SAFE AND OPEN
HIGHER EDUCATION

Manual: Integrated Safety and Security Management System Higher Education (MISH)

Table of Contents

0 Introduction

0.1 General

This standard applies to research universities and universities of applied science.
The fact that 'managing' integral safety and security is on the agenda of the Executive Boards of higher education institutions follows directly from the sector codes of both the Association of Universities in the Netherlands (VSNU) and the Netherlands Association of Universities of Applied Sciences (VH). In a nutshell, managing integral safety and security means making well-considered choices in dealing with risks (and implementing those choices accordingly). This standard focuses on those aspects.

Apart from sector codes, the management of an institution simply has a duty towards its stakeholders to ensure the continuity and continued existence of the institution. Proper risk management brings this within reach.

Against this background, this standard serves as an action framework that can be used by the institution's management for planning and decision-making purposes in preparing for (if possible: preventing) and responding to disruptive incidents (an emergency situation, a crisis or a disaster).

This standard increases the institution's ability to manage and recover from a disruptive incident and sets out all the necessary measures to continuously ensure the viability of the institution.

This standard (section 4 et seq.) essentially sets out generally verifiable criteria for establishing, auditing, maintaining and enhancing a management system to improve prevention, readiness, mitigation, response, continuity and recovery from disruptive incidents. The implementation of any management system requires the necessary time and sufficient management attention and engagement. There is no point in demanding that such a system be fully implemented at once. The system's organic growth is usually expressed in stages of maturity:

1. *Unpredictable* Problems can only be resolved after they have arisen. Processes have a chaotic or ad-hoc nature.
2. *Repeatable* Decisions are taken on the basis of experience. The institution's level of professionalism is reflected in the fact that it applies previously acquired knowledge to the development process (by implementing project management, for instance).
3. *Defined* The most important processes have been standardised.
4. *Controlled* The quality of developments is measured so that adjustments can be made.
5. *Optimised* Risk management runs like a well-oiled machine and all that remains is the fine-tuning (dotting the i's and crossing the t's).

Determine where the institution stands in terms of integral safety and security and when you plan to reach the next level.

0.2 Process approach

A management system facilitates the analysis of both the institution's and other stakeholders' requirements and defines the processes that contribute to the institution's success. A management system provides a framework for the continuous improvement of safety, readiness, response, continuity and resilience. It instils confidence in the institution and its 'customers' when it comes to the institution's ability to create a safe environment that can meet the institution's and stakeholders' requirements.

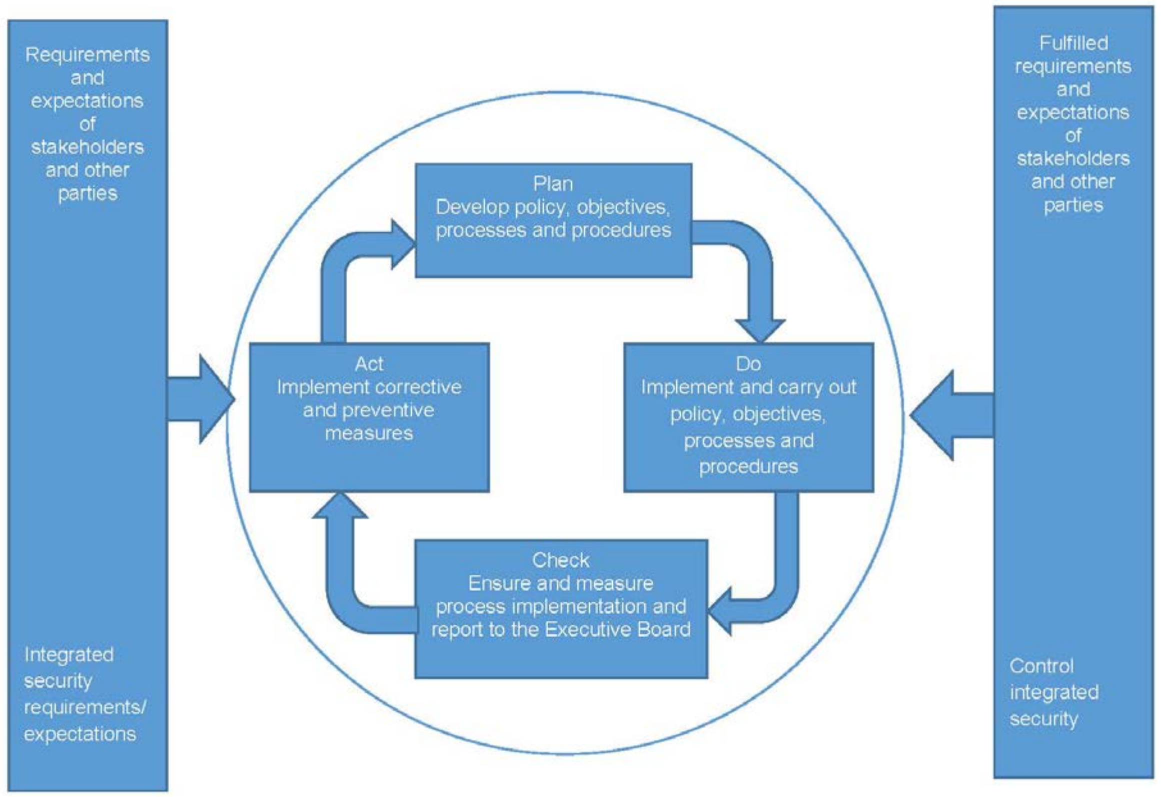
This standard adopts a process approach in determining, implementing, executing, monitoring, assessing, maintaining and continuously improving (the level of) integral safety and security. An institution needs to identify and manage numerous activities to operate effectively. Any activity that consumes resources and converts inputs into outputs in a controlled manner is deemed to be a process. The output of a process will often be used as input for a following process.

The use of a whole system of processes within an institution, combined with identification of the processes and how they are managed, is deemed to be a 'process approach'.

The process approach applied to the management of integral safety and security in higher education institutions (MISH) as described in this standard challenges users to highlight the importance of the following:

a. understanding the institution's requirements relating to:
i. risks;
ii. safety;
iii. integrity (vision, norms and values, rules and procedures, human resource policy and staff culture, incidents and enforcement, monitoring and accountability, organisation and safeguarding);
iv. privacy;
v. the safety chain (proaction, prevention, preparation, repression and aftercare);
b. defining a policy and objectives for managing risks;
c. implementing measures to manage the institution's attendant risks in the context of the institution's mission;
d. monitoring and assessing the implementation and effectiveness of MISH;
e. continuous improvement based on objective measurements.

This standard uses the 'plan-do-check-act' (PDCA) model. The accompanying diagram illustrates how MISH uses the institutional requirements for integral safety and security and stakeholders' expectations as input, and through a series of processes generates output that meet the requirements and expectations.


Requirements and expectations of stakeholders and other parties
Integrated security requirements/ expectations
Plan
Develop policy, objectives, processes and procedures
Do
Implement and carry out policy, objectives, processes and procedures
Check
Ensure and measure process implementation and report to the Executive Board
Act
Implement corrective and preventive measures
Fulfilled requirements and expectations of stakeholders and other parties
Control integrated security

Plan
Develop MISH policy, and the objectives, processes and procedures required for integral safety and security and to achieve results in line with the institution's overall policy and objectives.

Do
Implement MISH policy, the measures, processes and procedures and ensure they are actually followed.

Check
Monitor and measure the execution of the processes, against integral safety and security management policy, the objectives and practical experiences. Report the findings to executive management for their review.

Act

Carry out corrective and preventive actions, based on internal audits and the management review, thereby ensuring continuous improvement.

0.3 Contributions

Numerous parties contributed to the development of this standard, including Carla van Cauwenberghe (the Dutch Inspectorate of Education), Beer Franken (Academic Medical Center), Paul Goossens (Rotterdam University of Applied Sciences), Peter de Groot (Avans University of Applied Sciences), Aldert Jonkman (Netherlands Association of Universities of Applied Sciences) and Michael Mehrow (Windesheim University of Applied Sciences).

1 Scope

This system of standards (referred to in this document in shortened form as the 'standard') relates to integral safety and security at higher education institutions and the manner in which the institution's management systematically manages integral safety and security (governance). It therefore provides a framework for designing and implementing a management system for integral safety and security in higher education institutions (MISH).

Furthermore, MISH provides a basis for assessment (based on self-audits, peer reviews and external audits).

The primary target group for MISH comprises Executive and Supervisory Boards.

2 Reference standards

This standard is in line with standards such as:

Dutch standard NEN 7131:2010 Public safety – Safety management systems, preparing for incidents and continuity – Requirements and recommendations for use

ISO 9001:2008 Quality management systems – Requirements

ISO 14001:2004 Environmental management systems – Requirements with guidance for use

ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

ISO 28000:2007 Specification for security management systems for the supply chain

Dutch RJ400 Guideline for annual reporting (Corporate Social Responsibility)

The 2013 Education Audit Protocol (Onderwijscontroleprotocol *2013*) issued by the Dutch Inspectorate of Education (owinsp.nl)

3 Terminology and definitions

The terminology and definitions will be further specified in a following version of this MISH document.[1]

[1] The scope of the constituent project excluded providing definitions for the terms used. However, given the importance of consistency in communication they will be added to a following version

4 Preparation: The institution in its environment

4.1 The institution and its environment

The institution determines the internal and external topics that are relevant to the achievement of its objectives (based on its mission, vision and accountability policy) and influence the intended results of MISH.

4.2 Parties' needs and expectations

The institution determines the following:

– which stakeholders are relevant to MISH;
– what their needs are.

4.3 Scope of MISH

The institution determines the range and applicability of MISH for the purpose of defining its scope. The following aspects should be considered in doing so:
– the internal and external topics stated in 4.1;
– the needs stated in 4.2.

4.4 MISH

The institution will develop, implement, maintain and continuously improve MISH in line with this standard.

5 Leadership

5.1 Leadership and engagement

The institution's executive management will demonstrate leadership and engagement with MISH by:

– ensuring that MISH policy and MISH targets are defined and are in line with the strategic direction of the institution;
– ensuring that MISH requirements resulting from MISH targets are internalised in the institution's normal business processes;
– ensuring that the resources required for MISH are made available;
– communicating the importance of effective MISH and compliance with MISH requirements;
– ensuring that the intended results of MISH are achieved;
– supervising and supporting individuals in contributing to the effectiveness of MISH;
– actively communicating continuous improvement;
– supporting other management levels in demonstrating leadership in their areas of responsibility.

5.2 MISH policy

The institution's executive management defines MISH policy that:

– is in line with the institution's objective;
– provides a framework for defining MISH targets;
– contains a self-imposed obligation to meet the applicable requirements;
– contains a self-imposed obligation to continuously improve MISH.

MISH policy must:

– be available as an officially approved document;
– be communicated across all levels of the organisation;
– be available to stakeholders, where applicable.

5.3 Responsibilities and powers

Executive management ensures that responsibilities and powers are assigned to the relevant roles and are communicated across the institution. Executive management will assign responsibilities and powers aimed at:

– ensuring that MISH meets the requirements set out in this standard;
– continuously keeping informed of the implementation of MISH.

6 Planning process

6.1 Actions focusing on risks and opportunities

The topics stated in 4.1 and the requirements described in 4.2 will be included in the MISH planning process in addition to the risks and opportunities arising when:

– ascertaining that MISH targets are achievable;
– preventing or limiting undesirable activities;
– achieving continuous improvement.

The institution will incorporate the following in the planning process:
– the activities required to manage the risks and opportunities effectively;
– how:
  - o to integrate and implement the activities in MISH processes;
  - o to evaluate the effectiveness of these activities.

6.2 MISH targets and how they will be achieved

The institution will determine MISH targets for the relevant levels and roles.

MISH targets must:
– be consistent with MISH policy;
– be measurable (if workable);
– take the applicable requirements into account;
– be monitored;
– be carried out;
– updated if necessary.

The institution will document information relating to MISH targets.

When planning how to achieve MISH targets, the institution will determine:

– what must be done;
– what resources are needed;
– who is responsible for carrying out the activities;
– when the activities must be completed;
– how the results should be assessed.

7 Support

7.1 Resources

The institution will determine and make available the resources needed to develop, implement, maintain and continuously improve MISH.

7.2 Competencies

The institution must:
– define the required competencies of the staff under its authority which (could) influence the implementation of MISH;
– ascertain that these individuals are competent on the basis of their education, training and/or experience;
– take action, if applicable, to ensure staff acquire the required competencies and to evaluate the effectiveness of the action taken;
– retain relevant documentation on file as proof of competence.

7.3 Awareness

Individuals who perform activities under the authority or instructions of the institution must be aware of the following:
– MISH policy;
– the contribution they are expected to make towards the effectiveness of MISH, including the benefits arising from improving the performance of MISH.
– the consequences of non-compliance with the MISH requirements.

7.4 Communication

The institution must determine the need for internal and external communication which is relevant to MISH, including:
– the information to be communicated;
– when the information should be communicated;
– to whom the information should be communicated.

7.5 Documented information

7.5.1 General

The institution's MISH system must at least comprise the following:
– the mandatory documented information pursuant to this standard;
– the documented information deemed necessary by the institution for the effectiveness of MISH.

7.5.2 Producing and processing

When producing or processing documented information, the institution will provide for the following, if applicable:
– identification and a description (e.g. title, date, author or reference number);
– the format (e.g. language, software version, diagrams) and media (e.g. on paper or electronic);
– assessment and approval in terms of suitability and adequacy.

7.5 3 Document management

The documented information required by the MISH system or this standard must be managed to ensure that:
– it is available and suitable for use, at the time and place where it is needed;
– it is sufficiently secure (e.g. against breaches of confidentiality, improper use or loss of integrity).

For the purpose of managing the documented information, where applicable, the institution will identify the following activities:
– distribution, access, requests for documented information and use;
– storage and retention, including the preservation of readability;
– management of changes to the documented information (e.g. version management);
– retention period and destruction.

8 Do: Operating effectiveness

8.1 Operational planning process and management

The institution must plan, implement and manage the necessary processes to meet the requirements and to implement the actions defined in 6.1 by:
– defining the criteria for the processes;
– implementing management of the processes in line with the criteria;
– keeping documented information up to date where necessary to be confident that the processes have been carried out as planned.

The institution will manage the planned changes and assess the consequences of unplanned changes, thereby taking action to mitigate the negative consequences, if necessary. The institution will ensure that any outsourced processes are managed.

9 Check: Evaluation of the operating effectiveness

9.1 Monitoring, measurement, analysis and evaluation

The institution determines the following:
– what must be monitored and measured;
– the monitoring, measurement, analysis and evaluation methods for ensuring valid results;
– when to monitor and measure;
– when to analyse and assess the monitoring and measurement results.

The institution will retain the relevant documented information on file as proof of the results.

The institution will assess the implementation of MISH as well as its effectiveness.

9.2 Internal audit

The institution will conduct internal audits at planned intervals to obtain information about whether MISH:
a. complies with:
– the requirements imposed by the institution on MISH;
– the requirements pursuant to this standard;
b. has been effectively implemented and maintained.
The institution will:
a. plan, define, implement and maintain one or more audit programmes, including methods, responsibilities, planning requirements and reporting. An audit programme will incorporate the significance of the relevant processes and the results of previous audits;
b. define the audit criteria and the scope of each audit;
c. select auditors and safeguard the objectivity and neutrality of the audit process;
d. ensure that the audit results are reported to the relevant management;
e. retain the documented information as proof of the audit programme and the audit results.

9.3 Management review

Executive management will assess MISH at planned intervals to ascertain the continuous suitability, adequacy and effectiveness of the system.

The management review will include the following considerations:
a. the status of actions arising from previous management reviews;
b. changes in external and internal matters that are relevant to MISH;
c. information on the implementation of MISH including developments relating to the following:
d. non-conformities and corrective action;
e. monitoring and measurement results;
f. audit results;
g. opportunities for continuous improvement.

The results of a management review will include decisions relating to continuous improvement and the need to make any changes to MISH. The institution will retain the documented information on file as proof of the results of management reviews.

10 Act: Improvement

10.1 Non-conformities and corrective action

If a nonconformity is identified, the institution will:
a. respond to the nonconformity and
– take action to manage and correct it;
– resolve the consequences;
b. assess the need to take action to eliminate the causes of the nonconformity to prevent it from recurring or arising elsewhere, by:
– assessing the nonconformity;
– identifying the causes of the nonconformity;
– determining whether comparable nonconformities have arisen or could arise;
c. implement the necessary actions;
d. assess the effectiveness of each corrective activity;
e. make changes to MISH, if necessary.
Any corrective action taken will be in line with the nonconformity that has arisen. The institution will retain documented information as proof of the following:
– the nature of the nonconformities and the resulting actions taken;
– the results of the corrective actions taken.

10.2 Continuous improvement

The institution will continuously improve the suitability, adequacy and effectiveness of MISH.

Foreword

About this manual
The ‘Integrated Security for Higher Education’ project aims to support higher education institutions with an integrated approach to security issues by combining expertise, acting in concert, and providing resources for monitoring risks and making them manageable in a sustainable way.

The ‘Governance’ sub-project defines a ‘Higher Education Integrated Security Management System’ (MISH in Dutch) as a tool to help structure integrated security. This document is the MISH manual. Institutions can use it to help design their security systems, and it also includes references to useful approaches to various security issues. To this end, a questionnaire is attached that can be used as a self-assessment.

This manual is the first of its kind for higher education, and aims to provide footholds for achieving synergy in security policy through an integrated approach. What stands out straight away is the sheer scope of an institution's security interests. This manual can be seen as a framework that provides references to practical approaches for various sub-areas where synergy can be achieved through an integrated approach. It should also be regarded as an initial document that will gradually take shape as time goes on.

Core elements of a management approach to security.
A management approach to security consists of a number of aspects that function in concert.

<u>Commitment and Vision</u>
Integrated security policy can only succeed if it is considered important, is visibly supported and is allocated sufficient resources by the organisation's management (including upper management). In addition to a desire to move towards integrated security and to express its importance, management must also formulate a clear vision on integrated security and risk management. Key questions in this respect include: why do we want to focus on integrated security? What do we think it is, and what are our objectives?

<u>Standards and Values</u>
Standards and values form the entirety of an organisation's written and unwritten rules that define what it and its employees stand for, and where their accountability lies. They form the basis of integrated security policy, including the integrity policy.
Relevant questions in this respect include: ‘Is this possible?’, ‘Is this permissible?’ and ‘Is this what I want?’.
It is important to set out an organisation's standards and values in a code of conduct. Relevant topics that may be covered include: core values, general regulations applicable to common security and integrity issues (e.g. fraud, conflicts of interest, academic integrity, knowledge security and information security), and where staff and students can go with concrete questions. How does the executive ensure a safe environment for students and staff? How do managers set an example in their conduct, and how do executives prevent over-regulation without compromising on appropriate alertness levels in relevant cases, or losing the ‘sense of urgency’ when dealing with incidents?

Regulations and Procedures

Standards and values are given concrete implementation through the sum total of an organisation's official rules and procedures, and are reflected in internal Administration and Internal Control. Important topics in this respect include: setting up internal supervision and audit systems, describing work processes and risk-management measures (such as the four-eyes principle), segregation and rotation of duties, board and management regulations, current laws and regulations (Social Assistance Act, Higher Education and Research Act, etc.) sector codes and codes of conduct, and the Students' Charter. Another relevant point concerns the regular verification of whether existing regulations and procedures are functioning properly and achieving their desired outcomes, to avoid any surprises when they need to be called upon. Effectiveness, after all, is related to integrality.

HR policy and culture

Attention to integrated security (which includes integrity) is a key component of HR policy, and comes into play even during the initial recruitment and selection of staff. Is screening necessary, and if so, to what extent? Integrity is also a topic that should be covered in various staff interviews (e.g. annual plans, and progress/performance/exit interviews). Oath-of-office sessions, introductory meetings, direct employee consultations and integrity workshops are also ideal times to work on improving organisational culture and employee awareness. In organisations, it is a question of culture.
Awareness of security risks in higher education is a matter that concerns all stakeholders, executives, staff and students.

Monitoring and Reporting

It is essential to monitor integrated security policy in order to safeguard the progress and performance of the integrated risk management system. Based on the monitoring data, the management can monitor whether the set goals are being met, or whether additional action is necessary. Incorporating interim evaluations will not only give the organisation an idea of the measures' effectiveness, but also allows for their improvement. Evaluations and reports are forms of management information and management accountability concerning the implementation and effectiveness of integrity policy.

Incidents and Enforcement

Values, standards and regulations are only worthwhile if everyone adheres to them. Addressing any breaches will demonstrate the value attached to compliance and exemplary behaviour (i.e. ethical conduct). It affirms the existing standards and reduces the risk of future violations. Setting up an enforcement policy that includes regulations governing the investigation, sanctioning and communication of any suspected/observed abuses, and detecting risks and making them manageable, are essential components of integrated security policy. Provisions that facilitate dealing with incidents (such as notification regulations, confidential counsellors and investigation protocols) are part of integrated risk management for security issues within research universities and universities of applied sciences.

Organisation and Safeguards

Any focus on security issues in higher education (including integrity and information/knowledge security) must be cohesively and sustainably structured and safeguarded within the organisation. Executives are jointly responsible for the results of their own institutions, which not only means that education and research must deliver quality, but also that financial and supporting systems need to be in proper order. Higher education is part of the public domain and has an obligation to society, part of which includes openness, transparency and – as administrators – being in control in all areas. Attention to integrated security and ethical administrative conduct are essential.

Further development of this manual

We would like to emphasise that this manual is the first of its kind to be produced for the higher education sector. It has shown that, although there are many useful approaches for certain specific areas of security, there is little available concerning some other areas. We encourage the readers and users of this manual to contribute practical lines of action, e.g. by providing references to practical approaches used by a particular institution that may also benefit other institutions. We can also imagine that certain aspects of the management approach may be further teased out into joint initiatives, giving them further depth and structure. A subsequent edition of this manual will incorporate any such contributions.

On behalf of the project,

Paul Goossens
Integrated Security Manager, Rotterdam University of Applied Sciences

Beer Franken
Chief information security & privacy protection officer, Academic Medical Centre (University of Amsterdam)

How to use this manual

The following three documents were developed in succession, and are interrelated in their use.

1. Higher Education Integrated Security Management System (MISH): the MISH is an example of a practical management system whose structure includes evaluable elements.
2. The present MISH manual: the manual provides methods for setting up the MISH, and covers the various security aspects that affect institutions. It also includes references to various useful approaches.
3. Self-assessment tool: this is a questionnaire that can be used as a self-assessment for MISH.

The sections of the manual correspond to those of the MISH itself; we recommend reading the MISH first, and then the manual. The MISH consists of a number of introductory sections, after which the aspects are covered as part of the 'Plan-Do-Check-Act' cycle.

The manual is also intended to provide an overview of security aspects that may affect institutions. These mostly appear in Section 8 (Effectiveness), Section 9 (Evaluating Effectiveness) and in the appendices (sources of and relationships between threats, interests requiring protection, and security aspects).

11 Introduction

Research universities and universities of applied sciences have a complex obligation to society, performing statutory duties in education, research and knowledge valorisation. They enjoy a considerable degree of autonomy in carrying out their duties, which are mostly performed in large, complex organisations where (sometimes problematic) interests are continually weighed up against one another. Guaranteeing the quality of results and the accuracy of procedures requires checks and balances, which are provided by the Higher Education and Research Act (*Wet op het hoger onderwijs en wetenschappelijk onderzoek*, WHW). Under the WHW the institutional administration – the Executive Board – is wholly responsible for governing and managing the institution. This means that the Executive Board is both *responsible* and *accountable* for the quality of education and research, for compliance with laws and regulations, and for dealing with the applicable sector code to which universities of applied sciences and research universities have committed themselves.

In their various Good Governance Codes of Practice, the Netherlands Association of Universities of Applied Sciences (VH[2]) and the Association of Universities in the Netherlands (VSNU[3]) have reached agreements with their members on what constitutes ‘good governance’ (i.e. adequate management and policy, and effective internal supervision in higher education). The Explanatory Memorandum to the Improved Governance (Higher Education) Act (*Wet versterking besturing*) states that a sector code for good governance increases the social environment's confidence in institutions' performance, and can play an important part in horizontal accountability. A code also provides flexibility and freedom to determine how institutions within a certain sector meet their good-governance responsibilities (other than by statutory means).

Sometimes, incidents or problems occur that put institutions and their security at risk. Education institutions can get into hot water if unjustifiable risks are taken, deliberately or otherwise. Such risks are occasionally underacknowledged due to a lack of expertise, or because they have not been thoroughly assessed. At sector level, education institutions should be expected to share their insights with each other, develop standards and call each other to task on their conduct. The development and application of governance codes plays an important part in strengthening sectors' capacity for self-correction.[4]

As part of the ‘Integrated Security for Higher Education’ project, the higher education sector (in consultation with the sector associations, the ministry and higher education institutions) has joined forces to develop instruments and resources that can be used to support institutions in taking an integrated approach to security risks. Tools and processes are now available, and the time has come to demonstrate that they work (and how), both within individual institutions and in the higher education sector as a whole.

[2] The VH sets compliance with the sector code as a prerequisite for membership, see: http://www.vereniginghogescholen.nl/bedrijfsvoering/goed-bestuur [in Dutch]

[3] See: http://www.vsnu.nl/code-goed-bestuur.html [in Dutch]

[4] See: http://www.rijksoverheid.nl/ministeries/ocw/documenten-en-publicaties/kamerstukken/2013/04/20/kamerbrief-versterking-bestuurskracht-onderwijs.html [in Dutch]

0.1 Higher Education Integrated Security Management System (MISH)

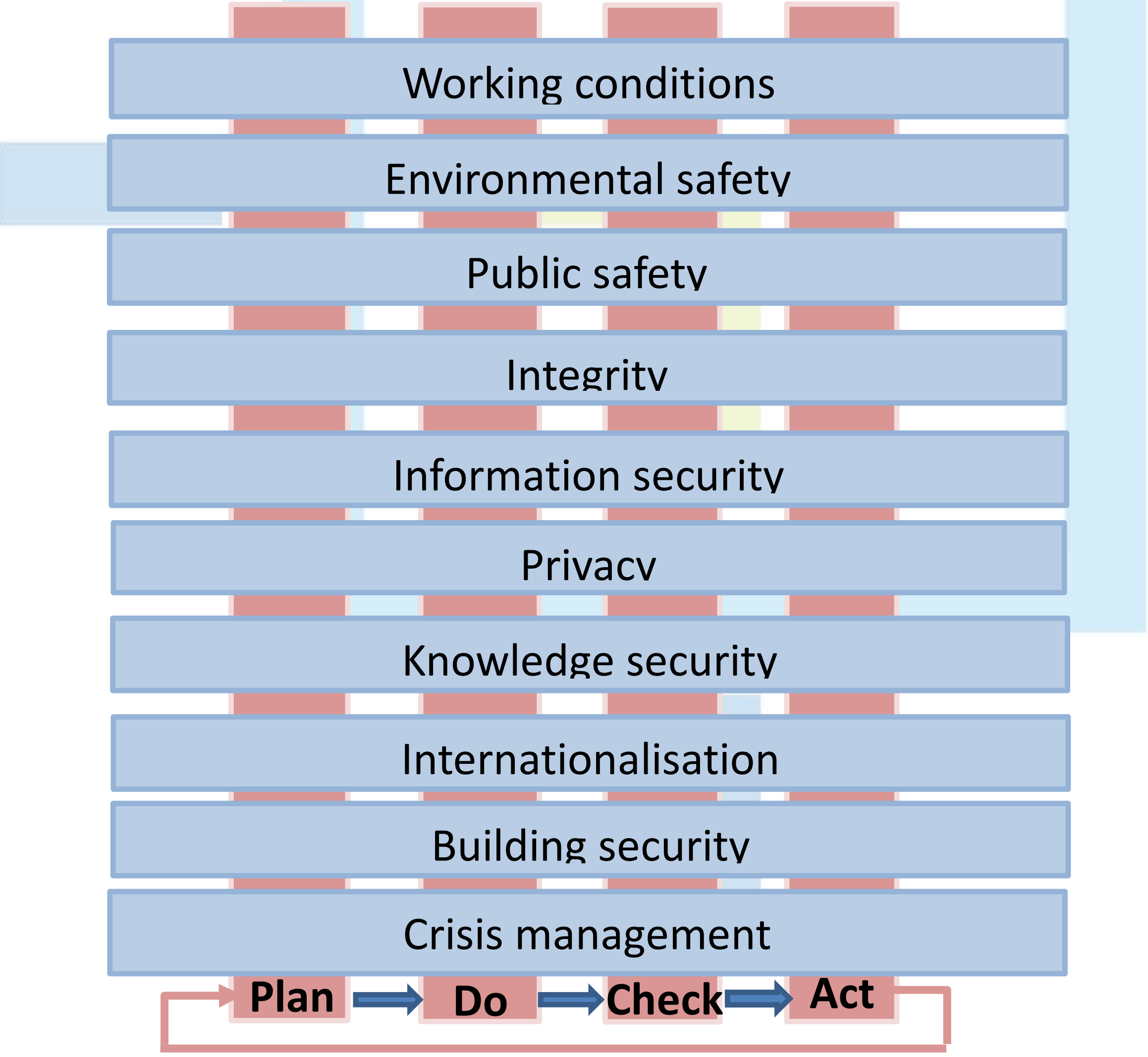
The Integrated Security Project Group has developed a Management System for Integrated Security in Higher Education (MISH) as a means of aiding security management. Although institutions have already achieved much in the field of security, what is generally missing is an overview of the various aspects and the approaches taken. This is the intended purpose of the MISH.

This document is a manual for the MISH, and provides useful tips and references to external standards, resources and consultative bodies relevant to specific security aspects. The sections of the manual correspond to those of the MISH itself.

0.2 Why an integrated security management system?

Various developments in the field of security have shown that the required action can best be taken based on a management system approach. This will encourage forging relevant links between the activities, focusing on targets, enabling accountability towards stakeholders, and a desire to achieve improvement. A common management system approach involves dividing activities into a PDCA (Plan-Do-Check-Act) cycle.

A fragmented approach is frequently taken to security issues. Often incidents and measures take initial priority, and in a later stage the approach focuses more on vision, risk management and the management approach to the particular aspect of security. This may result in the simultaneous existence of multiple management systems for various security aspects within the same institution and no general overview, hindering an approach based on cohesion and synergy.



The MISH was derived directly from ISO's High Level Structure for management systems, and follows the PDCA cycle that is present within all ISO management systems. Various management system standards (as well as institutional standards) can easily be ‘plugged’ into it. From a management perspective, there is a logical need for a single management system that can manage all aspects of security within an organisation.
Different security aspects share common ground and affect one another. Internationalisation, for example, goes hand-in-hand with various security aspects and overlaps with ‘Public Safety’, ‘Knowledge Security’ and ‘Information Security’, but is approached from the perspective of international student, staff and knowledge exchange. Policy regarding all of these aspects must be well-balanced and consistent. The MISH is a resource aimed at managing this consistency.

0.3 Relationship to institutional policy

The Improved Governance (Higher Education) Act (*Wet versterking besturing*) brought about a number of important changes in the Higher Education and Research Act (WHW) in 2010, in particular with respect to the conditions for good governance and a strong legal position for students, promoting quality of education, and the international position of higher education. These changes were implemented with a specific view to putting research universities and universities of applied sciences in a better position to fulfil their obligation to the Dutch knowledge society, as specified in the Explanatory Memorandum[5]. In their respective Good Governance Codes, the Netherlands Association of Universities of Applied Sciences (VH) and the Association of Universities in the Netherlands (VSNU) have set out the agreements with universities of applied sciences and research universities regarding good governance for their members.

In 2013, the VNSU reviewed the ‘Good Governance Code for Universities 2013’ (*Code goed bestuur universiteiten 2013*), which now includes the following with respect to risk management:

2.1.5 The Executive Board will submit the internal risk management and monitoring systems to the Supervisory Board.

Figure 1 Article from Good Governance Code for Universities

In 2013, the VH revised and adopted the ‘Good Governance Sector Code for Universities of Applied Sciences’ (*Branchecode goed bestuur hogescholen*). One addition to the Good Governance Code concerns the Executive Board's obligation to provide an account in the annual report of the effectiveness and key results of the internal risk management system. By adopting the code, universities of applied sciences commit to monitoring compliance on an annual basis, and discussing the monitoring outcomes with the VH. Among other things, the sector code discusses the presence of a risk management system, and reporting via the annual report. The aim is to allow the risk monitoring to be performed in part using the tools provided by Integrated Security for Higher Education. The MISH is intended as one of the various risk-management and control systems available to research universities and universities of applied sciences, and gives executives footholds for guiding security risk management and reporting thereon.

[5] Parliamentary Papers II 2008-2009, 31 821 no. 3, p. 1

II.1.2
The Executive Board is responsible for ensuring compliance with the relevant laws and regulations and for managing the risks associated with performing the university of applied sciences' primary tasks (i.e. teaching, research and knowledge valorisation), as well as the risks associated with other institutional activities.

II.1.3
The Executive Board shall ensure that an internal risk management system tailored to the university of applied sciences is both present and operational. The university of applied sciences must include at least the following instruments in any such system:

a) a description of the key risks inherent to the performance of primary tasks and other institutional activities, and of the control measures designed specifically to counteract them;
b) a Code of Integrity that must be published on the university of applied sciences' website in any event;
c) manuals for structuring financial reporting, budgeting data and the teaching and research quality policy, as well as the procedures to be followed for their creation;
d) a continuity section that uses key financial data to clarify trends in the university of applied sciences' financial position; and
e) a monitoring and reporting system.

II.1.4
In its annual report, the Executive Board must present information on the effectiveness and key results of the internal risk management system.

II.1.5
The Executive Board must ensure that employees are able to report any suspected irregularities of a general, operational or financial nature within the university of applied sciences to the Executive Board's president or his/her delegated officer, without any threat to their legal position. Suspected irregularities pertaining to members of the Executive Board shall be reported to the chair of the Supervisory Board. The whistleblowers' regulations must be published on the institution's website in any event.

II.1.6
The Executive Board must ensure that students and staff are able to report any undesirable behaviour to an officer to be appointed by the Executive Board, without any threat to their own academic career or legal position. The undesirable behaviour regulations must be published on the university of applied sciences' website in any event.

Figure 2 Summary of the Good Governance Sector Code for Universities of Applied Sciences

0.4 Synergy in integrated security

The MISH contributes to an integrated approach to security aspects, which may at first prove subject to neglect. This manual refers widely to standards, resources, good practices, sources of information and consultative bodies which can be put to good use in customising the MISH to specific institutions. This will also reveal the hidden connections between various security aspects, including areas of aspects that are not yet effectively organised.

Once the MISH has been fleshed out with input from the various security aspects, opportunities for synergy will become clear. Steering towards security awareness and knowledge development among a specific target group, for example, could qualify for an integrated approach covering multiple security aspects, instead of the same group being addressed by multiple separate awareness programmes. This is only one example; this kind of synergy can also be achieved via other activities including risk analysis, selection of measures, organisation, implementation, documentation, evaluation and reporting.

0.5 Maturity approach

Management approaches can be implemented with varying levels of integration. When implementing and improving the MISH, it is useful to apply the concept of ‘maturity’: a helpful approach when phasing in the MISH, and one that places an emphasis on the activities that will provide the greatest benefits during each stage of maturity.

An example of the maturity scale is as follows:

Initial Unpredictable (chaotic) and ad hoc. Problems are only addressed once they appear.

Repeatable An acquired level of organisational professionalism (e.g. by implementing project management) that puts previously-gained knowledge to use in development processes. Decisions are therefore made based on experience.

Defined A level at which key processes have been standardised (and therefore also adopted).

Managed Here, the quality of development processes is measured in order to take action where necessary.

Optimized A level at which development processes run like a well-oiled machine, and only fine-tuning is necessary (dotting i's, crossing t's).

This approach can be used to ascertain the current level of maturity regarding integrated security and the various security aspects. Where is maturity disproportionately low compared to the average? Improving these aspects first will provide the greatest benefit. The approach is also useful for boards in determining the MISH objectives. What is the target level of maturity (‘point on the horizon’) and what are the objectives of the MISH for the next one or two years?

A maturity-based approach also requires an auditing model, for which two practical resources are already available:

- SURF has a system of standards and a benchmark model based on ISO27002 for information security, continuity of business data and privacy that gives a clear indication of an institution's level of maturity concerning information security.
- ASIS International has developed a manual and system of standards (including six maturity levels) for the NEN 7131 Organizational Resilience Management System (ANSI/ASIS SPC.4-2012, Maturity Model for the Phased Implementation of the Organizational Resilience Management System).

12 Scope

Security is a broad concept that transects virtually all of an institution's activities. During practical implementation, institutions quickly run up against the question of how to define the different security categories that they identify. This definition must be clearly described in an institution's MISH. The MISH divides the security domain of an institution into the following security aspects: Working Conditions, Environmental Safety, Public Safety, Integrity, Information Security, Privacy, Knowledge Security, Internationalisation, Building Security and Crisis Management.

It is also practical to develop and implement the MISH in a stepwise fashion. It can be implemented and experience gained within a relatively short time; it can then be expanded with a wider scope during a subsequent ‘round’. There are various possible approaches: one way is to start by implementing the MISH for all security aspects at a single location. The experiences at this location can then be employed when rolling out the MISH across the entire institution. Another approach is to first implement the MISH in a number of familiar security areas within the institution, and to add the remaining areas during the following round.

This manual is intended for managers and staff at higher education institutions whose job it is to implement, manage and improve on a range of security aspects. It is the express intent to take an integrated and cyclical approach to the activities relating to these security aspects.

The manual can also offer some support during self-audits and peer reviews – to this end, it can be used to draw up questionnaires.

13 Normative references

The following normative references support the use of this MISH:

- ISO Guide 83 ‘High level structure and identical text for management system standards and common core management system terms and definitions’: a description of the core management system, to which all ISO management system standards are adapted. When updating an ISO management system, the structure of the new management standard is to be adapted in accordance with ISO Guide 83.
- NEN-EN-ISO 19011 – Guidelines for Auditing Management Systems. These guidelines can be used for drawing up and studying, reviewing and auditing the MISH.
- NEN-ISO 31000 Risk management – Principles and guidelines. This is a framework and process description for managing risks, and is intended primarily for the integrated management of various types of organisational risks (enterprise risk management). These principles and guidelines can be applied in order to manage the risks in the MISH.

From a security domain perspective, the following management systems are in line with the MISH:

- NEN 7131 Societal security – Security, preparedness and continuity management systems – Requirements with guidance for use [in Dutch]. This is an ‘organisational resilience’ management system that focuses on security, incident resolution and continuity management.
- ISO 14001 Environmental management systems – Requirements with guidance for use. This is the environmental safety management system.
- OHSAS 18001, Occupational Health and Safety Assessment Series. This is the occupational health & safety management system.
- NEN-ISO 22301:2012-06, Societal security – Business continuity management systems – Requirements. This is the business continuity management system.

- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements. This is the information security management system.

14 Terminology and definitions

Clear communication with stakeholders (both internal and external to the institution) requires concepts to be clearly defined. Usually these concepts are defined in the relevant documentation of the various security aspects.
For integrated management, it can be useful to create and disseminate a centralised list of definitions. Appendix 4 offers a starting point for this purpose.

Preparation

An implemented MISH is ultimately a continuous management process with mechanisms for continually improving the approach taken to security issues. But how to get the cycle rolling? This aspect of the MISH concerns the preparation for its implementation, and consists of the sections titled ‘The institution and its environment’ and ‘Leadership’.

The best way to prepare and guide the implementation of the MISH is to take a project-based approach. In this context, it must be realised that the MISH is a socio-organisational system that must be actively supported by the management, which is only possible if the MISH is closely linked to the organisational and management objectives. It is also important for results to be achieved fast. All management systems are results-based. When choosing the scope of the MISH and setting up the project plan, it must be clear that concrete results will be achieved within a matter of months in terms of improving both the security situation and the MISH methodology. At first it is often useful to implement the MISH in a single organisational unit or for a single process. Based on the initial successes and learning experiences, it can then be implemented on a broader scale. The MISH will also need to be implemented as much as possible by those who are going to work with it the most. This means that team members must be trained in the MISH approach and working method, after which they must transfer it to the risk management of their own processes and security domains. Implementation therefore automatically constitutes awareness and the creation of a support base among MISH stakeholders. An MISH is systematic by definition; an effective MISH will have requirements and objectives that it must satisfy, be consistent, and aim to continually improve security as well as the management system.

15 The institution and its environment

4.1 The institution and its environment

An understanding of one's own organisation and its environment is essential in order to delineate the scope of the MISH and create a business case. Based on this understanding and these documents, the management can then make a decision regarding the implementation of an MISH.

Before actively beginning to generate an understanding of the institution and its environment, a provisional scope for the MISH can be established, i.e. which parts of the institution will/will not be subject to the MISH. Any sections that are outside the scope need not form part of the inventory. Likewise, during the preliminary survey it may turn out that the initial thoughts regarding the scope are not effective. The ultimate scope of the MISH will be confirmed during step 4.3 (Scope of the MISH).

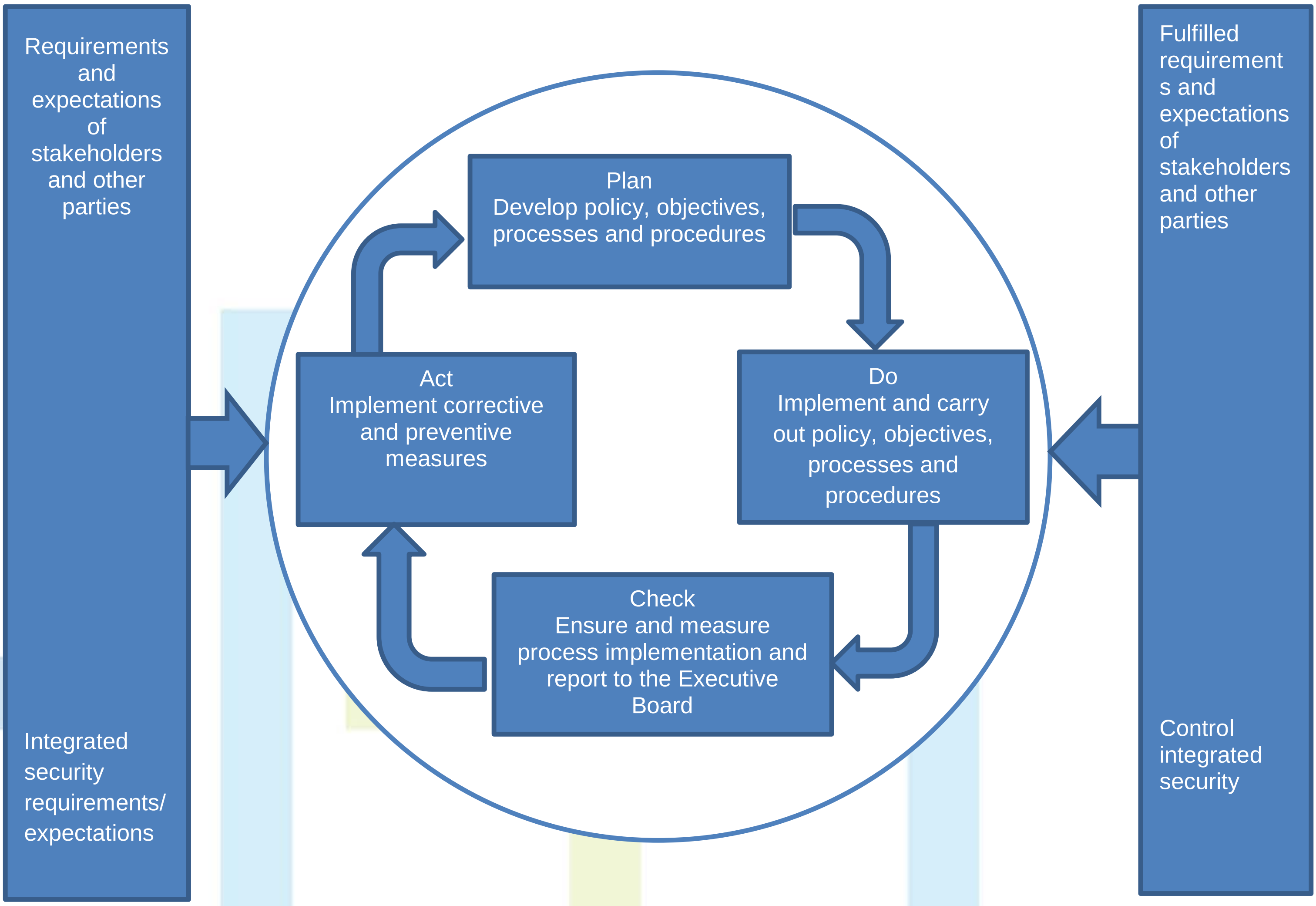
This understanding may be constructed via a preliminary survey, using a GAP analysis resulting in an initial document for decision-making purposes. The purpose here is to review the extent to which current procedures satisfy the MISH criteria. Which security aspects and stages of the PDCA cycle are adequate? Which ones require improvement? The review may consist of interviews, checklists, inspections, audits and measurements.

As a minimum, the preliminary survey should cover policy objectives, operational resources and activities, the institution's products and services and how they relate to the institution's mission statement.
Process dependencies must be clearly evident in each instance, such as energy, ICT, critical resources and suppliers.
Security risks must also be identified; keep in mind that risk categories for non-standard operational situations must also be included. Identify legislative and other institutional obligations, e.g. concerning contract research. Also investigate current risk management practices and procedures (including activities performed by third parties) and their cost levels. Additionally, an evaluation of prior incidents and non-compliance will give insight into the organisation and an idea of the need for certain types of risk management.

Where relevant, the legal, political, cultural, social and economic factors affecting the MISH must also be specified. The essential processes and customers must be made clear, as well as what constitutes normal and extraordinary circumstances and business functions. An overview must be created of potentially disruptive circumstances and incidents. The relationships with key stakeholders must be identified along with their risk perception, and the standards listed that are automatically assumed within the sector.

4.2 Parties' needs and expectations

The MISH aims to provide a response to security expectations. Stakeholders will usually have varying needs, however: an Executive Board will usually want information on compliance, risk-management and cost levels, whereas the needs of individual employees, students and visitors will generally revolve more around public and physical safety.


Requirements and expectations of stakeholders and other parties
Integrated security requirements/ expectations
Plan
Develop policy, objectives, processes and procedures
Do
Implement and carry out policy, objectives, processes and procedures
Check
Ensure and measure process implementation and report to the Executive Board
Act
Implement corrective and preventive measures
Fulfilled requirements and expectations of stakeholders and other parties
Control integrated security

A clear and finely-tuned stakeholder analysis is essential for configuring and implementing the MISH. Who are the security stakeholders within the institution? What are the needs of decision-makers, individuals within the organisation, chain partners, commissioning bodies, suppliers and service parties, trade unions, individuals and groups who are affected by the institution's activities (e.g. local residents), general interest groups, financers and insurers, government and supervisory authorities, emergency services, and the media? From the institution's perspective, not all stakeholders have the same impact. Which stakeholders require explicit consultation? The institution (i.e. the management) will also need to decide on the extent to which stakeholders' needs can be met.

An explicit stakeholder analysis forms the basis for decision-making regarding policy, security programmes and types of measures, as well as for communication with target groups. Such communication may focus on the setup and implementation of the MISH, awareness and training, and roles and responsibilities during incidents, for example. This will speak more to the needs of the target group, generating a greater appreciation for security policy.

4.3 Scope of the MISH

The scope of the MISH is defined by the risk types (security aspects) ascribed to the MISH in the first instance, and the business processes/locations to which the MISH applies.

Effective delineation of scope requires an understanding of what is going on internally within the organisation. This is developed during the sections titled ‘the Institution and its environment’ (4.1) and ‘Parties' needs and expectations’ (4.2).

The scope of the MISH must be defined as clearly as possible in order to facilitate implementation, and is always determined using a PDCA cycle consisting of the following elements:

- drawing up an adequate operational integrated security policy;
- identifying threats in order to determine risks and impact;
- identifying statutory (and other) requirements;
- setting priorities and objectives;
- creating a structure and programme for realising policy and objectives;
- planning, managing and monitoring preventive and response measures, and auditing them to ensure that the policy objectives are achieved and the security system works effectively; and
- being in a position to respond to changing circumstances.

Phased introduction of the MISH is also possible. In this scenario, institutions can establish the scope of the initial phase, and define how it will be broadened over the subsequent phases. This method allows for the gathering of experience, rapid communication of successes, and an improved understanding of critical business processes, compliance requirements and risks.

16 Leadership

5.1 Leadership and commitment

Without active top-down institutional support, it is not possible to raise the quality of an organisation-wide issue such as security. It requires more than just mandatory agreement to a policy proposal.

Management commitment pitfalls

In practice, the level at which security aspects and activities are delegated within the organisation is often too low, which can result in steps being taken in isolation and insufficient integrality. In these scenarios, executives miss out on information concerning the actual risks and effectiveness of security approaches, rendering the institution incapable of providing any accountability.

In other instances, security may be considered important and there may be a desire to get it organised, but there will be no money available or all other projects have top priority and nobody has time. Sometimes essential information is undocumented and only available from several key figures who are too often unavailable, or there may be too little expertise available within the institution to manage the MISH.

Obtaining active support from the management

Active support from the management is essential in order to secure sufficient funding for security measures, and to ensure momentum to keep the new security procedures rolling. Security measures will only work if they are actually implemented. The example set by the management – the 'tone at the top' – is essential in this regard. It is also important for the management to support the entire MISH as a 'big picture' issue, and not just cherry-pick individual security aspects or certain security measures. Likewise, the MISH must not be regarded as a one-off project, but as a continuous process that is a part of day-to-day operations.

There are two possible approaches to generating support for an MISH among the upper management. Firstly, the management may wish to realise quality improvements by implementing an MISH, after which risks will be more manageable. Another possible track is establishing a need for the multitude of existing requirements and risks to be made more manageable, which can provide a reason for implementing an MISH (by extension, such reasons may also include a lack of supervision or a lack of accountability).

Whatever the case, gaining active support at least requires aligning the scope of the MISH with management priorities. The management will make decisions based on a preliminary study, a project plan and a cost-benefit analysis (or business case). In any case, it should be clear which managers are involved in the project, how the management expresses its support, and whether any external involvement is necessary.

Depending on the scope and the organisational context, the MISH could also be implemented at departmental level, e.g. in the laboratories. At the very least, it will give the relevant organisational unit a systematic approach to dealing with security incidents. In such cases, decision-making will be the responsibility of the management of the relevant department.

Business case (cost-benefit analysis)
The benefits of the MISH include improvements to security performance and risk management, increased compliance, accountability for security issues, the institution's ability to function properly in unsafe environments, increased process efficiency (lower costs), increased confidence and morale among staff and students, improved reputation among the public, legislators and financers, and lastly, increased security awareness.

The costs of implementing an MISH mostly involve time investments.

Project plan
The project plan (implementation plan) is based on the results of the preliminary survey/GAP analysis. As a minimum, the project plan must devote attention to delineation, long-term objectives (the 'point on the horizon'), short-term objectives, the project unit, the anchor point for the management, the results to be delivered, the activities to be performed, the resources and budget required, completion times, and communication. See also Appendix 2 for a sample framework of activities required to implement an MISH.

5.2 MISH policy

An MISH policy document must be drawn up and adopted by the management. See 'NEN 7131 Societal security – Security, preparedness and continuity management systems – Requirements with guidance for use' for aspects to include in the policy declaration, such as exclusions, explicit commitments by the management, and the organisation's risk tolerance. This standard also addresses matters such as the ownership, formal acceptance and maintenance of policy.

This policy must be announced. The executive responsible for security may ‘take the stage’ during appropriate meetings to announce the policy, after which other line managers can take over. The policy must also be made available to stakeholders via the intranet or an external website as necessary.

5.3 Rights and responsibilities

Roles, rights and responsibilities must be clearly designated. In organisational terms, this can be achieved in a variety of ways.

First of all, an organisational unit must be assembled for the integrated security process.

Many higher education institutions do not yet have such a process – in these cases, it is best to organise the development and implementation of the MISH as a project, and to keep the future ongoing organisation of the security process in mind when staffing the project. This will allow the future manager of the integrated security process to start managing documentation at this early stage, and to structure it in a way desirable for the institution. Appendix 2 contains a framework suitable for use as a basis in setting up an MISH. The development and implementation of the MISH at institutional level may be adapted to suit the institution's specific situation and needs.

Security is often embedded vertically as an integrated management responsibility. Here it must be clear what the rights and responsibilities are at central and decentralised level. Processes are often carried out at joint locations. In addition to responsibility originating from process ownership, there will also be a location manager with security-related rights and responsibilities.

There are many sub-aspects to security, and the coordination of each one will need to take place at institutional level in order to guarantee consistency. Coordination between the aspects will also need to be structured.

One structure for clarifying the roles, rights and responsibilities is what is known as an RASCI matrix, which places the relevant results, processes and tasks on the Y-axis, and those who play a role in the security process on the X-axis. Every line (result, process, task) then states who is involved and the nature of their involvement (responsible, accountable, consulted, supported, informed).

Plan

The MISH has a number of activities and results that are implemented/achieved during the planning stage.

17 Plan formation

6.1 Steps aimed at risks and opportunities

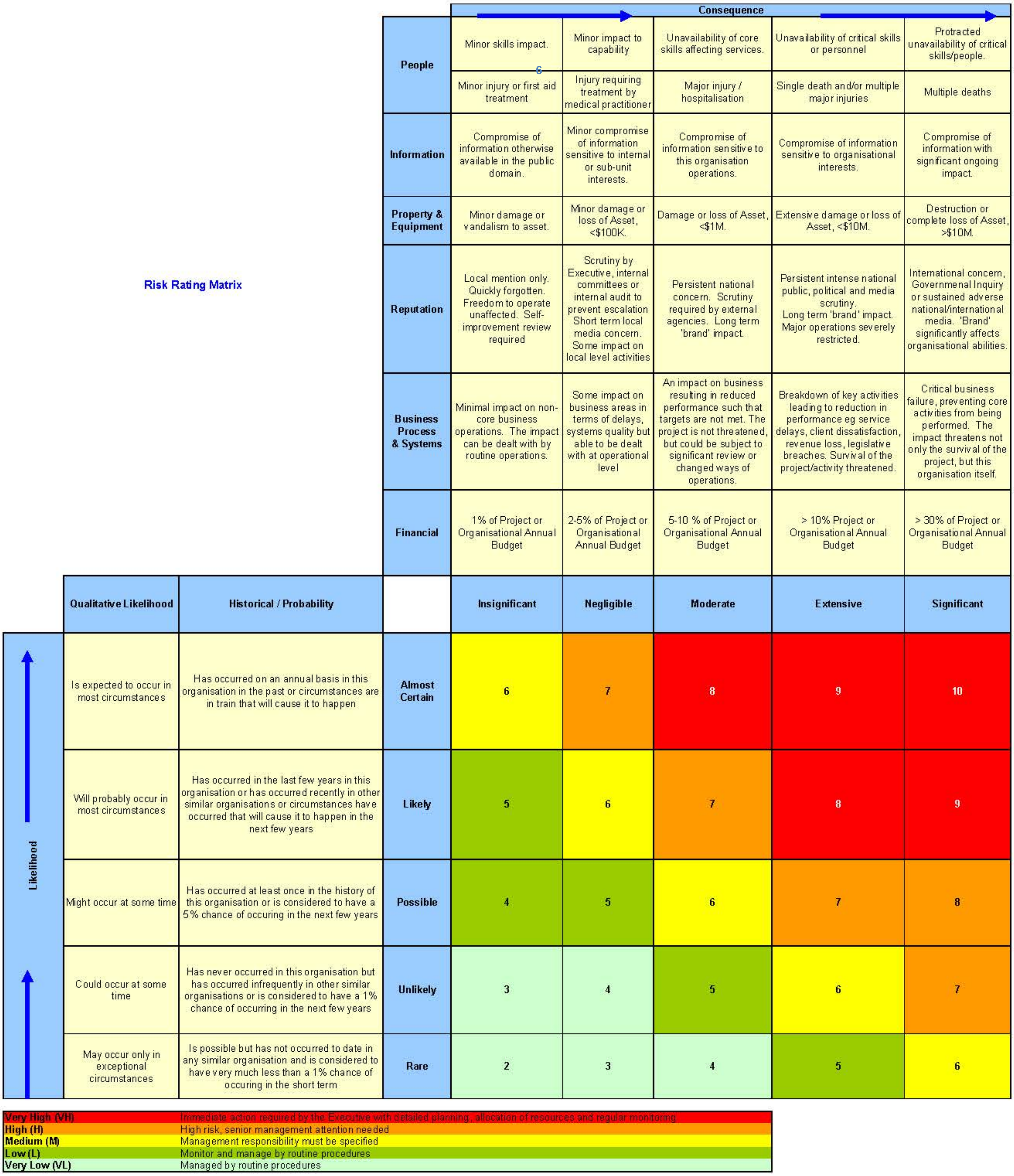
Higher education institutions have limited resources. The working day is only eight hours long, and each Euro can only be spent once. How are institutions to distribute these limited resources across all of their policy areas? Security, under the banner of MISH, is only one such area, and security aspects can even compete with one another for attention and resources within the MISH itself. On the one hand, the institution's mission and vision (as well as the wants and needs of the stakeholders) provide the framework within which these scarce resources are allocated. On the other, laws, regulations and normative references dictate how allocation may take place. Managing risks and taking opportunities are what enable an institution to achieve its goals. Security risk management is part of the risk management of the organisation as a whole, which is also known as Enterprise Risk Management (ERM). It should also be realised that positive and negative risks exist that must be weighed up against one another. A risk analysis will provide insight into these risks and lay the foundation for the measures to be taken, for their evaluation, and for being accountable for these decisions.

The allocation of time and resources in the institution will be supported by the results of risk and impact analyses, which will weigh up the interests of the institution against the possible impact of any disruptions on the one hand, and their likelihood and the costs of risk-reduction on the other. These analyses should concentrate primarily on the interests of the institution and its stakeholders, while keeping in mind that the various policy areas (e.g. education, research, business operations, accommodation and HR) present a range of risks.

Conducting the risk analysis

At the start of the risk analysis, it is important to have a clear idea of the objectives of the institution, the interests of stakeholders, and the purpose and scope of the risk analysis. These were all determined in Section 4, but may be further detailed in the risk analysis. Risk perception and risk acceptance may also be included in this overview.

The next step is to state the risks of the institution and identify the key risks. Under the MISH, it is a challenge to identify enough representative risks for each security aspect. Creating the security risk overview could be included in the stakeholder analysis, or could be an activity unto itself. An initial risk inventory will consist of a table of interests requiring protection, and the possible threats thereto. Appendix 3 presents a sample table at high level.
Next, the possible impact of each incident can be estimated, along with the likelihood that the incident will occur.



Risk Rating Matrix[6]

	Consequence				
People	Minor skills impact.	Minor impact to capability	Unavailability of core skills affecting services.	Unavailability of critical skills or personnel	Protracted unavailability of critical skills/people.
	Minor injury or first aid treatment	Injury requiring treatment by medical practitioner	Major injury / hospitalisation	Single death and/or multiple major injuries	Multiple deaths
Information	Compromise of information otherwise available in the public domain.	Minor compromise of information sensitive to internal or sub-unit interests.	Compromise of information sensitive to this organisation operations.	Compromise of information sensitive to organisational interests.	Compromise of information with significant ongoing impact.
Property & Equipment	Minor damage or vandalism to asset.	Minor damage or loss of Asset, <$100K.	Damage or loss of Asset, <$1M.	Extensive damage or loss of Asset, <$10M.	Destruction or complete loss of Asset, >$10M.
Reputation	Local mention only. Quickly forgotten. Freedom to operate unaffected. Self-improvement review required	Scrutiny by Executive, internal committees or internal audit to prevent escalation Short term local media concern. Some impact on local level activities	Persistent national concern. Scrutiny required by external agencies. Long term 'brand' impact.	Persistent intense national public, political and media scrutiny. Long term 'brand' impact. Major operations severely restricted.	International concern, Governmenal Inquiry or sustained adverse national/international media. 'Brand' significantly affects organisational abilities.
Business Process & Systems	Minimal impact on non-core business operations. The impact can be dealt with by routine operations.	Some impact on business areas in terms of delays, systems quality but able to be dealt with at operational level	An impact on business resulting in reduced performance such that targets are not met. The project is not threatened, but could be subject to significant review or changed ways of operations.	Breakdown of key activities leading to reduction in performance eg service delays, client dissatisfaction, revenue loss, legislative breaches. Survival of the project/activity threatened.	Critical business failure, preventing core activities from being performed. The impact threatens not only the survival of the project, but this organisation itself.
Financial	1% of Project or Organisational Annual Budget	2-5% of Project or Organisational Annual Budget	5-10 % of Project or Organisational Annual Budget	> 10% Project or Organisational Annual Budget	> 30% of Project or Organisational Annual Budget

Likelihood	Qualitative Likelihood	Historical / Probability		Insignificant	Negligible	Moderate	Extensive	Significant
	Is expected to occur in most circumstances	Has occurred on an annual basis in this organisation in the past or circumstances are in train that will cause it to happen	Almost Certain	6	7	8	9	10
	Will probably occur in most circumstances	Has occurred in the last few years in this organisation or has occurred recently in other similar organisations or circumstances have occurred that will cause it to happen in the next few years	Likely	5	6	7	8	9
	Might occur at some time	Has occurred at least once in the history of this organisation or is considered to have a 5% chance of occuring in the next few years	Possible	4	5	6	7	8
	Could occur at some time	Has never occurred in this organisation but has occurred infrequently in other similar organisations or is considered to have a 1% chance of occurring in the next few years	Unlikely	3	4	5	6	7
	May occur only in exceptional circumstances	Is possible but has not occurred to date in any similar organisation and is considered to have very much less than a 1% chance of occuring in the short term	Rare	2	3	4	5	6

Very High (VH)	Immediate action required by the Executive with detailed planning, allocation of resources and regular monitoring
High (H)	High risk, senior management attention needed
Medium (M)	Management responsibility must be specified
Low (L)	Monitor and manage by routine procedures
Very Low (VL)	Managed by routine procedures

[6] Image taken (partially) from SRM BOK (see Sources).

Comparing risks

The Security Risk Matrix can be used to visualise the risk distribution and prioritise the risks to be managed. 5x5 matrices (potential impact and likelihood) are often used, allowing for a matrix of 4-5 risk levels. Sometimes risk levels are purposefully not classified, in order to remove the impression of mathematical precision and accurate risk estimation.

Eighteen risks are plotted in the figure above as a sample matrix.

The matrix shown scores the risks by the following effect types: People/skills, People/injury, Information, Property & Equipment, Environment, Permits, Reputation, Finances, and Business Processes. The matrix is an initial move towards meeting the criteria, which may be further discussed and established during the institution's policy process.

Each event has a single probability, and may have a range of effects at varying levels. It is common to use the highest effect level when determining risk extent.

Addressing risks

Colours can be used to express an institution's risk policy. In the sample matrix risks in red are never acceptable; blue and green risks are. The risks in the yellow and orange boxes require special management attention.

Priorities in addressing risks may include: risks with the highest impact, with the highest probability, and/or risks with the highest product of impact x probability.

Addressing risks may involve a risk-management or a risk-financing approach. In an operational sense, risk management focuses on the risk itself and consists of the following options:

- Terminate. This involves ceasing a high-risk activity, after which the risk no longer exists.
- Treat. This approach concentrates on measures that reduce the likelihood of an incident (= prevention) or its impact.

The following options are available under risk financing:

- Transfer. This involves transferring the financial risk to the customer, supplier, insurer or government authority.
- Take. With this option, the risk is deemed acceptable, and potential losses are incorporated in the budget.

Risk financing is mostly useful for financial risks. It is not suitable for other effect types (such as reducing physical injury or reputation damage), and it is often not possible to terminate high-risk activities if they concern core business activities.

This generally points to reducing the risk from the operational side. In principle, prevention is considered to be the main means of limiting risks. It reduces the likelihood of the high-risk event occurring, or of developing into a more serious incident. Measures should also be in place to combat the incident, and to reduce its effects.

The risk evaluation must also examine the costs of risk reduction – these may include financing costs or overheads. Some higher-level risks can only be reduced at disproportionately high cost. The desired risk level can be set using the ALARP principle – As Low As Reasonably Practicable – which means striving for a level of risk that is cost-effective.

Risk register

Figure 3 Security risk matrix

Many risks will be identified in the institution, after which it is practical to enter the key risks in a register, including at least their likelihood and impact, and the person in the institution responsible for further dealing with the risk. This register can then be expanded to include the key risk controls, the residual risk and any measures yet to be implemented.

Standards and good practices:

- NEN-ISO 31000 Risk management – Principles and guidelines. This is a framework and procedure for assessing and managing risks, intended for use in enterprise risk management. Institutions can use this reference to manage both security and other risks within the organisation.
- NEN-ISO/IEC 31010:2009 Risk management - Risk-assessment techniques. This is an overview of techniques that can be used to assess risks.
- ISO/IEC 27005:2014 Information technology -- Security techniques -- Information security risk management. Covers risk management with relation to information security.
- Risk inventory and Evaluation (RIE). This is an instrument for generating an overview of working conditions.

6.2 MISH objectives, and how they are achieved

The goals of the MISH must be clearly defined. They will be derived from the MISH policy (see 5.2) and risk analysis (6.1), statutory requirements, other requirements and the wishes and needs of stakeholders (4.2).

An example goal could be: personal safety should always be given highest priority.

High-level statutory and other requirements should be identified straight away during the preparatory stage, to be further detailed during the planning stage. Draw up a list of statutory and other requirements, and create a procedure that is up-to-date and accessible by employees of the organisation. This step is often missing in practice, in which case a relevant legislation analysis will not be made until the checking stage. See Section 9.4 for a suggested approach to assessing statutory frameworks.
Examples of other requirements include agreements with government and other parties, customer contracts, sector codes of conduct, and public commitments made by the Executive Board. They may also concern the architecture of measures and cost levels, e.g. the desirability of a single ID/entry pass for everyone connected to the institution that can be used for physical entry, logical entry and for other purposes requiring ID.

The next step is to convert these requirements into MISH objectives, which must be consistent with organisational policy. After that, they should be made measurable (i.e. turned into targets). Planning and achieving the MISH objectives must be formulated as much as possible in SMART[7] terms, by establishing at least:

- what has to happen;
- which resources are available;

[7] ‘SMART’ stands for Specific, Measurable, Acceptable, Realistic, Time-Bound

- who is responsible for implementation (e.g. using a RASCI table);
- when it should be complete; and
- how the results are to be evaluated (who does the evaluation, and what criteria are used?).

An approach to planning the MISH objectives and steps is included in Appendix 2.

Security objectives can also be linked to security aspects, and be further specified later according to each aspect. This MISH manual concentrates on the following security aspects: Working Conditions, Environmental Safety, Public Safety, Integrity, Information Security, Privacy, Knowledge Security, Internationalisation, Building Security and Crisis Management. Section 8 looks more closely at these aspects and, in addition to sample relationships between threats and interests requiring protection, Appendix 3 also sketches the links between security aspects and threat types/interests requiring protection.

One useful approach is to set the objectives as part of the security chain. Some risks can be reduced through the reorganisation of business processes – this is called 'proaction'. Preventive steps can also be taken to reduce the likelihood of disruptive incidents. Approaches taken to fire, technical/organisational/human failure, and natural disasters/environmental threats are called 'safety'; addressing deliberate unlawful acts falls under 'security'[8]. Being ready for a disruptive incident is known as 'preparation', and action taken during or after the incident is called 'response'. Responses consist of combating the incident in order to minimise damage, and include resources such as company emergency response, digital/physical firefighting, salvage, and crisis communication/organisation. An incident may trigger the activation of the business continuity plan, which is intended to ensure that the essential business functions can continue in some form and that the situation can be restored.

The focal points of the measures must be given for each risk category. Should efforts concentrate mainly on measures for identifying threats at an early stage, on preventive action so that threats are less likely to result in incidents, on responsive/combative action, or on business continuity and recovery following an incident? The above can also be clarified using a 'bow-tie' diagram (see figure 5).

[8] Some aspects are primarily aimed at security, while others concentrate more on safety. Information security concerns both, and draws no clear distinction between safety and security.

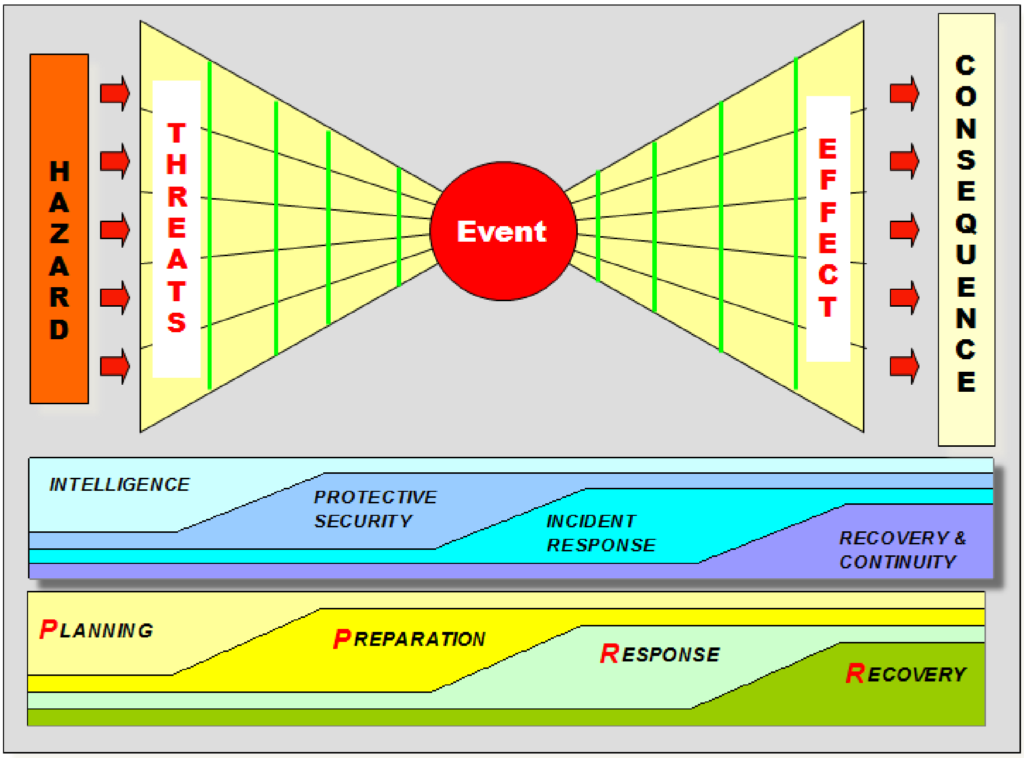


Figure 5 Bow-tie diagram[9]

18 Support

7.1 Resources

The design and implementation of an integrated security management system requires the allocation and designation of sufficient manpower and financial resources.

Employees at all levels and in (virtually) all departments must be given duties and responsibilities in order to manage security risks. The management must underscore the MISH vision and policy, and ensure implementation and compliance therewith. To this end, officers must be designated for the operationalisation of this policy (these policy objectives were operationalised as part of Section 6.2). Experts must be engaged to carry out risk analyses, identify vulnerabilities and formulate improvement proposals for the various security aspects. All employees should contribute to the institution's MISH according to their capacity.

Organisational structures and procedures should be put in place in order to counter security incidents and manage crises. A crisis response unit with unambiguous rights and responsibilities must be created and exercised. Various institutional units and disciplines should be represented in or associated with the crisis team, such as management, communication, legal, faculties, HR, ICT and facilities management.

Response teams can be assembled and trained to deal with specific security incidents, which in turn requires customised plans and procedures. Examples of response teams include Company Emergency

[9] Figure taken from SRM BOK.

Response for emergency aid during incidents in buildings, Computer Emergency Response Teams (CERT) for help with serious computer failures, and the Student Emergency Support Centre, which offers assistance to students abroad.

7.2 Competencies

Employees at all levels of the institution will be charged with MISH-related roles, rights and responsibilities (these are set under Section 5.3).

It makes sense to embed these security tasks within job profiles, in order to facilitate the description of the required competencies and simplify the management of their development and maintenance. Adequate time and resources must be made available for ongoing security training. These competencies must also be included as part of performance interviews and evaluations.

7.3 Awareness

Many security incidents have human action as their source. Lack of familiarity with a risk or with security measures, negligence, and organisational/human failure can all cause and exacerbate security incidents. Although humans can be the weak link, they can also play a major part in the identification and combating of (potentially imminent) security incidents.

Systematic raising of awareness is an effective way of limiting such risks. Awareness programmes target specific groups of people. An initial step involves ensuring sufficient knowledge transfer to these groups. What are the risks, what requires vigilance, and what roles do individuals play in incident prevention? Measurements can be used to monitor whether the group possesses sufficient knowledge, and whether further attention to these aspects is required. Over a longer period, a culture may emerge in which the desired behaviour is demonstrated. As such, the management must set an example (the ‘tone at the top’); the culture must be one in which people can be held accountable for their conduct, and where the desired behaviour is also exercised.

In any case, the starting point is the transfer of sufficient knowledge. Staff and students should be aware of the security risks that are inherent to work, study and research. The institution will need to continually focus attention on the presence and handling of these risks, e.g. via an introductory session on the first day of work or study for staff/students, issuing instructions on specific security procedures, security videos, brochures, performance interviews, posters, incident evaluations and public lectures.

The Integrated Security for Higher Education project includes a separate section on awareness.

7.4 Communication

The effectiveness of the MISH will depend on good communication, which requires planning, communication opportunities and communication procedures.

Communication is necessary with regard to the management structure: in this respect, make a distinction between communication at strategic, tactical and operational level. Section 4.2 sets out the stakeholders involved in the MISH and what the requirements are – this information can be communicated in a targeted fashion. Large target groups (such as staff and students) can be informed about security aspects, objectives and the structure and method of the MISH via meetings, working parties, newsletters and the intranet.

Communication regarding security aspects and incident types is also required. Here, a distinction is drawn between the pro-active (cold) stage, mid-crisis and follow-up to an incident.

Coordination and communication with the outside world must also be retained. The institution must maintain a network of external parties, both under normal circumstances and during a security incident or crisis. Collaboration with external parties may be organised in various domains and at various points in the security chain. For example: the acquisition of threat information and warnings about tendencies towards radicalisation, preventive action at a major event, or the response to a fire alarm and emergency aftercare. Depending on the nature and scope of the institution and the type of security domain, relationships are required with parties such as the municipal authorities, police, fire brigade, security region, the National Anti-Terrorism and Security Coordinator (NCTV) or the General Intelligence and Security Service (AIVD). Clear (joint or other) working agreements are essential in the region, with national platforms or communities of practice.

The objectives, methods and resources for internal and external communication should be set out in procedures, which may also describe the communication process with regard to the parties involved, times, methods and frequency of communication.

In addition to ordinary circumstances, the MISH communication procedure must also provide for communication during incidents and crisis situations. Preparing communication protocols, running sheets, training spokespeople and the coordination and practice of crisis communication deserve extra attention.

7.5 Documented information

The structure and functioning of the MISH must be described and documented. The allocated responsibilities, interrelationships between security aspects, the risk analysis method and the decisions on how to deal with non-conformities and risks must be set out.

Examples of MISH documents include: policy documents, organisational charts, schedules of objectives, risk/impact analyses, procedures and processes, standards, manuals, crisis plans, and evaluation, review and audit reports. Reporting through departmental and annual reports, and demonstrations of compliance and governance are also examples of MISH documents.

Do

The ‘Do’ stage of the management cycle covers the implementation and functioning of the security measures.

Following an introductory paragraph (8.1), the ten security aspects are briefly discussed below. The standards and resources currently known to be available for the security aspects are included in Appendix 1.

19 How does it work?

8.1 Operational planning and management: General

The institution must plan, implement and manage the processes required for performing the steps determined by the risk analyses outlined above. Such steps may also originate from management reviews and audits that have revealed ‘non-conformities’. For more information, see Section 9.

The proper implementation of improvement processes requires establishing criteria that are formulated in SMART terms, for which KPIs (key performance indicators) are also useful.

The management and control of these processes and their documentation should aim to have them executed as planned and allow for adequate reporting thereon.

The institution must evaluate and assess the effects (including side effects) of planned modifications, as well as the consequences of unplanned changes. Where necessary, new improvement steps must be carried out to mitigate any negative effects and consequences.

The institution must also ensure the management of outsourced processes.

The sub-sections below briefly describe the security aspects that are relevant to higher education institutions. Each aspect includes a short introduction, outlines a number of possible risks, and also suggests possible management measures and any potentially relevant standardisation frameworks.

8.1 Working conditions

Higher education institutions are classified as employers under the Working Conditions Act (*Arbeidsomstandighedenwet* – this act also applies to student care). Staff, researchers and students have no choice but to work in the conditions facilitated by the institution.

Institutions must do their utmost to prevent accidents and physical injury on their premises. which can be caused by slippery or otherwise unstable surfaces, collapsing objects, the use of special machinery or non-approved manual electrical tools and devices, as well as exposure to high voltages, vapours, radiation, bacteria or viruses. A healthy workplace must have enough light, a pleasant climate and devote attention to ergonomics in order to prevent RSI and other physical conditions. Hazardous sites must be made inaccessible to unauthorised persons, and their security increased through controlled access, clear rules of conduct, and the provision of training and information.

Internal legal protection for students is provided for under the Higher Education and Research Act (WHW). For example, higher education institutions must provide a single facility or service desk where students can go to make complaints. Additionally, all institutions must have instruments in place such as a complaints procedure, staff ombudsman, a procedure for improper conduct, code of integrity and whistleblowers' regulations.

Occupational stress and improper conduct can cause psychosocial damage – a focus on this aspect, and on work absence in a broad sense, is important for the effective management thereof. The occupational health and safety catalogues of the VSNU and VH devote attention to the effects of psychosocial work stress on staff.

8.2 Environmental safety

Environmental protection and the creation of a sustainable society must be high priorities within the institution. Different institutions will face vastly different challenges in this regard. Animal research laboratories will want to avoid threats such as diseases and the attention of animal-rights activists, while institutions with a research reactor will aim to prevent radiological/nuclear contamination and safeguard the management of fissile materials.

In addition to sustainability, permit maintenance also plays a role here. The institution's primary process is directly linked to the ‘licence to operate’, and incidents can lead to considerable damage to reputation, high penalties, mounting sanitation and repair costs, and damage claims.

Environmental protection involves a range of aspects. Energy footprints are fed mainly by heating, cooling and lighting. Waste is determined by reusability, separation of waste flows, and quantities of sewage and surface water. Locations with warm water can harbour legionella, and asbestos may still be present in older buildings.

Particular sites within an institution may be hazardous to people and the environment due to the presence and use of chemicals, genetic modification, and radiological/nuclear activity. The use of laboratory animals in animal-friendly environments may also be included in this policy area.

The various environmental permits are grouped together under the integrated environmental permit (*omgevingsvergunning*). All institutions will at least need to have an environmental officer to coordinate this policy area. If there is a possibility of radiation, the institution must also have a radiological/radiation officer who also coordinates security for these sources. Institutions with biological labs must appoint a biological security officer for the same purpose.

8.3 Public safety

At higher education institutions, people work, study and conduct research together in a wide variety of circumstances. Guaranteeing public safety for these people is one of the institution's key responsibilities. People must feel safe, and their physical and mental integrity must be safeguarded. The security of personal property is a further aspect of public safety, which must be ensured within the institution's buildings and on the premises. The responsibility extends beyond that, however, to areas such as public safety in accommodation, social interaction, and during study trips. Institutions must remain alert and take steps to prevent public safety threats such as bullying, sexual harassment, theft of personal property and threats to employees.

Because institutions are a reflection of society, they are also subject to social developments that include violent acts by individuals, and radicalisation. In this respect, institutions operate at the cusp of social, personal and institutional interests, necessitating cautious and tactful action.

8.4 Integrity

The need for a moral compass
Integrity is the cornerstone of professional conduct – a core value and driver for professionals in all sectors of society. People navigate according to their moral compass in order to ‘do the right things’ and ‘do things right’, based on an intrinsic motivation. In addition to these internal factors, external incentives also play a part in the performance of activities. Sometimes an imbalance between intrinsic and extrinsic motivators will cause one's moral compass to become skewed, upsetting the moral balance between what is and what is not (or no longer) acceptable and causing a possible violation of integrity. Issues are emerging in various domains that point to a lack of integrity, recently concerning sectors of society that were previously considered reliable. Incidents at banks, housing associations, hospitals, education institutions and within academia have led to social indignation and loss of trust.

Prevention is better than cure
Damaged trust cannot always be easily restored, and often requires a lot of time and energy. Trust plays an important part in our society, and higher education and research are no exception. It determines to a large extent how we view and interact with one another.
The remedy for restoring trust is to prevent its loss in the first place. This means it is time to consider what integrity in higher education actually means. Upholding and guaranteeing high-quality and reliable education and research is a responsibility that students, staff and executives and other relevant parties can only achieve together. A focus on integrity – both professional and academic – is crucial in this regard. Society must be able to rely on higher education institutions that function properly. Professionalism, reliability, steadfastness and due caution all contribute to this reliability, and the integrity of the sector as a whole is dependent on the integrity of each and every employee, executive, lecturer and student.

There are many practical examples of violations of integrity in the sector – such incidents generally attract a lot of media attention, and cause a lot of damage to reputation.

There is much that higher education institutions can do to safeguard the integrity of the management, lecturers, researchers, other staff and students. A code of conduct that describes the procedures for handling dilemmas and standards with regard to deviant behaviour forms an important initial step in this regard. Other examples of integrity measures include the appointment of confidential counsellors, a standard of conduct for good governance and integrity, and steps to counteract fraud during tests/examinations.

8.5 Information security

All of society (and therefore higher education institutions) is becoming more and more reliant on the use of computers, the internet, smartphones and all kinds of digital applications. We can essentially no longer do without them: not as individuals, as institutions, or society as a whole. Information security is about protecting and safeguarding these digital facilities. The complexity of ICT infrastructure (networks, providers, the cloud), hardware (laptops, tablets, servers, mobile devices), operating systems (Windows, Linux, iOS) and countless software packages and applications make this an extremely complex field that involves many disciplines and areas of expertise.

One major risk of inadequate information security could be defined as: ICT infrastructure becoming unavailable, thereby removing access to the institution's own data. Theft of ICT equipment and the loss of large quantities of data can also lead to considerable damage costs. Corrupted databases, and unreliable modifications to research data, operational data and student administration files can cause significant problems. In higher education too, however, aspects such as digital fraud, violation of student/staff privacy and penalties for failure to comply with legislation are never far away. Even damage claims (e.g. from contract research) and intellectual property offences cannot be fully excluded.

Higher education institutions must make investments in order to manage the risks associated with ICT failure and cybercrime as effectively as possible. Policy formulation, multi-year plans and the engagement of experts are indispensable in this regard. A framework often used is ISO 27002 – a standard that includes the following sections: Information Security Policies, Organisation of Information Security, Human Resource Security, Asset Management, Access Control, Cryptography, Physical and Environmental Security, Operations Security, Communications Security, System Acquisition, Development and Maintenance, Supplier Relationships, Information Security Incident Management, Information Security Aspects of Business Continuity Management, and Compliance. SURF has developed a range of resources for higher-education institutions based on this standard (and others). See Sources (Appendices 1-5).

8.6 Privacy

It needs no explanation that higher education institutions use personal data in countless processes. In this context, data privacy concerns the individual's right to the careful processing of his/her data.

Data processing legislation is based on a number of privacy principles formulated by the OESO and the Council of Europe, i.e.: that the purpose of collecting the data be made clear; that only necessary data be collected; that the use of the data be restricted to the purpose for which it was collected; and that the personal data be correct and properly secured. All individuals whose data is processed also have the right to transparency (information), to view and correct the data, to submit a complaint or claim damages, and in some cases: the right to object (opposition), the right to approval before the data is used, or to request that personal data be deleted. The organisation must also be able to justify the use of the data.

Europe is seen as a single digital zone with unrestricted data traffic – it is for this reason that the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*, WBP) is based on a European Directive. Given the rise in digitisation and ways to connect and exchange data, and incidents resulting in personal data being misused or becoming publicly available, legislation is currently being tightened up. Mandatory reporting of data leaks is introduced in the Netherlands in 2015, with failure to do so being subject to likely penalties of up to €820,000. The Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*) will gain authorisaty to issue penalties under the WBP of €820,000 per incident. Lastly, a new European privacy regulation has been in April of 2016, allowing possible penalties of up to 2% of companies' annual world-wideturnover, or €20,000,000 for businesses and government institutions that process personal data inappropriately. The European privacy regulation will replace most of the Dutch Personal Data Protection Act (WBP). In terms of content, the European privacy regulation will adhere to the OESO privacy principles, but with a greater focus on external accountability. These legislative changes will result in a large number of mandatory control measures for the protection of personal data, putting data processing and privacy on the executive agenda.

The rise of penalties for improper processing of personal data also means that it may become easier for persons affected to claim damages from institutions, and to claim greater amounts. Incidents will also cause damage to an institution's reputation.
Increased penalties will also present a material risk to institutions that fail to comply with current or future European privacy regulations and legislation. For this reason, annual report accountants will also start requesting evidence that the management is ‘in control’, e.g. by means of a management system

approach to privacy. If accountants believe that the management is not in control, they will demand substantial provisions to be made for future penalties.

Appropriate privacy compliance policy can enable institutions to balance the various interests, personal risks and practical control measures, and to report on them. At SURF, developments are underway that are aimed at allowing institutions to prepare for the upcoming changes in European legislation.

8.7 Knowledge security

Higher education institutions are knowledge generators, where valuable knowledge is created and managed. Knowledge creation (or research) is generally conducted jointly with other parties, such as knowledge institutions or commercial parties. Third parties also conduct research. As part of the outline agreement, institutions have also made agreements regarding knowledge valorisation, i.e. the marketing of the 'knowledge' developed by higher education ('from knowledge to profit'). To this end, research universities and universities of applied sciences (as knowledge institutions) collaborate with companies and government authorities in public-private partnerships. Institutions are subject to great risk if this knowledge ends up in the wrong hands. In addition to protecting intellectual property, monitoring knowledge security is also a prime concern. After all, there is much at stake.
Sometimes third parties entrust valuable knowledge to higher education institutions, who may then be charged with protecting it. Unauthorised access thereto, either accidental or purposeful (i.e. espionage), or loss of such information can have disastrous consequences for the institution's reputation. Inadequate knowledge security can thus allow third parties to patent knowledge developed inside institutions, potentially resulting in court cases on the violation of intellectual property rights. A further risk involves the appropriation and misuse of knowledge developed by an institution by 'rogue states', of which the nuclear proliferation by Pakistan is one example. Institutions will occasionally innocently breach Dutch export legislation under the Non-Proliferation Treaty. This also represents a form of 'knowledge security', as does reputation damage due to incidents of corporate espionage, and damage claims by contract partners in the face of inadequate knowledge security.

Improving and ensuring knowledge security is primarily a question of awareness and vigilance among researchers, staff and students. A code of conduct that offers guidelines on how to go about knowledge exchange (e.g. at congresses, in collaborative projects and publications) forms a good basis for improving knowledge security. Institutions may also consider matters such as non-competition clauses, employee screening and confidentiality statements. The categorisation, protection and patenting of information are also measures that promote knowledge security.

8.8 Internationalisation

More and more students, researchers and staff at higher education institutions are travelling to destinations abroad, and staying longer. Although some are seasoned travellers and know what to look out for, others may never have left home before, or are experiencing a foreign culture for the first time. Are such people well-prepared for potentially unfamiliar and high-risk situations? Is there a procedure available, and are any references to relevant documentation up-to-date to allow proper preparation for travel, or maybe even provide a reason not to travel? Has somebody been appointed to monitor the safety of travellers, and to take action if necessary? Is there enough attention to differences in culture, customs and legislation? Have medical facilities and primary living conditions been investigated, and is the traveller prepared for them?

In other countries, different standards and rules may apply to alcohol and drug use, the do's and don'ts of nightlife, and sexual ethics, for example. Taboos and etiquette can sometimes be strange and unexpected.
Proper preparation for travel will also devote attention to risks such as robbery, passport loss, accidents and serious illness. A sudden return home due to family circumstances sometimes also requires attention, and institutions must be prepared for a student or staff member to go missing when abroad.

More and more students, researchers and staff from international higher education institutions are also coming to the Netherlands, in which case the institution may be the host and only source of support for these travellers. Has the institution informed them sufficiently of the situation in the Netherlands, the city and the institution? Have these people been properly briefed by their home institutions on their journey to the Netherlands and their stay here? To what extent can these people take care of themselves?

Is it worth considering designating someone as a contact person and confidential counsellor for travellers? An information pack on different international customs and legislation, suggestions for proper travel preparation, and a source of further information on relevant destinations will often prove useful. A brochure in English for incoming students and researchers is advisable for institutions wishing to attract international guests.

Lastly, international exchange must also take due consideration of the risks presented by knowledge security, such as the use of tablets, laptops and telephones abroad, and other data stored digitally such as contact and login information.

The Internationalisation sub-project has released some tools for raising awareness of the security risks inherent to internationalisation.

8.9 Building security

At higher education institutions, lots of people congregate inside buildings. Guaranteeing the safety of these people is one of the institution's key responsibilities. Everything possible must be done in order to avoid any incidences of personal injury, and measures taken after any such incident in order to bring those affected and any bystanders to safety in a swift and controlled manner.

The regulations governing the construction and use of buildings are set out in the Housing Act (*Woningwet*), Section 1a of which states that the owner of any building retains primary responsibility for security. Secondary responsibility lies with the user, to the extent that this is within his/her power. The Housing Act serves as a ‘guideline’ for the Buildings Decree (*Bouwbesluit*) 2012, which sets out the construction regulations. The Buildings Decree outlines the minimum requirements; failure to satisfy these requirements means that a building does not meet the legal minimum.

This means that the owner and/or user will be held initially liable for any safety incidents. After an incident, it may be investigated whether the requirements were met. In other words: the issue of a permit or the usual ‘once over’ by the fire brigade are no guarantee that the requirements are being met.

The Buildings Decree contains requirements regarding safety, health, usability, energy efficiency, the environment, equipment and use. However, these requirements do NOT provide for the continuity of the organisation following an emergency. The owner or user must evaluate these risks themselves, and take additional steps where desired. Any requirements set by an insurer generally also exceed those of the

Buildings Decree, which also sets no requirements with respect to the company emergency response organisation within a building.
The Integrated Environmental Permit (*omgevingsvergunning*) combines the various permits for a single location, including those required under the Buildings Decree.

In addition to people, there are of course other aspects requiring physical protection in order to ensure institutional continuity or limit other types of damage. These include significant operational processes, ICT and other specialist resources, and the building itself. The requirements under the Buildings Decree and Integrated Environmental Permit revolve around safety, and NOT the continuity of the organisation. The institution will need its own vision on fire safety levels in the data centres and other essential facilities. The same applies to protection against water, cold and heat damage. Measures must be adjusted to accommodate a range of operating scenarios – a building at night is different than one during normal use, or a special event.

In addition to crime (including burglary, theft and vandalism), building security must also take disturbance and nuisance into consideration. Approaches such as CPTED (Crime Prevention Through Environmental Design) can prove cost-effective in creating a public environment whose occupants feel safe. Building security will also need to consider: fire, exposure to toxic gases and smoke, explosions, disturbances of the peace that can create panic, natural disasters, and traffic accidents on or in the vicinity of the premises.

Few statutory requirements exist concerning security against various forms of wilful conduct and public safety. One exception are new-build residential buildings (student accommodation), which are subject to some concrete requirements under the Buildings Decree 2012. It is up to the management of the institution to decide which interests must be protected against which threats, and to what extent.

8.10 Crisis management, company emergency response, business continuity management

All self-respecting organisations of any reasonable size will be prepared for a crisis. This guideline has already covered the various security and safety aspects where crises can emerge. Institutions may have already taken preventive steps in all of these areas, and of course, everybody hopes that these measures will be sufficient to avert a potential crisis in time. Institutions themselves may also be confronted with a crisis situation, in which case there are some important questions: Is the institution adequately prepared? Have roles and responsibilities been allocated? Does everybody know what is expected of them? Are adequate resources available? Are people informed, trained and competent?

Preparing for effective crisis management is first and foremost a matter of action. Allocating roles, resources and responsibilities, and aspects such as informing and training of staff require constant attention from the management. Training plans and cycles can help in this regard. In addition to informing and training students and staff, specific drills may be organised for bodies such as the board, the management, the IT department or the company emergency response team. Integrated drills centred around a particular theme can also be organised, such as 'students lost abroad' or 'major fire in main building'.

Company emergency response is also an element of crisis management, aimed at bringing people to safety during an incident. A business-continuity approach enables institutions to ensure that the key processes can continue to function at some level following an incident, and that the situation can be restored within an acceptable timeframe. Lastly, effective crisis communication is important in order to provide stakeholders with the right information during a crisis, and thereby limit consequential and reputation damage.

Check

The ‘check’ stage of the management cycle evaluates its effectiveness.

20 Evaluation

In accordance with the management structure, the higher education institution must continually monitor and evaluate its security plans and procedures, and the measures taken. To this end, a periodic cycle of management reviews, surveys, tests, exercises and audits must be undertaken.

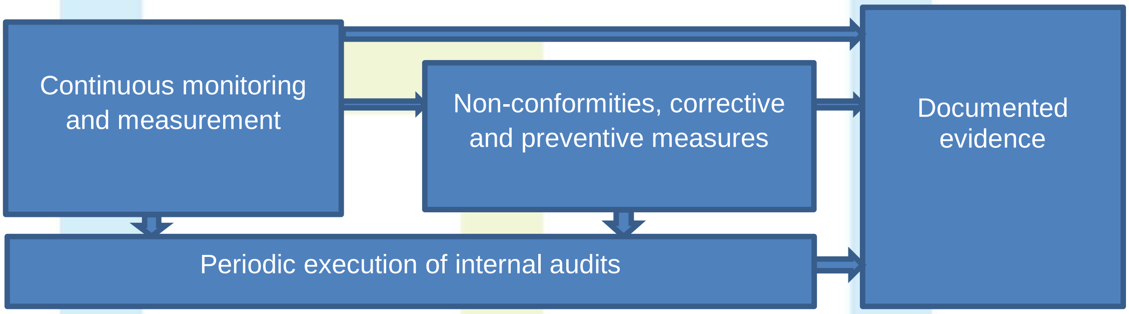
Any and all security incidents must be investigated and evaluated.

The institution must keep an overview of investigations conducted, and the resulting conclusions and recommendations.

In addition to incidents, scenarios must also be evaluated. For example, what is the vulnerability (i.e. likelihood) of a particular scenario, and how will the organisation respond to it? Is this acceptable to the board and stakeholders?

It is also possible to commence the MISH improvement process during the ‘check’ stage, in which case the first step is to scan the current situation. The scan results will be used to identify problem areas, which can be addressed first and will serve as input for a management decision (management review stage) for the start and objectives of an improvement process.

Being accountable for security performance is essential for institutions, and the following relationships exist between the activities in the ‘check’ and ‘act’ stages:


Continuous monitoring and measurement
Non-conformities, corrective and preventive measures
Documented evidence
Periodic execution of internal audits

One basic principle concerns making safety and security performance measurable. This may involve defining key performance infdicators (or KPIs), or other targets and associated measurable qualities. In addition to Section 8.1, this topic is also covered in Section 9.1.

These aspects must be continually measured and monitored, e.g. via tests, drills and daily reports. Results are to be kept as evidence of effective security performance.

If the measurements reveal an aspect of security performance that is not working properly, appropriate corrective/preventive steps must be taken. For more information, see Section 10.1. Results are to be kept as evidence.

Internal audits will be carried out periodically. For more information, see Section 9.2. Input for internal audits includes the results from the ongoing monitoring and measurements, as well as the non-conformities that have been corrected. The results of the internal audit are to be recorded as evidence.

9.1 Monitoring, measurement, analysis and evaluation

One monitoring instrument that has been tried and tested is the self-assessment. A self-assessment gives those responsible in an operational and policy sense insight into the quality of the relevant security process, enabling them to use it as a basis for further action.

The literature says that monitoring and measurement of security performance is best organised using KPIs (key performance indicators). The institution will therefore need to establish KPIs for all security aspects, and summarise and report on selected KPIs at monthly, quarterly and annual intervals via a management report. This process will shed light on trends and maturity levels for each security aspect.

In practice, defining effective KPIs has proven difficult; identifying the most useful KPIs via the community of practice may be a useful approach. Various sources are available to do so. Identify the KPIs that are already being used in the various areas. Some KPIs are required in external reporting, and are more or less fixed. There are also institution-specific indicators that can be used to actively improve security (the ‘act’ stage).

From the resulting overview, a system of KPIs can be drawn up such as ‘average no. of incidents per employee (employee is at fault)’; ‘average no. of incidents per international student (student is victim)’; or ‘no. of FTE[10]s charged with security tasks’.

Institutions will need to organise regular drills and tests to evaluate the effectiveness of the security measures taken. Some security aspects may be evaluated simultaneously (i.e. in an integrated fashion). Drills and tests (D&T) must be organised with due consideration of:

- targets, responsibilities and the institution's role;
- the goal, scope and impact of the D&T;
- risks inherent to D&T; and
- prior D&T results.

The incident register represents an important source of information. It must be clear to all parties involved where incidents can be reported. From this point, the report must be taken to an internal or external party for further assessment and processing. A distinction may be drawn, for example, between ICT incidents, physical security incidents and incidents involving people. The incident register will provide management information on types of incidents and vulnerabilities and on how effectively these incidents are processed, which can then be used to draw up improvement plans.

9.2 Internal audits

When positioning an internal audit, it can be useful to be aware of the following distinctions:

[10] full-time equivalent

- A **self-assessment** is performed by the very object of the evaluation (like the butcher assessing the quality of his own meat), and is intended primarily as preparation for an internal or external audit.
- An **internal audit** is carried out by the organisation itself, and may be performed by either in-house employees or external parties. The results are mostly used by the organisation itself for improvement purposes.
- An **external audit** is carried out to demonstrate the effectiveness of the security system to the outside world. External audits are led by external parties.

Institutions must organise annual internal audits on each security aspect or, where possible, for multiple aspects simultaneously. The institution must establish, implement and maintain an audit programme including methods, responsibilities and reporting. It must include the interests of the processes in question, as well as the results of previous audits.
Focus areas include:

- requirements set by the institution as included in the scope (see 4.3);
- security targets, processes and procedures;
- efficiency and suitability of measures; and
- the results of prior drills, tests and reviews.

In addition to internal audits, there are also various kinds of external audits. Security measures regarding contract research may be evaluated externally, and laboratories will also be regularly assessed externally for re-issuance of permits. Such an evaluation will generally be initiated by the permit issuer and carried out by the organisation itself, a competent external specialist, and may also include the results of internal institutional evaluations.
Create an overview of the external audits to be carried out and investigate options for simplifying their performance, in order to arrive more quickly at a positive result, with less of a burden on the organisation.

9.3 Management review

Each year, institutions must investigate the extent to which security aspects are being managed in an integrated way, and whether continuous improvement is being worked on. The effectiveness of the MISH must be evaluated, and the investigation will be based on:

- previous investigations and reviews, including conclusions and recommendations;
- progress on the implementation of prior recommendations;
- advice and recommendations from external/other security experts;
- the results of audits, drills and tests;
- developments in the reported KPIs;
- internal and external developments.

The annual management review must report conclusions and make recommendations with respect to:

- integrated security management;
- the effectiveness of the policy being pursued (measures taken);
- updating threat/impact/risk analyses;
- the training and readiness of crisis units;
- crisis plans being up-to-date;
- improvements to security plans, procedures and measures; and
- allocation of resources for all security aspects.

The organisation (see 5.3) must determine the parties to be involved in the management review. In addition to the board, this may include process owners. By signing the management review, the relevant executive or manager indicates that they are aware of all relevant investigations, that they have drawn their own conclusions regarding the MISH and the activities to be performed in the period ahead, and that there are also sufficient man-hours and resources available to do so.

9.4 Evaluation of each security aspect

Assessment instruments
Some of the security aspects in the MISH come with their own set of evaluation tools that institutions can use. See below for an overview of the available instruments. There are also assessment instruments available commercially on various aspects.

The ‘comply or explain’ principle applies to the use of these instruments. Use them. There may be reasons not to use them, but if so, you must explain how an appropriate level of security is ensured.

	Governance, risk, compliance	Working conditions	Environment	Public safety	Integrity	Information security	Privacy	Knowledge security	Internationalisation	Building security	Crisis management, company emergency response, business
SURF, Framework of standards, assessments and benchmark. This is a framework of standards based on ISO27002 covering information security, continuity of business data, and privacy.						x	x				
Integrated Security for Higher Education, SAINT (Self-Assessment of INTegrity).					x	x		x			

Regulation assessment
Regulation consists of a statutory framework and self-regulation within the sector. Testing compliance with this regulation is only possible after explicating the legal framework for each process.

Begin here by identifying the processes and determining their nature, which will then serve to identify the statutory and self-regulation requirements. Locations/processes with a unique character under regulation include catering/the kitchen, laboratories, the helipad, parking garage or major events. Often locations or processes are only subject to a part of legislation, which will result in a table stating which parts of the legislation will be evaluated and reported on for each process/location. It is also possible to determine which parts of legislation do not require immediate evaluation. The availability of a document stating clear decisions regarding regulation requirements that are and are not considered relevant is in and of itself an important accountability resource.

The table below provides a starting point for common legislation, and the security aspects to which it applies. The community of practice could further detail this list to incorporate relevance to processes.

	Governance, risk, compliance	Working conditions	Environmental safety	Public safety	Integrity	Information security	Privacy	Knowledge security	Internationalisation	Building security	Crisis management, company emergency response, business
Public Procurement Act (*Aanbestedingswet*)					x						
Working Conditions Act (*Arbeidsomstandighedenwet*), including the Working Conditions Decree (*Arbeidsomstandighedenbesluit*) and NEN standards		x								x	x
Asbestos Act (*Asbestwet*)			x								
Dutch Civil Code (*Burgerlijk Wetboek* e.g. unlawful acts)		x	x	x	x	x	x	x	x	x	x
Licensing and Catering Act (*Drank en horecawet*)										x	
Nuclear Energy Act (*Kernenergie wet*)			x							x	
Aviation Act (*Luchtvaartwet*, helipad)										x	
Tobacco Act (*Tabakswet*, smoke-free areas)		x								x	
Commodities Act (*Warenwet*, food handling)			x							x	
Water Act (*Waterwet*, drinking water, waste water disposal)			x								
Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*)							x				
Computer Crime Act (*Wet Computercriminaliteit*)						x					
Experiments on Animals Act (*Wet op dierproeven*)			x							x	
Higher Education and Research Act (*Wet op hoger onderwijs & wetenschappelijk onderzoek*)	x			x							
Private Security Organisations and Detective Agencies Act (*Wet particuliere beveiligingsorganisaties en recherchebureaus*)					x					X	
Abuse of Chemical Substances (Prevention) Act (*Wet voorkoming misbruik chemicaliën*)			x							X	
Environmental Management Act (*Wet milieubeheer*, soil quality)			x								
Housing Act (*Woningwet*), including the Buildings Decree and the Integrated Environmental Permit See also the note to Appendix 1 – 9 Building Security			x							X	x
Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financiering van terrorisme*)					x			x			
Penal Code (*Wetboek van Strafrecht*)		x	x	x	x	x	x	x	x	x	
Code of Criminal Procedure (*Wetboek van Strafvordering*)		x	x	x	x	x	x	x	x	x	
The Educational Institutions Reporting Regulations			x	x			x				x

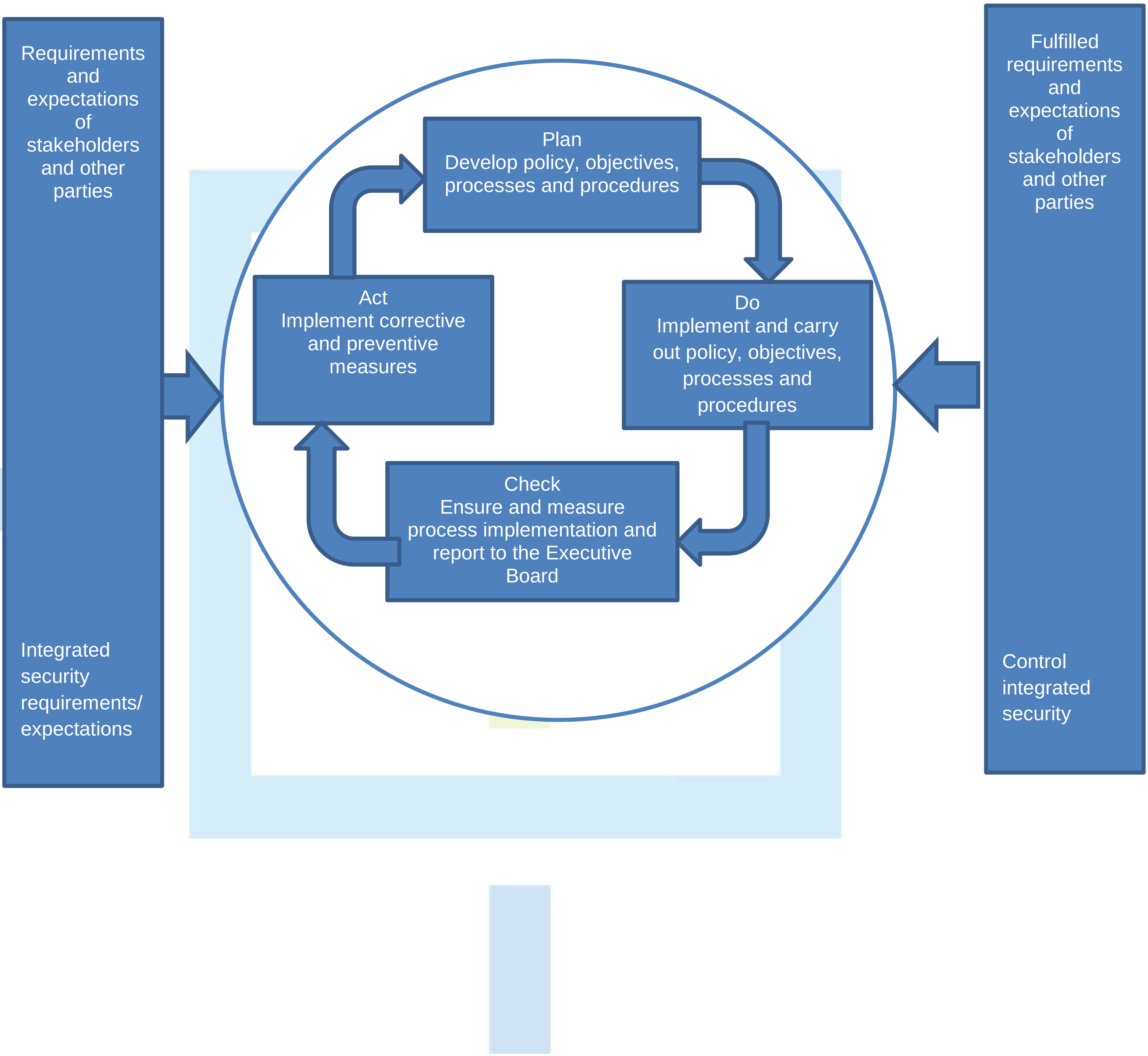
	Governance, risk, compliance	Working conditions	Environmental safety	Public safety	Integrity	Information security	Privacy	Knowledge security	Internationalisation	Building security	Crisis management, company emergency response, business
(*Regeling Jaarverslaggeving Onderwijs*, RJO) form a statutory reporting framework. The RJO is based on Draft Directive 400 on Reporting (*Ontwerp Richtlijn 400 Jaarverslag*) by the Dutch Accounting Standards Board (DASB). As a further specialisation of the RJO, the Education Inspectorate is drawing up the ‘Education Protocol’. This instruction sets out what needs to be reported on. The Education Protocol demands a paragraph on continuity, environmental safety, public safety and privacy.											
Implementing regulations on radiation protection (*Uitvoeringsregeling stralingsbescherming*)			x							x	
Whistleblowers' regulations (*Klokkenluidersregeling*)					x						
Code of Integrity or Code of Conduct											
Regulations on undesirable behaviour (*Regeling ongewenst gedrag*)				x							

Act

The ‘act’ stage of the management cycle is when improvements to security are introduced.

21 Continuous improvement

During the act stage of the management cycle, the corrections and improvement steps for security aspects and the management system are initialised. These steps are drawn up using previously-obtained management information.


Requirements and expectations of stakeholders and other parties
Integrated security requirements/ expectations
Plan
Develop policy, objectives, processes and procedures
Do
Implement and carry out policy, objectives, processes and procedures
Check
Ensure and measure process implementation and report to the Executive Board
Act
Implement corrective and preventive measures
Fulfilled requirements and expectations of stakeholders and other parties
Control integrated security

10.1 Non-conformities and corrective steps

Institutions can benefit tremendously from an effective non-conformities procedure.

Sources of information that may reveal non-conformities include self-assessments, incident reports, inspection and maintenance reports, project reports, audit reports, information relating to situations and events entailing special risks, stakeholder complaints and concerns, and observed instances of non-compliance with legislation. Non-conformities can be reported on and collected according to security aspect.

Various options are available once a non-conformity has been identified. The non-conformity itself must be addressed, and the consequences dealt with in the event of any damages.
Another idea is to look at the causes of the non-conformity: can any steps be taken to reduce the likelihood of a recurrence? Was it an isolated incident, or could there conceivably be other similar cases? In the latter instance, similar non-conformities must be actively sought out and addressed. With a pro-active stance, every observed non-conformity will lead to improvements to the security approach.

The results must be kept as documentary evidence in order to facilitate the institution's security performance reporting.

Due to the sheer numbers of security aspects and potential corrective steps requiring management, we recommend that the institution set up a system or registry to record all non-conformities per security aspect, as well as any planned steps and the current state of affairs. The registry could also be used to record (or refer to documents that contain) the analysis of shortcomings, which may include the cause(s) thereof, their severity (potentially higher risk), possible damage-control measures, their costs and effectiveness, a cost-benefit analysis, and an analysis of whether similar shortcomings may emerge.

10.2 Continuous improvement

Higher education institutions must convert the conclusions and recommendations from the management reviews, drills, tests and audits into improvements to the integrated security management system and concrete security measures.
For every failure to comply with laws and standards, these ‘non-conformities’ must be eliminated within a foreseeable timeframe. The improvements must be aimed at preventing the occurrence of new non-conformities in the future.

The board and management must communicate these improvements, ensure their implementation and report on them in the Annual Report. The budget must allocate sufficient annual funds to the management and improvement of the MISH.

Improvements to the MISH will always need to consider which link in the security chain will realise the greatest return on investment. Improvements will be prioritised partly based on the extent of their contribution to the intended risk reduction.

Threat overviews, impact and risk analyses, stress tests and vulnerability surveys must be kept up-to-date and repeated periodically. These analyses may give cause to adjust the measures being implemented. But even if no modifications are necessary, such analyses form part of the continuous improvement of the MISH.

Improvements must be formulated in SMART terms, and be clearly embedded within the organisation. Intended improvements, activity schedules, conclusion and delivery must be documented. Implemented improvements must be evaluated according to effectiveness.

The MISH must be maintained in a systematic and documented manner, and be subject to continuous improvement.
Institutions must continually improve and update their MISH documentation. The following aspects of MISH documentation must be organised as part of a procedure: updating, securing, access, distribution, storage, storage period and destruction.

Appendix 1: Sources

Higher education institutions must comply with Dutch legislation, and are subject to a number of standards. This appendix presents an overview of standards and good practices for higher education institutions, as well as links to relevant security aspects.

0 General, Governance, Risk, Compliance

Organisation

- Integrated Security for Higher Education 2012 project group: Integrated security in higher-education governance and operations management (*Integrale veiligheid in governance en bedrijfsvoering in het hoger onderwijs*) is the manual for implementing integrated security in higher education.
- ASIS International (ANSI/ASIS SPC.4-2012), Maturity Model for the Phased Implementation of the Organizational Resilience Management System is a manual for phased implementation and a system of standards including six maturity levels for NEN 7131 – an organisational resilience management system (reference management system) for the MISH.
- Julian Talbot & Miles Jakeman (2009), Security Management Body of Knowledge, provides a clear survey of current attitudes to security management.

Job descriptions

- SURF, Information Security Officer Job Description Guideline (*Leidraad Functieprofiel Informatiebeveiliger*) provides job descriptions for the most common information security positions.
- ASIS International, ANSI/ASIS CSO.1-2013, Chief Security Officer – an organizational model offers security manager profile descriptions.

Consultative bodies

- Association of Universities in the Netherlands, VSNU: Consultative platform for security officers at research universities
- Association of Universities of Applied Sciences (VH): Consultative platform for security employees at universities of applied sciences
- Netherlands Federation of University Medical Centres (NFU): Special interest groups Information security and Privacy protection

Risks

- Ministry of Education, Culture and Science (OCW) Policy vision on Security and Radicalisation, 2009. This document defines four vital OCW interests: the uninterrupted operation of OCW institutions as effective and efficient educational, cultural and research systems; the continued performance of people working for and within OCW institutions and sectors; the continuous operation of OCW infrastructure; and the permanent existence of a social climate in which groups of people can cohabit effectively subject to the democratic rule of law (and applicable core values) and eight threats (CBRN[11] terrorism, animal rights activism, digital paralysis, flooding, pandemics, CBRN proliferation, radicalisation, and public safety).

[11] Chemical, biological, radio-active and nuclear.

Awareness

- The Awareness sub-project within the Integrated Security for Higher Education project aims to raise awareness levels and develop resources for doing so within higher education.

1 Working conditions

Sources

- VSNU Occupational health and safety catalogue (www.vsnu.nl/arbocatalogus.html)
  A catalogue drawn up by the Association of Universities in the Netherlands (VSNU), covering the following areas:
  1. Psychosocial work stress (PWS):
     - Undesirable behaviour towards staff (sexual harassment, aggression and violence, bullying, discrimination, stalking),
     - Work pressure and occupational stress among employees
  2. Arm, neck and shoulder complaints (RSI) among staff and students
  3. Hazardous substances
  4. Risk inventory and evaluation (RIE)
  5. Company emergency response (CER)
  6. Information, instruction and supervision
- Occupational health and safety catalogue for higher professional education (www.arbocatalogushbo.nl)
  A catalogue drawn up by the Netherlands Association of Universities of Applied Sciences (VH), covering the following areas:
  1. Healthy workspaces (VDU work, sedentary work)
  2. Sickness absence and prevention
  3. Work pressure
  4. Undesirable behaviour (sexual harassment, aggression and violence, bullying, discrimination)
  5. Work, pregnancy and breastfeeding
  6. Hazardous substances, biological agents and machine safety
- Note: The good practices from the above catalogues mainly target staff, and sometimes students. This means that some aspects are detailed for staff, but not for students.
- The Higher Education Appeals Tribunal (*College van beroep voor het hoger onderwijs*) is an independent body that deals with higher education court cases. Students may make an appeal if they do not agree with a decision made by the institution, which may also include failure to comply with policies and procedures, or the institution's disciplinary measures.
- NPR 5001 – Model for an OH&S management system
- NTA 8031 – Registration of workplace/business accidents

2 Environmental safety

Sources

- An Environmental Impact Assessment (*Milieueffectrapportage*) summarises the environmental effects of any decree before it is adopted. This way the government (i.e. the competent authority) issuing the decree can consider the environmental effects when making its decision.
- The Integrated Environmental Permit (*Omgevingsvergunning*) combines the permits for the occupation of a location, including the various environmental permits.

- Implementing regulations on radiation protection (*Uitvoeringsregeling stralingsbescherming*) by the Ministry of Economic Affairs, October 2013. These regulations list security requirements regarding resistance and accessibility of radioactive substances.
- Ministry of Economic Affairs, 2013: Information pack on the security of radioactive substances (*Handreiking beveiliging radioactieve stoffen*).
- SAAZ-UNIE is the alliance of OH&S and environmental departments of research universities and university medical centres, and serves as a periodic consultative platform for environmental officers, biological safety officers and radiology/radiation specialists.

3 Public safety

- M&O Group, commissioned by the National Anti-Terrorism and Security Coordinator (NCTV, 2013), Guide to identifying and managing security and lifestyle risks in higher professional education (*Handreiking voor signalering en begeleiding veiligheids- en leefstijlrisico's in het HBO*).

Violence at school

- The Centre for School and Safety (*Centrum School en Veiligheid*, www.schoolenveiligheid.nl), Guide to preventing and dealing with school attacks (*Handreiking preventie en omgaan met schoolaanslagen*). An information sheet on school shootings is also available.

Undesirable behaviour

- The Centre for School and Safety (*Centrum School en Veiligheid*), various information packs regarding undesirable behaviour: Aggression towards staff, Aggressive students, Aggressive parents, Discrimination and racism, Online bullying, Sexual harassment, Obligation of Education to Ensure Public Safety (*Veilige Publieke Taak Onderwijs*, an information forum on public safety at schools, www.forumveiligeschool.nl), Armed violence

Teaching Climate

- The Centre for School and Safety (*Centrum School en Veiligheid*), various information packs regarding the teaching climate: Citizenship, Conflict resolution, Behaviour and clothing, Peers, Social skills, Resilience, Sexual diversity
- The Centre for School and Safety (*Centrum School en Veiligheid*), various information packs on related subjects: Domestic violence, Sexual violence at home, Honour killings and forced marriage, Extremism and radicalisation, Physical safety, Safety and disabilities, Drugs at school, Media smarts

NOTE: School and Safety targets secondary and senior secondary vocational education. Higher education institutions will need to customise the information to their specific situation.

4 Integrity

Sources

- VSNU (2012), The Netherlands Code of Conduct for Academic Practice: Principles of good academic teaching and research (*De Nederlandse Gedragscode Wetenschapsbeoefening, principes van goed wetenschappelijk onderwijs en onderzoek*).
- National Board for Research Integrity (*Landelijk Orgaan Wetenschappelijke Integriteit*, LOWI) is an independent advisory body for breaches of academic integrity.
- Good Governance Advisory Committee (*Adviescommissie Behoorlijk Bestuur*, 2013), 'A difficult conversation – Good Governance Advisory Committee' (*'Een lastig gesprek – Advies Commissie Behoorlijk Bestuur'*).
- Integrated Security for Higher Education, SAINT (Self-Assessment of INTegrity). SAINT is a questionnaire developed by the National Office for Promoting Ethics and Integrity in the Public Sector (*Bureau Integriteitsbevordering Openbare Sector*) and is based on the espionage vulnerability analysis (KWAS) by the General Intelligence and Security Service (AIVD) concerning information security, integrity and knowledge security. A group-decision application is also available on this topic. The questionnaire and group-decision tool are currently under development.

5 Information security

Information security

- SURF, SCIPR is the national consultative body for information security professionals in higher education. Within the framework of SCIPR, SURF works with research universities and universities of applied sciences to improve the quality of professional information security in the higher education sector. SCIPR has made a range of template texts available.
- SURF, Framework of standards, assessments and benchmark. This is a framework of standards based on ISO27002 covering information security, continuity of business data, and privacy. An assessment is also available to show institutions their current maturity level in terms of information security. A benchmark instrument is also available.
- NEN-ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements.
- NEN-ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security controls
- ISO/IEC 27005:2014 Information technology -- Security techniques -- Information security risk management. Covers risk management with relation to information security.

Cybersecurity

- National Cyber Security Centre (NCSC)
- Integrated Security for Higher Education & SURF, Higher education threat summary. Concerns the cyber threats faced by higher education institutions.
- SURF, SURFcert provides institutions with security-incident support 24 hours a day, seven days a week.

IT Business Continuity Management

- SURF, Business continuity starter kit (*Starterskit Bedrijfscontinuïteit*): an approach to establishing and maintaining IT continuity plans. The starter kit also includes a large number of sample documents.

Digital rights

- SURF, information on digital rights:
  - Copyright
  - Open educational resources (OER)
  - Web lectures
  - Audiovisual materials
  - Learning analytics
  - Licences
  - Research data

6 Privacy

Sources

- Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*, CBP). Various notices and guidelines, including the ‘CBP Guidelines on Personal Data Security’ (*CBP Richtsnoeren Beveiliging van persoonsgegevens*).
- SURF, manuals, studies and presentations on privacy:
  - Privacy and the cloud
  - Privacy and digital identity
  - Legal operational conduct in ICT

- Privacy and students' personal data
- Various seminars in preparation of new privacy developments

- Association of Universities in the Netherlands (VSNU, 2005): Code of conduct governing the use of personal data in scientific research (*Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek*)
- SURF working party for supporting higher education institutions with new legislation

7 Knowledge security

Sources

- Integrated Security for Higher Education, SAINT (Self-Assessment of INTegrity). SAINT is a questionnaire developed by the National Office for Promoting Ethics and Integrity in the Public Sector (*Bureau Integriteitsbevordering Openbare Sector*) and is based on the espionage vulnerability analysis (KWAS) by the General Intelligence and Security Service (AIVD) concerning information security, integrity and knowledge security. A group-decision application is also available on this topic. The questionnaire and group-decision tool are currently under development.
- Espionage Vulnerability Analysis (*Kwetsbaarheidsanalyse Spionage*, KWAS) and the Guide to the Espionage Vulnerability Analysis (*Handleiding Kwetsbaarheidsonderzoek Spionage*) www.aivd.nl/dossiers/spionage
- Brochures: 'Espionage in the Netherlands, what are the risks?' (*Spionage in Nederland, wat is het risico?*); 'Espionage when travelling abroad, what are the risks?' (*Spionage bij reizen naar het buitenland, wat is het risico?*); and 'Digital Espionage, what are the risks?' (*Digitale Spionage, wat is het risico?*) www.aivd.nl/dossiers/spionage
- National Anti-Terrorism and Security Coordinator (NCTV), Espionage e-learning pack, www.nctv.nl/onderwerpen/spionage
- Espionage risk information www.aivd.nl/dossiers/spionage/persberichten
- National Anti-Terrorism and Security Coordinator (NCTV), Cyber Security Strategy 2.0 and Cyber Security Survey of the Netherlands 3, www.ncsc.nl
- General Intelligence and Security Service (AIVD), publication: Bring Your Own Device, www.aivd.nl/dossiers/cyberdreiging/publicaties

8 Internationalisation

Sources

- The Internationalisation Sub-project (*Deelproject Internationalisering*, 2014) has produced information and awareness materials for security issues related to internationalisation.
- EP-Nuffic, Code of Conduct with respect to international students in Dutch higher education.
- Advisory Council for Science, Technology and Innovation (AWTI), Going Dutch (2013). Analysis of the knowledge society from an international perspective.

9 Building security

General

- Buildings Decree (*Bouwbesluit*). Sites must comply with the Buildings Decree. Key requirements concern the location and construction of fire and smoke barriers, and the width and construction of emergency exits. The Buildings Decree is primarily an umbrella encompassing general requirements applicable to various aspects of building safety.

  - The Buildings Decree 2012 prescribes when fire and evacuation alarm systems are subject to certification. Usually, this applies to buildings containing less resilient individuals or large concentrations of people, possibly in combination with sleeping facilities. In principle educational and office buildings require no certification, unless these functions are combined with conference facilities. Active fire-extinguishing and smoke-reduction equipment that has been installed as part of equivalent safety requires certification, which involves ongoing periodic checks (at frequencies of 1 or 3 years, depending on whether fire alarms are/are not automatically forwarded to fire brigades). Fire and evacuation alarm systems must be managed and maintained.
  - Section 1.16 of the Buildings Decree (Duty of Care) states that the building owner is liable for the adequate management and maintenance of systems and fire barriers. There is no further specification of monitoring frequency, however, except that fire-resistant elements must be properly checked following any installation work.
  - Owners may set additional requirements, or determine their own ongoing monitoring systems.
- Integrated Environmental Permit. Specific building occupancy and safety risks are evaluated prior to issuing an integrated environmental permit.

Specific NEN standards

- Standards as included in the Regulations Governing the Buildings Decree (*Regeling Bouwbesluit*, latest version April 2014).
- Other standards applicable to building security include:
  - NEN-EN-ISO 16000 – Indoor air – Sections 1-7 (sampling)
  - NPR 5313 – Computer rooms and data centres – Security
  - NTA 8012 – Limitation of the damage due to fire of electrical wiring systems or flame spread along electrical wiring systems
  - NTA 8073 – Fixed fire-fighting systems – Automatic sprinkler systems
  - NTA 8101 – Terms of facilities for education – Definition and classification
  - NPR 1090 – Ventilation in school buildings – Examples of solutions for school buildings
  - NEN 3140 – Electrical installations
- NEN-EN-ISO 20957 – Stationary training equipment – General safety requirements and test methods
- ISO 55000 – Asset management. This standard also includes an asset risk analysis.

Security and public safety

- Centre for Crime Prevention and Public Safety (*Centrum voor Criminaliteitspreventie en Veiligheid*, CCV), Improved Risk Classification (VRKI) – Guide to burglary prevention for education institutions (*Richtlijn inbraakbeveiliging onderwijsinstellingen*) version 1.4 March 2014. Includes guidelines concerning theft/burglary risk.
- Centre for Crime Prevention and Public Safety (CCV). Safety Effect Report (VER). The VER is a process instrument for incorporating all security aspects as part of a site development pathway. It concentrates mainly on security, public safety and how crisis-proof the site is.
- ASIS International, ANSI/ASIS PAP.1-2013, Security Management Standard: Physical Asset Protection is a management system approach to physical on-site security.

Event security

- NTA 8020 – Event security and public security services.

10 Crisis management, company emergency response, business continuity management

Sources for Crisis Management

Company emergency response sources

- In 2014, NEN 8112 ‘Guidance on evacuation schemes for buildings’ and NEN 4000 ‘In-company emergency services’ will merge into a new NEN 8112 ‘Internal emergency response’. This standard will also include a toolkit.
- Dutch Institute for Company Emergency Response (NIBHV 2010), Company Emergency Response Guidebook 2010 (*Handleiding BHV 2010*), www.nibhv.nl/bhv

Sources for Business Continuity Management

- NEN-ISO 22301:2012-06, Societal security – Business continuity management systems – Requirements. The business continuity management system.
- NEN-ISO 22313:2013, Societal security – Business continuity management systems – Guidance provides some practical footholds for the implementation thereof.
- SURF, Business continuity starter kit (*Starterskit Bedrijfscontinuïteit*). an approach to establishing and maintaining IT continuity plans. The starter kit also includes a large number of sample documents.

Appendix 2: Framework for scheduling MISH goals and measures

The implementation of any project will, of course, be specific to each organisation. Keep the goal in mind: that the MISH is to be implemented within the organisation. The MISH is not a piece of technical equipment.

Some success factors for implementation:

- Ensure that the upper management announces that the MISH project is high priority, and that everybody's contributions are welcome.
- Ensure that the project involves people with knowledge of the processes and expertise in the field of security issues.
- Consider training sessions and workshops as a means of increasing employee involvement in the process.
- Involvement and ownership of the MISH can be increased by two-way communication with internal and external stakeholders.
- Monitor progress regularly.
- Modify the approach where necessary.
- Communicate with the commissioning body and stakeholders.
- Share and build on successes, both small and large.
- Involvement and ownership will grow with success.

The following framework is an EXAMPLE, and can serve as a basis for scheduling the activities necessary for implementing the MISH.

1. Project Schedule: Example MISH Implementation

	Remit	Steps	Participants	Result	Scheduling
1A	Obtain top-level support, commitment and participation for MISH	Put agreement with the MISH on the Executive Board agenda. Who in the Executive Board will take on the security portfolio (for the time being), and which senior manager will coordinate?	• Executive Board (EB) • Manager XXX •	EB approval to start MISH project	Date
1B	Appoint MISH project manager	EB appoints project manager	• Executive Board (EB) • Manager XXX	XXX is project manager	Date
1C	Staff the MISH team	Issue the request to managers, and gauge interest among candidates Ensure dissemination within the institution.	• Manager XXX • Managers • MISH project manager •	Members of the project team	Time period
1D	Set the supervisory committee and preconditions for supporting the MISH project	Appoint committee members, finalise roles, responsibilities and meeting frequency of the committee. Safeguard the involvement and best-efforts obligation of committee members.	• Manager XXX • Quality manager • MISH project manager •	Mandate and committee members	Date
1E	Give project members and supervisory committee MISH training	Organise a workshop/training tailored to both target groups, invite participants, make sure people attend	• MISH team • MISH committee members • Trainer/consultant •	MISH Project team and supervisory committee are trained to handle MISH tasks	Time period
1F					

2. MISH Strategic environment

	Remit	Steps	Participants	Result	Scheduling
2A	The MISH must be in line with the institution's strategic objectives.	The board must update the strategic goals and plans with the committee.	• Manager XXX • MISH Committee • MISH project manager •	MISH strategic goals implemented as part of the institution's strategy.	
2B	The CEO supports the objective of integrated security risk management via the MISH.	Create procedure for integrating the MISH into operations management.	• Executive Board (EB) • Manager XXX • MISH project manager	Management statement for introducing the MISH.	
2C	Joint framework and terminology for customising the MISH to the institution.	Have a number of MISH project team members prepare this.	• MISH team	1. Working party to customise MISH to the institution 2. Own MISH framework	
2D	Raise awareness in the institution for security risks, safe conduct and evaluate risk acceptance levels.	The project team will evaluate existing risk reports, evaluations and policy documents.	• MISH team • MISH Committee •	Institution's risk acceptance level is determined.	
2E			•		

3. Create a framework for evaluating and prioritising risks

	Remit	Steps	Participants	Result	Scheduling
3A	Develop a portfolio of risks relevant to the institution.	1. List, evaluate and categorise an initial 100 risks in a risk matrix (impact and likelihood). 2. Select 10-20 risks for mitigation. 3. Repeat this activity periodically.	• MISH team	A list of the most relevant risks requiring mitigation.	
3B	Develop methods or tools for risk identification and evaluation that employees can use in their day-to-day work.	Identify which methods or tools are already being used. Determine whether they can be employed more broadly, and adapt them if necessary.	• MISH team	Resources for day-to-day use within the institution for identifying and prioritising own risks, and evaluating mitigating measures.	
3C			•		

4. Review the risk management process

	Remit	Steps	Participants	Result	Scheduling
4A	Verify that all mitigating initiatives are properly adapted and contribute to an acceptable risk level.	Select the strategies and measures that will most effectively mitigate the prioritised risks.	• MISH team • MISH Committee • Works Council •	Board and policymakers are supported in managing risks.	
4B	Boost and ascertain the progress of the risk-management process.	Monitor, evaluate and provide feedback on proposed strategies and mitigating measures.	• MISH Committee • Executive Board (EB) •	Risk-management initiatives are implemented.	Ongoing
4C	Safeguard the MISH process so that the entire institution is committed and feels responsible for managing risks.	Integrate MISH processes into existing operations management. Draw up additional procedures for implementation of MISH.	• MISH Committee • Executive Board (EB) • MISH team	Defragmentation of security initiatives MISH process integrated into the organisation	
4D			•		

5. Develop an MISH communication, monitoring and reporting system

	Remit	Steps	Participants	Result	Scheduling
5A	Communication of MISH strategy and implementation	Assemble a working party for MISH promotion/communication. Determine the roles and prerequisites of this group.	• MISH team	Competent working party that shoulders promotion and communication responsibilities.	
5B	Communication of MISH strategy and implementation	Present MISH information to the Supervisory Board (SB), Works Council, to new staff, students and during strategic meetings.	• MISH team	Awareness of MISH throughout the institution and surrounding environment.	
5C	Communication of MISH strategy and implementation	Make MISH information available via the institution's website	• MISH team • Communications dept.	Information on MISH available to everybody	
5D	Communication of MISH strategy and implementation	Write articles for newsletters and the like.	• MISH team • Communications dept.	MISH awareness and education for all employees.	
5^{E}	Monitoring and Reporting	Develop KPIs for the monitoring and improvement of the MISH.	• MISH team •	MISH will become measurable and manageable.	
5F	Monitoring and Reporting	Develop a training programme and tool set for MISH monitoring and reporting.	• MISH team •	All employees are trained in dealing with security risks, and have access to tools for analysing and reporting on risks.	
5G	Monitoring and Reporting	Run MISH ‘tabletop’ and crisis management drills.	• MISH team • MISH Committee • Management	MISH objectives are adjusted and MISH is continuously improved	
5H	Monitoring and Reporting	Create an annual report for the EB and SB on MISH.	• MISH team • MISH Committee • Management	Accountability for MISH goals and results as been provided.	
5I			•		

Appendix 3: Relationships between threats, interests to be protected, and security aspects

All security issues can be reduced to an interest requiring protection, threats to that interest, and measures to protect it.

Meassure
Interest
Threat

It is also essential to have a clear understanding of the power-play of those involved. In the first instance, these people will be all of the stakeholders relevant to the interests. Who are the stakeholders, and what types of interests do they have? The parties involved can also be identified using a measures-based approach. They must implement the processes effectively, and have sufficient knowledge and expertise. Some measures will require weighing up several different interests (e.g. video surveillance: privacy vs. public safety). The threat analysis will reveal the agents responsible for any threats.

Taking a top-down approach, it is useful to organise efforts around security aspects, which must then be embedded as high up as possible and furnished with programmes and approaches. Their practical implementation, however, will run up against the complex web of interests, threats and measures/approaches. The ten security aspects mentioned each have the following inherent points of departure:

Security aspect	*Interest*	*Threat*	*Measure*
Integrated approach/Governance, Risk, Compliance			x
Working conditions	x		
Environment	x		
Public safety	x		
Integrity	x		
Information security	x		
Privacy	x		
Espionage/knowledge security	x	X	
Internationalisation	x		
Building security	x		
Crisis management, company emergency response, business continuity management	x		X

This still does not give a concrete idea of the interests to be protected, the types of threats envisaged and the principal categories of measures.

Breakdown of interests and threats, and relationships to security aspects

The following overviews set out the following relationships:

- Interests and threats
- Interests and security aspects
- Threats and security aspects

This is only an initial starting point, which institutions must further concretise themselves.

		Interests requiring protection	People	People abroad	Foreigners in NL	Knowledge	Personal data	Other information	ICT	Exam registration	Purchasing process	Financial process	Buildings	Labs, workstations, equipment, installations	Nuclear equipment	Lab animals
	To be protected against															
Organisational/technical failure																
Fire			x		x				x				x	x	x	x
Breakdown																
Power blackout									x				x	x	x	x
External ICT failure									x							
Waste, asbestos, chemical, radiological, nuclear process failure			x										x	x	x	
Animal care failure			x													x
Building systems failure													x	x	x	x
Traffic control failure			x										x			
Event/crowd control failure			x										x			
Food provision failure			x													
Wilful misconduct																
Theft																
	Trespassing and burglary (physical or digital)			?	?				x				x	x	x	x
	Theft of goods and information		x	x	x	x	x	x	x	x	x	x	x	x	x	x
Fraud						x	x			x	x	x		x		
Espionage			x	x	x	x	x			x	x					
Cyber attacks			x	x	x		x		x							
Violence																
	Bullying		x	x	x		x		x				x			

	Threats and intimidation		x	x	x		x									
	Blackmail or bribery		x	x	x		x									
	Serious (physical) threats		x	x	x								x	x	x	x
	Hostages, abduction			x												
Public order																
	Occupation, barricading, protest												x	x	x	x
Sabotage																
	Small acts of destruction		x						x				x	x	x	x
	Arson												x	x	x	x
	Wilful damage to buildings												x	x	x	x
Other																
	Buildings blown up/shot at		x	x	x								x	x	x	x
	Bomb scare (real or fake)		x										x			
Negligence and lack of discipline																
	Gross negligence		x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Ignoring no-smoking regulations		x										x	x	x	x
	Ignoring parking regulations		x										x			
External threats																
	Extreme flooding, snow, ice		x						x				x	x	x	x
	Extreme heat/cold		x						x				x	x	x	x

		Security aspect	Governance, risk, compliance	Working conditions	Environmental safety	Public safety	Integrity	Information security	Privacy	Knowledge security/espionage	Internationalisation	Building security	Crisis management, company emergency response, business continuity management
	To be protected against												
Organisational/technical failure													
Fire			x	x	x			x				x	x
Breakdown													
Power blackout			x					x				x	x
External ICT failure			x										x
Waste, asbestos, chemical, radiological, nuclear process failure			x	x	x							x	x
Animal care failure			x	x	x							x	x
Building systems failure			x	x		x						x	x
Traffic control failure			x			x						x	x
Event/crowd control failure			x			x						x	x
Food provision failure			x	x									x
Wilful misconduct													
Theft													
	Trespassing and burglary (physical or digital)		x	x		x		x		x	x	x	x
	Theft of goods and information		x	x		x		x		x	x	x	x
Fraud			x				x	x		x			x
Espionage			x					x		x	x		x
Cyber attacks			x			x		x		x			x
Violence													
	Bullying		x	x		x			x		x		x
	Threats and intimidation		x	x		x			x		x		x
	Blackmail or bribery		x	x		x			x		x		x
	Serious (physical) threats		x			x					x		x
	Hostages, abduction		x	x		x					x		x
Public order													
	Occupation, barricading, protest		x									x	x
Sabotage													
	Small acts of destruction		x			x						x	x
	Arson		x									x	x
	Wilful damage to buildings		x									x	x
Other													
	Buildings blown up/shot at		x	x								x	x
	Bomb scare (real or fake)		x	x								x	x

Negligence and lack of discipline													
	Gross negligence		x	x	x	x	x	x	x	x	x	x	x
	Ignoring no-smoking regulations		x	x								x	x
	Ignoring parking regulations		x									x	x
External threats													
	Extreme flooding, snow, ice												
	Extreme heat/cold												

		Interests requiring protection	People	People abroad	Foreigners in NL	Knowledge	Personal data	Other information	ICT	Exam registration	Purchasing process	Financial process	Buildings	Labs, workstations, equipment, installations	Nuclear equipment	Lab animals
	Security aspect															
	Governance, risk, compliance		x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Working conditions		x	x	x								x	x	x	x
	Environment												x	x	x	x
	Public safety		x	x	x				x							
	Integrity		x	x	x	x	x			x	x	x				
	Information security		x	x	x	x	x	x	x	x	x	x		x	x	
	Privacy		x				x									
	Knowledge security/espionage		x	x	x	x				x	x					
	Internationalisation			x	x											
	Building security												x	x	x	x
	Crisis management, company emergency response, business continuity management		x	x	x	x	x	x	x	x	x	x	x	x	x	x

SAFE AND OPEN
HIGHER EDUCATION

Publication details

Commissioning Body:	Project Group: Integrated Security for Higher Education
Project contact person:	Paul Goossens (p.a.m.goossens@hr.nl)
Created by:	Joris Hutter en Marcel Spit (*Adviescentrum BVI*)
Contributors:	Jeroen Terstegge (Privacy Management Partners) Alex Ivanovic (*Adviesbureau Forta Nova*)
Date:	MAY 2014