 6 months, compared to tests run after completion of awareness training. **Action plan** We need to maintain awareness and knowledge on important security themes by increasing the frequency of awareness initiatives.

Audit process

As well as ensuring that the internal audit is performed in a structured manner, we also need to identify how the security posture is changing over time and our effectiveness rate in relation to mitigation efforts stemming from audit observations.

Is spending used to addressing non-conformities reducing the amount of non-conformities and security incidents?

It's also important to review audit results over time to ensure that audit scope is directly correlated to actual risk posture and to ensure that high-risk areas are addressed and areas with few or no critical observations are scoped out.

<table>
<tr><th>Measurement</th><th>Targets</th><th>Findings</th><th>Action plans</th></tr>
<tr><td>% of critical observation compared
to last audit. E.g. as shown per audit area or location.
What are the trends when comparing data to prior audits?

<b>Method/sources:</b>
Compare number of critical observations. Examples could be priority 1 and 2 observations and CVSS score above a defined threshold.</td><td colspan="3"><b>Target</b>
A reduction in numbers of critical observations and no recurring critical observations.
<b>Findings</b>
This year's critical observations are identical to prior year's observations. In addition, the UK location and software development processes have seen an increase in observations.
<b>Action plans</b>
We need to ensure that critical observations are being addressed. We need better management backing and budgetary support for fixing the critical observations.

We need to take a look at the related IT-processes and see where they are broken.</td></tr>
<tr><td>% of agreed upon critical observations being
addressed with an action plan.

<b>Method/sources:</b> Compare the numbers of approved critical observations with actual suggested action plans.</td><td colspan="3"><b>Target</b>
The target rate is 100%. All critical observations must be formally reviewed along with suggested action plans and required efforts (workload and budget estimates).
<b>Findings</b>
We have ascertained that only 70% of critical identified observations have been addressed in an action plan.
<b>Action plans</b>
The audit process needs to be reviewed. There needs to be a formal review (control) done by Information Security or the audit committee to ensure that all critical observations are being addressed with mitigating efforts.</td></tr>
</table>

Amount of resources allocated to address critical observations e.g. time, money and manpower. **Method/sources:** Compare total amount of resources spent on addressing critical observations. This could be compared with prior year's spending. Does money spent pay off with fewer audit observations or fewer security incidents?	**Target** Unless we have major changes in our infrastructure, spending to address observations should be maximum 10% of our IT budget. **Findings** Resource spending has risen by 15% since last year, but that is expected because of the technological investments and change of ERP system. **Action plans** No action plans needed.
Extent and significance of changes brought about as a direct result of audits. **Method/sources:** Indicators that could be included include: Perceived reduced risk exposure from IT-risk assessments, trends in relation to security incidents and cost savings.	**Target** We need to be able to detect the value provided to the business as a result of audits. As well as the mandatory requirements for audits, they also need to bring value to the business. **Findings** Output from audit processes has provided input on how to manage our IT-processes more effectively. This includes better management of change processes, ensuring backup strategy is aligned with business requirements and implementing a risk-based approach to vendor management. **Action plans** No action plan needed

Consolidating the results and some thoughts on how to get started

Typically, big companies in the manufacturing, telecom or hosting industry are highly dependent on measuring processes and service levels, whether it's LEAN, ITIL, ISO 9001 or similar. These measurements are often semi-automatic and are consolidated in a dashboard-like reporting tool.

ISO 27001 does not require the use of a dashboard tool. This would be a natural evolvement when a company has reached a certain maturity and has been through a series of continual improvement iterations.

We recommend that you begin by selecting a couple of measurements from each process, and incorporate those as a part of your IT organisation's work-routines.

The collection of output from the selected ISMS processes can easily be done in a spreadsheet or similar and consolidated for use in management reporting.

Our examples serve as inspiration and can, with a little modification, be applied to most organisations that have incorporated all or some of the 5 ISMS processes we have looked at.

It's important to remember that for many organisations, an ISO 27001 certification will never become relevant and, with that in mind, the ISO 27001 standard would instead serve as an inspirational catalogue for better IT security governance.

References

Cobit:
http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx

SANS.org *"Gathering Security Metrics and Reaping the Rewards":*
http://www.sans.org/reading-room/whitepapers/leadership/gathering-security-metrics-reaping-rewards-33234?show=gathering-security-metrics-reaping-rewards-33234&cat=leadership

BSI group *"Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001"*:
http://shop.bsigroup.com/upload/Shop/Download/Books/BIP0074sample.pdf

KPI library:
http://kpilibrary.com/

SmartKPIs:
http://www.smartkpis.com/

NIST publication 800-55 *"Performance Measurement Guide for Information Security"*:
http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

DIVA -Academic Archive On-line *"Information Security Metrics – State of the Art":*
http://www.diva-portal.org/smash/get/diva2:469570/FULLTEXT01.pdf

Thanks to Gary Hinson for his contribution on measurement points.

SecureAware®

SecureAware® ISMS

SecureAware from Neupart helps your organisation spend less time on IT Governance, Risk and Compliance management while allowing you to optimize your information security and achieve continuous compliance with common security standards and regulations.

SecureAware is an all-in-one information security management system (ISMS) that manages policies, IT controls and risk information. It is offered as a complete ISMS, or as individual modules to best meet your needs.

Get more information and a free trial here: www.neupart.com/products

Key features

- ISO 27001 Information Security Management System (ISMS)
- IT risk management in accordance with ISO 27005 and NIST SP 800-39
- Statement of Applicability
- Management and communication of company policies
- Compliance with security regulations and known standards, e.g. ISO 27001/2, EU Data Protection Regulation and PCI DSS
- Business Continuity Planning
- Continuous improvement processes
- Ready-to-use content templates for security policies, business continuity plans and threat catalogue
- Compliance and security task management
- Cloud vendor analysis based on Cloud Security Alliance GRC Stack
- Active directory user management
- Delivered as a software solution or as a service

Neupart, an ISO 27001 certified company, provides an all-in-one, efficient information security management SecureAware® solution allowing organizations to automate IT governance, risk and compliance management. Whether you need to manage evolving business risks or achieve continuous compliance with ISO 27001, EU Data Protection Regulations, PCI DSS, Cloud Security Alliance Control Matrix, or WLA SCS, Neupart allows you to respond effectively. More than 200 organisations worldwide are Neupart customers, including governments, utilities, banks, insurance firms, IT service providers and lotteries.

Neupart A/S
Hollandsvej 12
DK-2800 Lyngby
T: +45 7025 8030
www.neupart.com