

TECHNICAL
SPECIFICATION

ISO/IEC TS
27022

First edition
2021-03

**Information technology — Guidance
on information security management
system processes**



Reference number
ISO/IEC TS 27022:2021(E)



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure and usage of this document	2
5 Overview	3
6 Management processes	6
6.1 General.....	6
6.2 Information security governance/management interface process.....	7
7 Core processes	9
7.1 General.....	9
7.2 Security policy management process.....	9
7.3 Requirements management process.....	10
7.4 Information security risk assessment process.....	13
7.5 Information security risk treatment process.....	14
7.6 Security implementation management process.....	17
7.7 Process to control outsourced services.....	19
7.8 Process to assure necessary awareness and competence.....	21
7.9 Information security incident management process.....	22
7.10 Information security change management process.....	25
7.11 Internal audit process.....	27
7.12 Performance evaluation process.....	29
7.13 Information security improvement process.....	31
8 Support processes	33
8.1 General.....	33
8.2 Records control process.....	33
8.3 Resource management process.....	35
8.4 Communication process.....	37
8.5 Information security customer relationship management process.....	39
Annex A (informative) Statement of conformity to ISO/IEC 33004	41
Bibliography	43

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

An information security management system (ISMS) includes a collection of interacting processes and is operated by performing those processes. This document provides a process reference model (PRM) for information security management, which differentiates between ISMS processes and measures/controls initiated by them.

A PRM is a model comprising definitions of processes described in terms of process purpose and results, together with an architecture describing the relationships between the processes. Using the PRM in a practical application can require additional elements suited to the environment and circumstances.

The PRM specified in this document describes the ISMS processes implied by ISO/IEC 27001. The PRM is intended to be used as a process implementation and operation guide.

Any organization can define processes with additional elements in order to tailor it to its specific environment and circumstances. Some processes cover general management aspects of an organization. These processes have been identified in order to support organizations in addressing the requirements of ISO/IEC 27001.

Information technology — Guidance on information security management system processes

1 Scope

This document defines a process reference model (PRM) for the domain of information security management, which is meeting the criteria defined in ISO/IEC 33004 for process reference models (see [Annex A](#)). It is intended to guide users of ISO/IEC 27001 to:

- incorporate the process approach as described by ISO/IEC 27000:2018, 4.3, within the ISMS; — be aligned to all the work done within other standards of the ISO/IEC 27000 family from the perspective of the operation of ISMS processes
- support users in the operation of an ISMS – this document is complementing the requirements-oriented perspective of ISO/IEC 27003 with an operational, process-oriented point of view.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1

core process

process that delivers apparent and direct customer value and is derived from the *core competencies* (3.1) of the management systems

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO 38500:2015. Note

2 to entry: In this definition, "core competency" is understood as the set of skills and know-how present within a management system, directly aligned with the objectives of the management system, supporting the achievement of the objectives and not elsewhere present within the organization at a competitive level.

3.2

integrated management system

IMS

management system that integrates all of an organization's systems – like information security management and business continuity management – and processes in to one complete framework, enabling an organization to work as a single unit with unified objectives

3.3

key goal indicator

indicator that is an ex-post measure for the achievement of a goal/objective

3.4

key performance indicator

indicator that is an ex-ante measure, which allow a prediction if a goal/objective is achieved in the future

3.5

management process

process that defines the objectives of the management system to achieve the strategic objectives set by the organization's governing body

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO/IEC 38500:2015.

3.6

support process

process that supports core processes by providing and managing necessary resources without delivering direct customer value

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO/IEC 38500:2015.

4 Structure and usage of this document

The objective of this document is to guide the users of ISO/IEC 27001 on the operation of the ISMS. No additional requirements are defined within this document.

It is not intended to be used “out of the box” without adapting it to the implementing organization and it should not be used as requirements within ISMS certification audits.

The model architecture specifies a process architecture for the domain and comprises a set of processes, with each described in terms of process, purpose and results. The PRM is closely aligned to the information security requirements as contained in ISO/IEC 27001:2013. Processes are differentiated in core, management and supporting processes. The PRM is also meeting the criteria defined in ISO/IEC 33004 for process reference models.

Each process of this PRM is described in terms of:

- process category;
- brief description;
- process flowchart;
- objective/purposes;
- input and results;
- activities/functions;
- references.

The PRM does not attempt to place the processes in any specific environment nor does it pre-determine any level of process capability/maturity required to fulfil the ISO/IEC 27001 requirements.

The PRM provides a detailed but generic blueprint regarding the core processes of an ISMS. The PRM is applicable to all organizations independent of their size, objectives, business model, location, etc. The ISMS PRM should be used as a prototype for an ISMS, which needs to be tailored to the objectives, needs and individual requirements of the implementing organization. The tailoring of the PRM can include omission of some of the listed processes, where they are inapplicable or would be reduced to vestigial form.

The process orientation of the PRM also supports the transition from designing and implementing an ISMS (project phase) to the operation of the ISMS (performing the processes). The process orientation also supports and allows the integration of the ISMS processes in further domains of an integrated management system, described within the ISO handbook “The Integrated Use of Management System Standards (IUMSS)”.

5 Overview

The fundamental elements of a PRM are the descriptions of the processes within the scope of the model. The process descriptions in the PRM incorporate a statement of the purpose of the process, which describes at a high level the overall objectives of performing the process.

An ISMS incorporates processes, for example shown in [Figure 1](#). The listed processes illustrate key topics that should be considered during the process design phase when implementing an ISMS.

The PRM should not be used “out of the box” without adapting it to the objectives, needs and individual requirements of the implementing organization. For every ISMS process, the individual necessary maturity level should be determined, implemented and operated. A possible result of determining the necessary maturity level of a process can be, that the process is not needed at all (maturity level zero).

ISMS processes should be individually integrated into existing management systems and processes. This is not displayed in the figure to ensure readability and due to existing management systems differing too much in praxis.

Interfaces to the ISMS processes are described within the detailed process profiles and process flow charts. Interfaces to the records control process and to the security policy management process are only described within the detailed process profiles to ensure readability of the process flow charts.

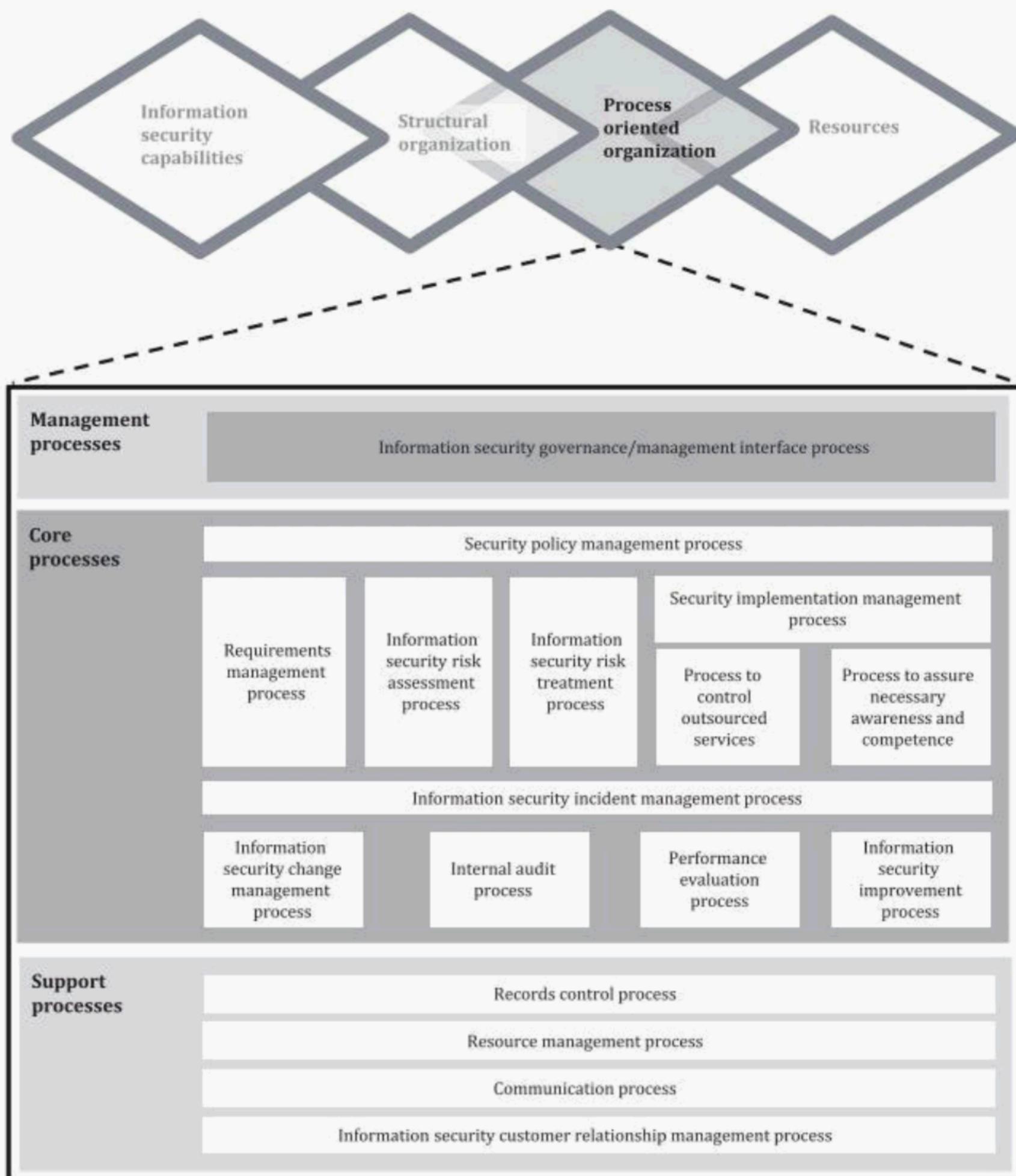


Figure 1 — ISMS process reference model

The **information security governance/management interface process** should ensure an alignment of the ISMS with the objectives and needs of the overall organization and its stakeholders.

The **security policy management process** should be the process for the development, maintenance and retention of information security policies, standards, procedures and guidelines – referred to as “IS policies”.

Key to satisfying the ISMS objectives is an up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS. This should be realized within the **requirements management process**, which should identify legal, statutory, regulatory and contractual requirements for the risk assessment process, the internal audit process and the process to control outsourced processes.

In the **risk assessment process**, risks should be identified, analysed and evaluated. The results of this process should be documented and the evaluated risks captured in a list of prioritized risks with risk owners, which should be input for the communication process and the information security risk treatment process.

In the **information security risk treatment process**, risk treatment options should be identified and selected, and control objectives/controls should be determined necessary for the chosen risk treatment options. The results of this process should be lists with determined controls and control objectives, a risk treatment plan including acceptance of residual risks, a control implementation plan and requests for changes for the information security change management process, which are used as input in various ISMS processes.

The **security implementation management process** should be the process to initiate and verify the implementation of the risk treatment plan and necessary changes.

As services are outsourced, these services need to be determined and controlled, which should be realized within the **process to control outsourced services**.

Within the **information security awareness process**, an information security awareness, training and education program should be developed and implemented to ensure that all personnel receive the necessary security training and/or education.

The **information security incident management process** should be for detecting, reporting, assessing, responding to, dealing with and learning from information security incidents. The results of this process are identified incidents, which should be used in various ISMS processes including the information security change management process and the process to ensure necessary awareness and competence.

The implementation of controls always constitutes changes, which should be managed within a general change management process of the implementing organization or – if the change focuses on an ISMS element – within the **information security change management process**. The information security change management process is the process to control changes of ISMS elements and review the consequences of unintended changes. This process only focusses on change management of the ISMS. The results of this process should be necessary changes (for records control process), proposed and necessary changes as well as results of changes (for and from risk assessment process), initiation of risk assessment when significant changes are proposed or occur, and the results of changes to information security incident management process, as that process initiated them.

The **performance evaluation process** should contain monitoring, measurement, analysis and evaluation of two main criteria. First, the performance of the security controls and second the performance of the ISMS processes. Performance measurement differs from performance audit (within the **internal audit process** where effectiveness and efficiency of the ISMS and implemented controls are audited), which should be performed independently.

Results from the performance evaluation process, the internal audit process as well as results from the service provider audits from the process to control outsourced services should be used to improve effectiveness, efficiency, suitability and adequacy of the ISMS and the controls. This should be realized within the **information security improvement process**.

Within the **records control process** information determined to be necessary for the effectiveness and/or the demonstration/provision of documented evidence of the effectiveness of the ISMS should be identified, created, updated and controlled.

To implement the controls as well as to run the ISMS processes resources are needed which should be identified, allocated and monitored in the **resource management process**. Results of the resource management process should be planned/document resources to implement and run determined controls, categorization of controls regarding who funds the control, planned and documented resources to run the ISMS core processes, reports regarding resource usage of ISMS core processes, and for the information security customer relationship management process: reports on resource usage.

Results of nearly all ISMS processes should be centrally communicated within the **communication process** to interested parties outside the ISMS. This should include the communication of risks and information security management reports. Those reports as well as identified requirements should serve as input for the information security governance/management interface process.

The information security governance/management interface process forms the interface between the ISMS and its interested parties. Beside this, the operational management of the customer satisfaction level as well as the continuous demonstration of the added value of investments in information security should be realized. This should be done within the **information security customer relationship management process**.

All processes have the potential to be designed and implemented as integrated processes within an IMS. Synergy effects resulting from the integration of processes into an IMS should be identified and realized wherever possible as suitable.

The processes are described in more detail in [Clause 6 to 8](#) and [Tables 1 to 17](#).

6 Management processes

6.1 General

This clause describes management processes of an ISMS. The concepts and purposes embodied in these example processes should be considered during the process planning phase of an ISMS implementation project.

6.2 Information security governance/management interface process

Table 1 — Process profile — Information security governance/management interface process

Process name	Information security governance/management interface process
Process category	Management process
Brief description	This process ensures that information security is managed in a way that meets the needs of the organization.
Objective/purposes	Objective of this process should be to ensure an alignment of the ISMS with the objectives and needs of the organization.
Input	<ul style="list-style-type: none"> — From requirements management process: Requirements for approval. — From communication process: Information security management reports containing: <ul style="list-style-type: none"> — former management reports; — status of actions from former management reports; — changes in requirements (external and internal issues as they are relevant for the ISMS); — audit reports (including feedback on the information security performance, including trends in nonconformities and corrective actions, monitoring and measurement results, audits results and fulfilment of information security objectives); — feedback from interested parties; — results of risk assessment and status of risk treatment plan; — opportunities for continual improvement; and — incident reports.
Results	<ul style="list-style-type: none"> — For requirements management process: <ul style="list-style-type: none"> — strategic objectives, goals, vision, restrictions, approved requirements; — list of interested parties of the ISMS; — risk criteria; — existing management systems; — approved requirements. — For records control process: Decisions related to the governance of the ISMS.
Activities/functions	<ul style="list-style-type: none"> — For information security change management: Change requests. — Initiate the ISMS. — Review reports (measurement, audit reports, results of risk assessment and status of risk treatment plan and feedback from interested parties). — Generate and provide feedback to top management, decisions and, if necessary, change requests.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 5.1 and 9.3 — ISO/IEC 27003:2017, 8.4

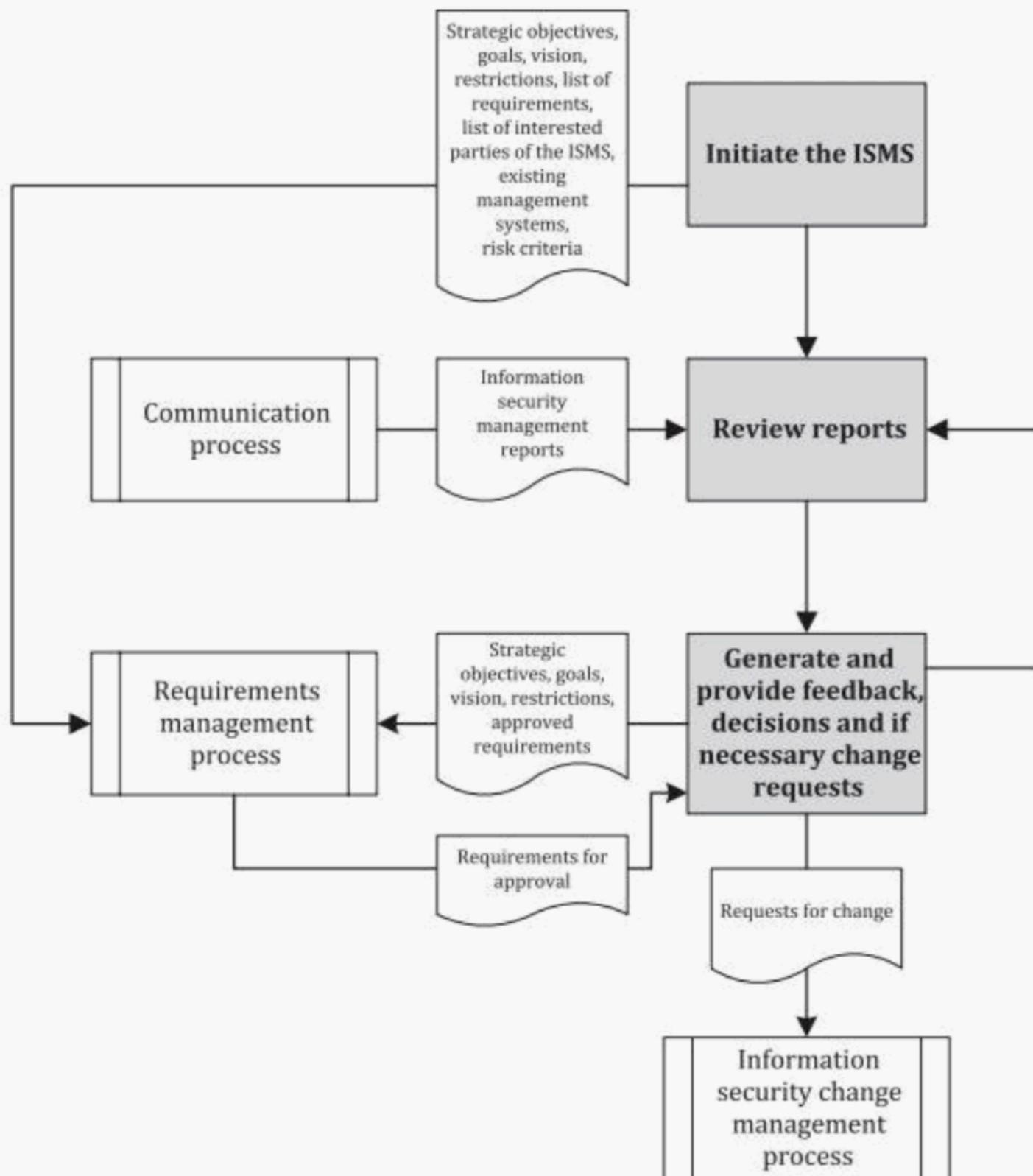


Figure 2 — Process flow chart — Information security governance/management interface process

7 Core processes

7.1 General

This clause describes example core processes that can be found in an ISMS. The concepts and purposes embodied in these example processes should be considered during the process planning phase of an ISMS implementation project.

7.2 Security policy management process

Table 2 — Process profile — Security policy management process

Process name	Security policy management process
Process category	Core process
Brief description	The security policy management process should be the process to develop, maintain and retention of information security policies, standards, procedures and guidelines (referred to as “IS policies”).
Objective/purposes	Ensure that appropriate policies, standards, procedures and guidelines (IS policies) regarding information security are developed, maintained, available and understood by the target group.
Input	<ul style="list-style-type: none"> — From all other information security processes (as basis for policies): Results of the processes. — From change management process: Necessary changes of policies in form of change requests.
Results	<ul style="list-style-type: none"> — For communication process, internal audit process, performance evaluation process, records control process and the process to assure necessary awareness and competence: Appropriate IS policies.
Activities/functions	<ul style="list-style-type: none"> — Obtain input from ISMS processes and develop IS policies. — Obtain formal approval of IS policies. — Distribution of IS policies (via communication process). — Storage and preservation, including preservation of legibility. — Control of changes/version control. — Obtain replaced versions of IS policies. — Deletion or disposal of IS policies after retention period.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 5.2, 7.4 and 7.5 — ISO/IEC 27003:2017, 5.2, 7.4, 7.5 and Annex A

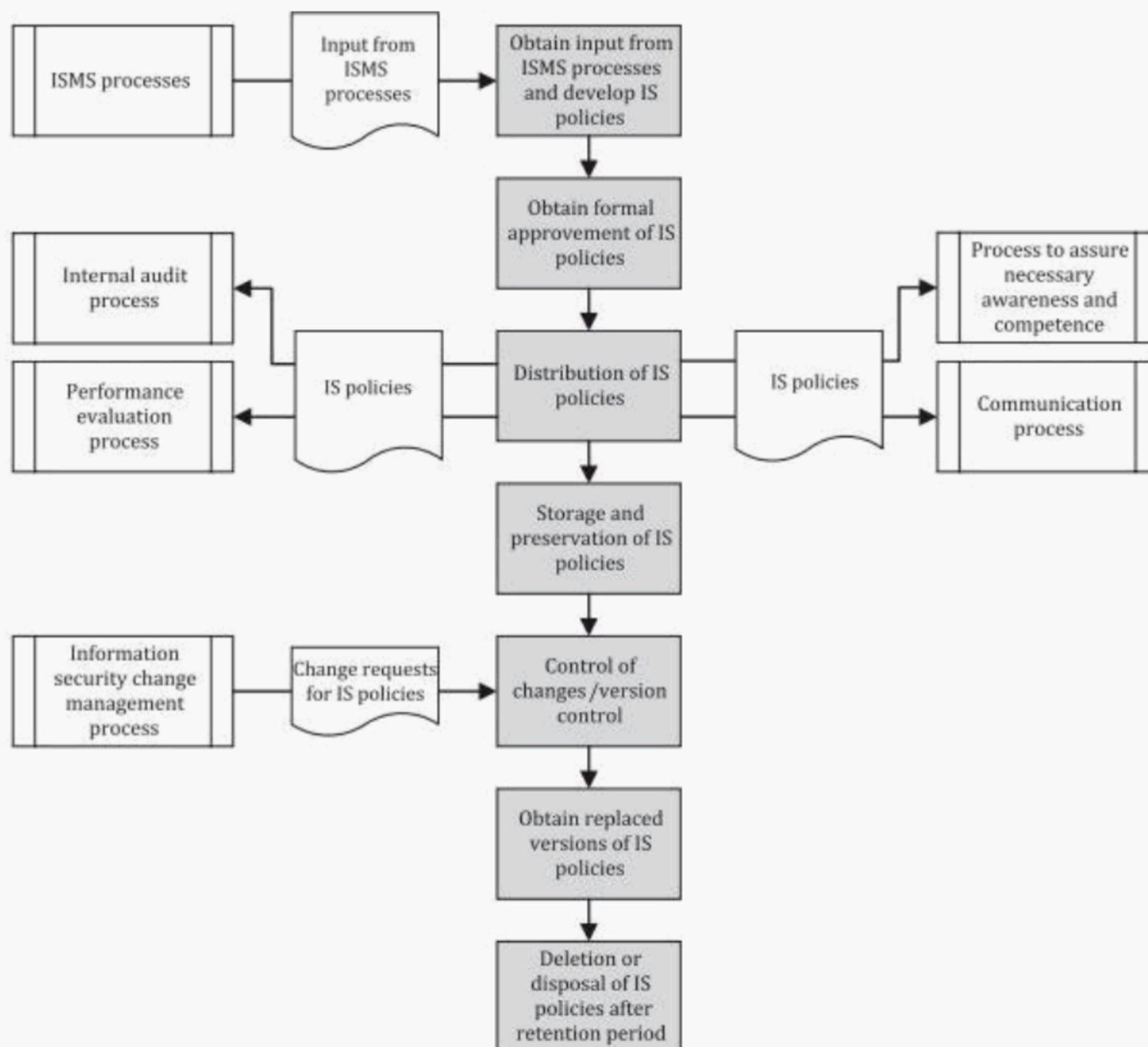


Figure 3 — Process flow chart — Security policy management process

7.3 Requirements management process

Table 3 — Process profile — Requirements management process

Process name	Requirements management process
Process category	Core process
Brief description	Requirements management process should be the process to ensure an up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS.
Objective/purposes	All relevant legislative statutory, regulatory, contractual requirements are met.

Table 3 (continued)

Process name	Requirements management process
Input	<ul style="list-style-type: none"> — From information security risk assessment process: List of prioritized risks. — From information security governance/management interface process (top management): <ul style="list-style-type: none"> — strategic objectives, goals, vision, restrictions and list of requirements; — list of interested parties of the ISMS; — existing management systems; — risk criteria; — approved requirements. — From other organizational units or functions: Already identified requirements. — From information security customer relationship management process: Requirements of customers. — From information security incident management process: Incidents.
Results	<ul style="list-style-type: none"> — For internal audit process, the information security risk assessment process, the process to control outsourced services, communication process and the records control process: Documented and assigned requirements regarding information security including a list of the legislative and regulatory references including contracts and agreements applicable to the organization. — For information security governance/management interface process (top management): Requirements for approval.
Activities/functions	<ul style="list-style-type: none"> — Understand the internal and external context (organization and ISMS). — Identify and document requirements: <ul style="list-style-type: none"> — identification of risk criteria; — identification of applicable legislation and contractual requirements; — identification of requirements from assessed risks (current and projected information security threat environment); — identification of requirements from principles, objectives, requirements for information processing; — identification of requirements from incidents; — identification and prioritization of conflicting requirements. — Top management review and approval of identified requirements. — Assign responsibilities to meet the requirements. — Communicate requirements and responsibilities. — Document approach to meet identified requirements. — Keep requirements up to date (start process again).
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 4.1, 4.2, 5.1 b), 6.2 c) and 8.1 — ISO/IEC 27003:2017, 4.1, 4.2, 5.1 b), 6.2 c) and 8.1

.....

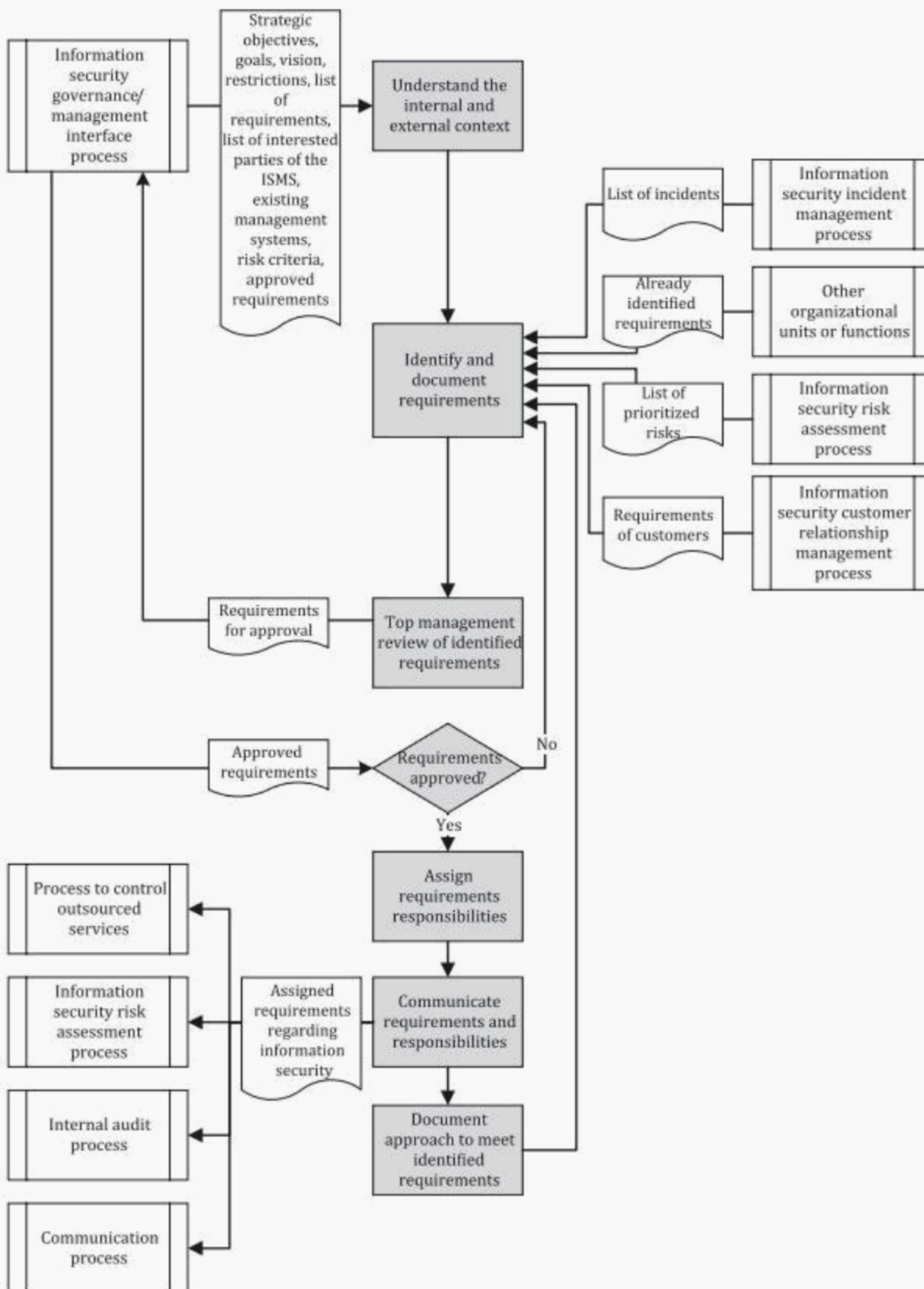


Figure 4 — Process flow chart — Requirements management process

7.4 Information security risk assessment process

Table 4 — Process profile — Information security risk assessment process

Process name	Information security risk assessment process
Process category	Core process
Brief description	The information security risk assessment process should be the overall process of risk identification, analysis and risk evaluation.
Objective/purposes	<ul style="list-style-type: none"> — Identify, analyse and evaluate all relevant information security risks. — Identify risk owners: Ensure consistent, valid and comparable results of risk assessment.
Input	<ul style="list-style-type: none"> — From information security risk assessment process itself: <ul style="list-style-type: none"> — previous results from information security risk assessment; — previously identified information security status. — From configuration management process: Information assets. From requirements managements: Assigned requirements regarding information security. — From information security change management process: Proposed changes and results of changes. — From information security incident management process: Incidents.
Results	<ul style="list-style-type: none"> — For information security risk treatment process, communication and requirements management process: Documented, evaluated and prioritized risks (list) and risk owners. — For information security change management process: Evaluated risks of proposed changes. — For information security risk assessment process itself: <ul style="list-style-type: none"> — previous results from information security risk assessment; — previously identified information security status. — For communication process: List of prioritized and evaluated risks. — For requirements management process: List of prioritized and evaluated risks. — For records control process: Results from information security risk assessment (information security risk register).
Activities/functions	<ul style="list-style-type: none"> — Identify risks. — Identify consequences of risks: <ul style="list-style-type: none"> — identify consequences of incurred or realized risks; — assess business impact of risks. — Assess likelihood of risks. — Risk evaluation – compare levels of risk (consequences and likelihood) against evaluation and acceptance criteria. — Update information security risk register.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 6.1.2 — ISO/IEC 27003:2017, 6.1.2



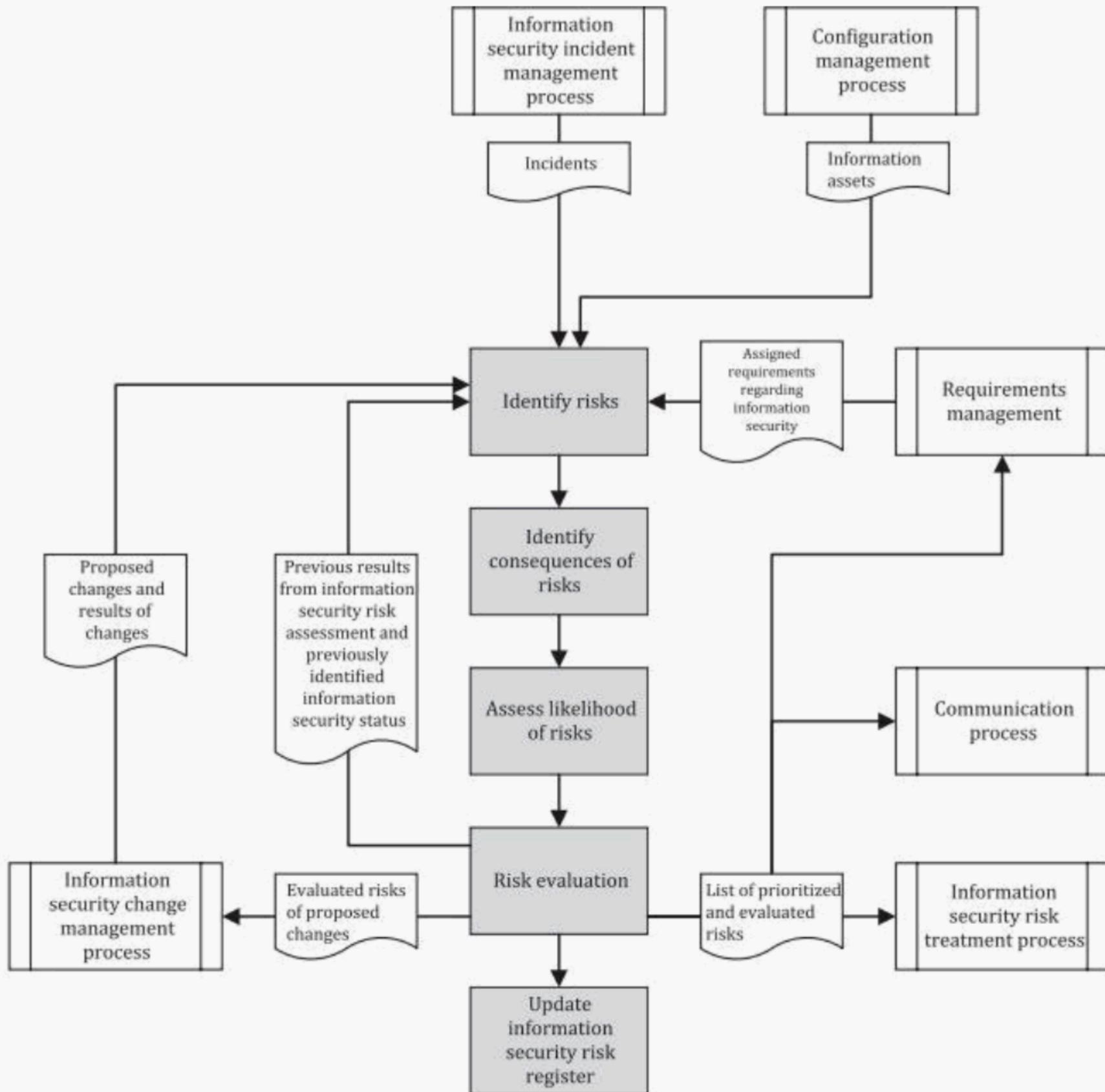


Figure 5 — Process flow chart — information security risk assessment process

7.5 Information security risk treatment process

Table 5 — Process profile — Information security risk treatment process

Process name	Information security risk treatment process
Process category	Core process
Brief description	The information security risk treatment process should be the process to identify and select risk treatment options including determination of control objectives and controls necessary to implement the information security risk treatment option(s) chosen.
Objective/purposes	<ul style="list-style-type: none"> — Identify and select appropriate risk treatment options. — Determine necessary control objectives and controls.

Table 5 (continued)

Process name	Information security risk treatment process
Input	<ul style="list-style-type: none"> — From information security risk assessment process: Documented and evaluated risks in a list of prioritized risks. — From resource management process: Estimation of necessary resources for the control implementation. — From security implementation management process: Results of control implementation.
Results	<ul style="list-style-type: none"> — For resource management process: Determined controls, control objectives, list of approved ISMS controls. — For process to control outsourced services, communication process, internal audit process, performance evaluation process, and process to assure necessary awareness and competence: Risk treatment plan including acceptance of residual risks as well as a list with determined controls and control objectives. — For security implementation management process: Control implementation plan. — For information security change management process: Requests for changes. — For communication process: Results of control implementation. — For records control process: Results from information security risk treatment.
Activities/functions	<ul style="list-style-type: none"> — Identify options for the treatment of risks. — Determine the control objectives and controls. — Compare controls with those in ISO/IEC 27001:2013, Annex A. — Communicate list of determined controls to resource management process to obtain initial resource requirements – if necessary, repeat this step and the determination of controls if necessary resources for a control are not appropriate. — Describe residual risks. — Obtain risk owners approval for risk treatment plan. — Produce Statement of Applicability (SoA). — Derive control implementation plan from risk treatment plan including: <ul style="list-style-type: none"> — owner of the control/responsible person for the implementation; — priority, time target and resources for the implementation; — tasks or activities to implement the control. — Initiate control implementation. — Obtain and communicate results of control implementation. — Update information security risk register.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 6.1.3 — ISO/IEC 27003:2017, 6.1.3

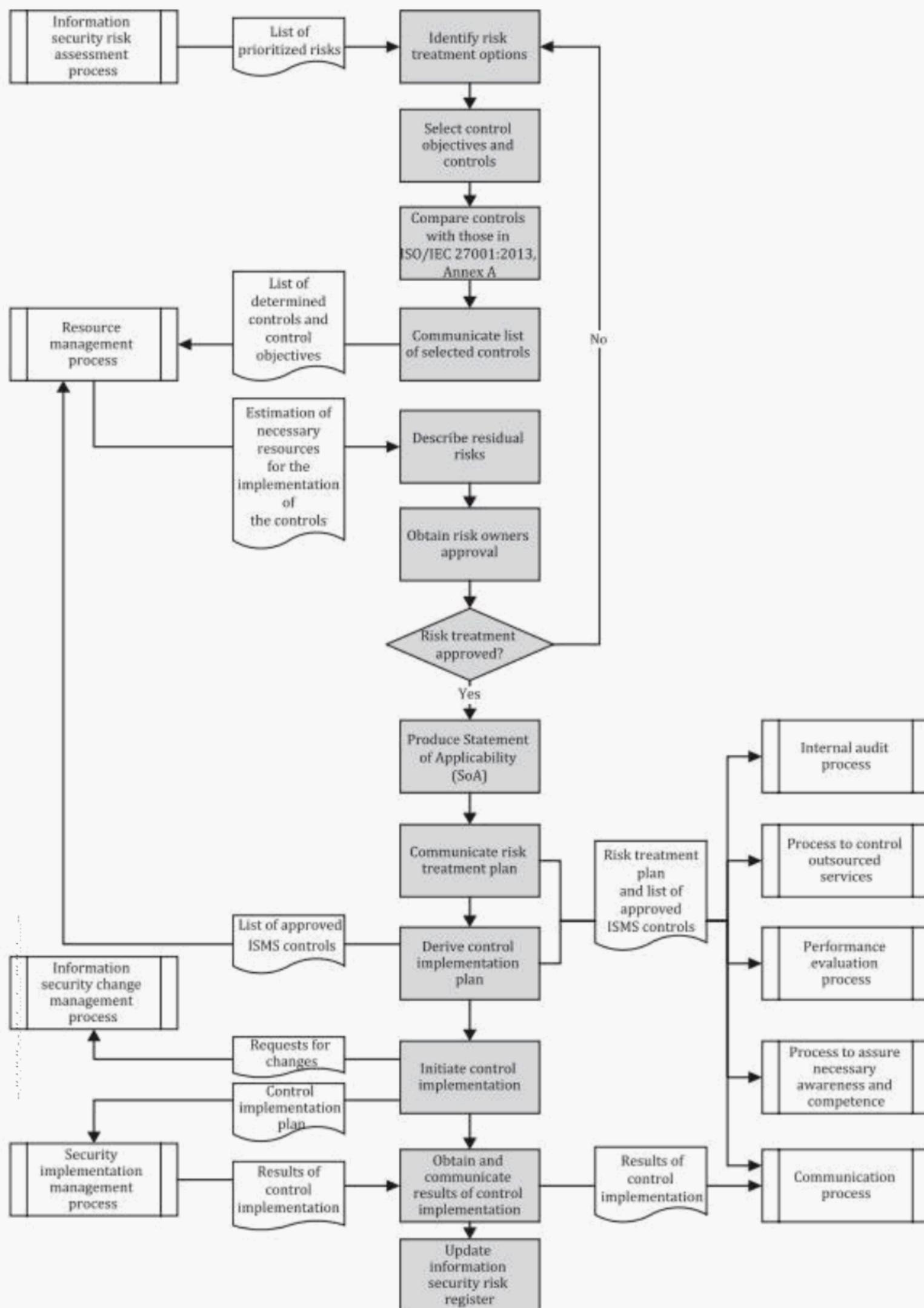


Figure 6 — Process flow chart — information security risk treatment process

7.6 Security implementation management process

Table 6 — Process profile — Security implementation management process

Process name	Security implementation management process
Process category	Core process
Brief description	The security implementation management process should be the process to initiate and verify the implementation of the risk treatment plan and necessary changes.
Objective/purposes	— Ensure that the risk treatment plan and necessary changes are executed as planned.
Input	<ul style="list-style-type: none"> — From information security risk treatment process: Control implementation plan. — From information security change management process: Control implementation plan. — From change management process: Status regarding implementation.
Results	<ul style="list-style-type: none"> — For information security change management process: Results of changes. For — information security risk treatment process: Results of control implementation. — For change management process: Proposed changes and control implementation plan.
Activities/functions	<ul style="list-style-type: none"> — Initiate implementation: <ul style="list-style-type: none"> — define and prioritize proposals for work packages/internal projects; — perform workshops with asset owners and/or necessary departments (for example IT, facility management, personnel management, etc.) regarding work packages and internal projects and ensure understanding of accountability and responsibility of the asset owners. — Support implementation in the change management process in the role as an interested party. — Verify implementation.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 8.1 — ISO/IEC 27003:2017, 8.1

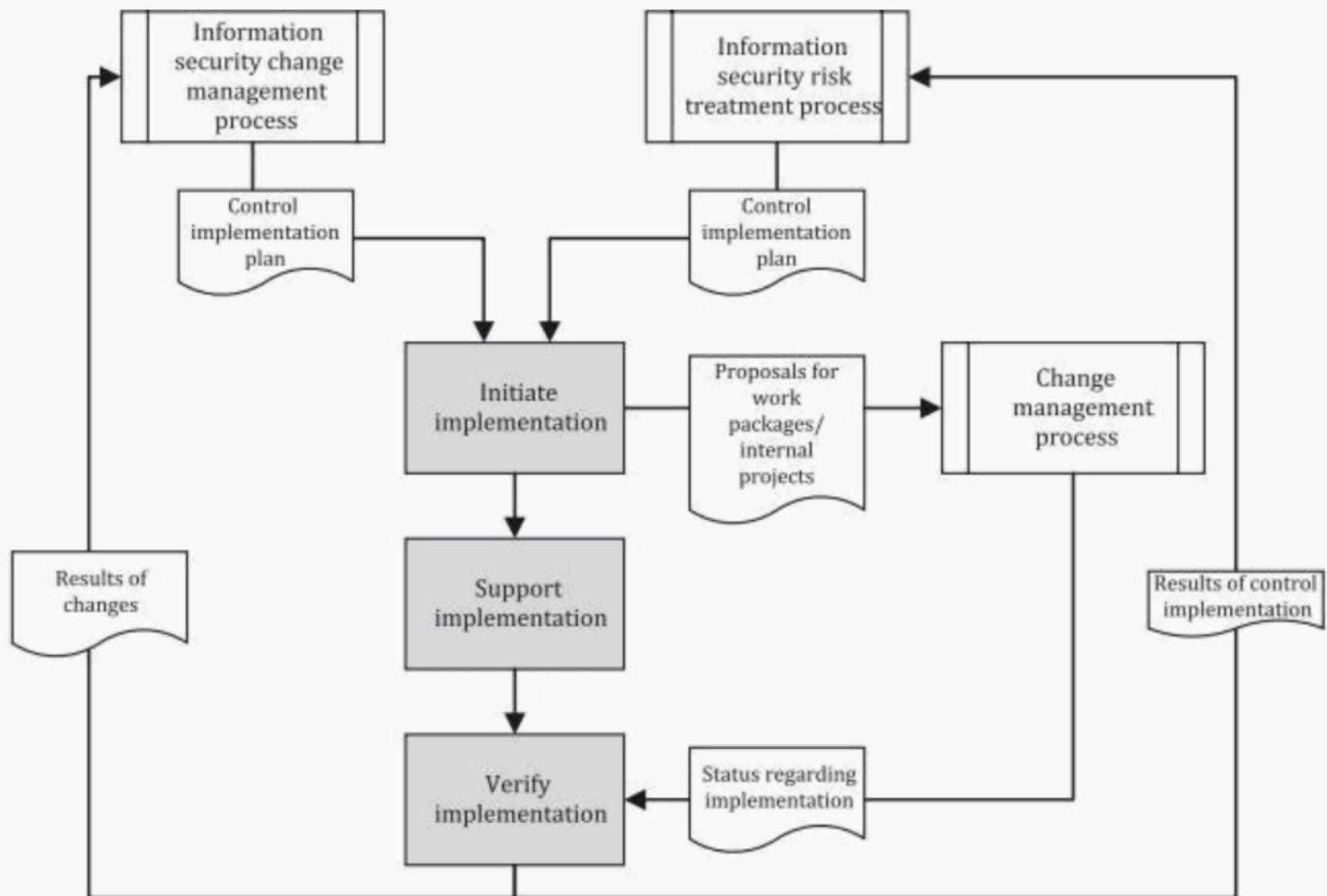


Figure 7 — Process flow chart — Security implementation management process

7.7 Process to control outsourced services

Table 7 — Process profile — Process to control outsourced services

Process name	Process to control outsourced services
Process category	Core process
Brief description	The process to control outsourced services should be the process to ensure that outsourced services are determined and controlled. This includes identification and documentation of outsourced services as well as dependencies from external parties.
Objective/purposes	The objective of this process should be to mitigate any adverse effects of outsourced services and to ensure that information provided to external service providers are processed in compliance with the information security requirements of the outsourcing organization.
Input	<ul style="list-style-type: none"> — From requirements management process: Applicable security requirements. — From other organizational units: Contracts, list of external suppliers and service providers; overview of outsourced services including contractual agreements and assessed dependencies. — From security risk treatment process: Controls and control objectives regarding outsourced services. — From information security incident management process: (Potential) security incidents regarding the provision of services from third parties.
Results	<ul style="list-style-type: none"> — For information security change management process: Request for changes – Initiation of necessary changes in contracts or of service providers. — For records control process: Audit program and plans for service provider audits regarding information security, audit results (not displayed in process chart). — For communication process (management review and improvement process): Audit reports for service provider audits regarding information security. — For information security incident management process: Direct information of potential incidents detected during service provider audits. — For information security improvement process: Audit reports of service provider audits.
Activities/functions	<ul style="list-style-type: none"> — Identify and document outsourced services. — Identify security requirements for outsourced services. — Analyse drafts or final contracts if security requirements are met (Ensure that information security requirements are addressed properly in the contracts). — Develop request for changes regarding requirements stipulated in contracts. — Analyse dependencies from external parties. — Plan and execute service provider audits regarding compliance with information security requirements. — Report/communicate results of service provider audits.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 8.1 — ISO/IEC 27003:2017, 8.1

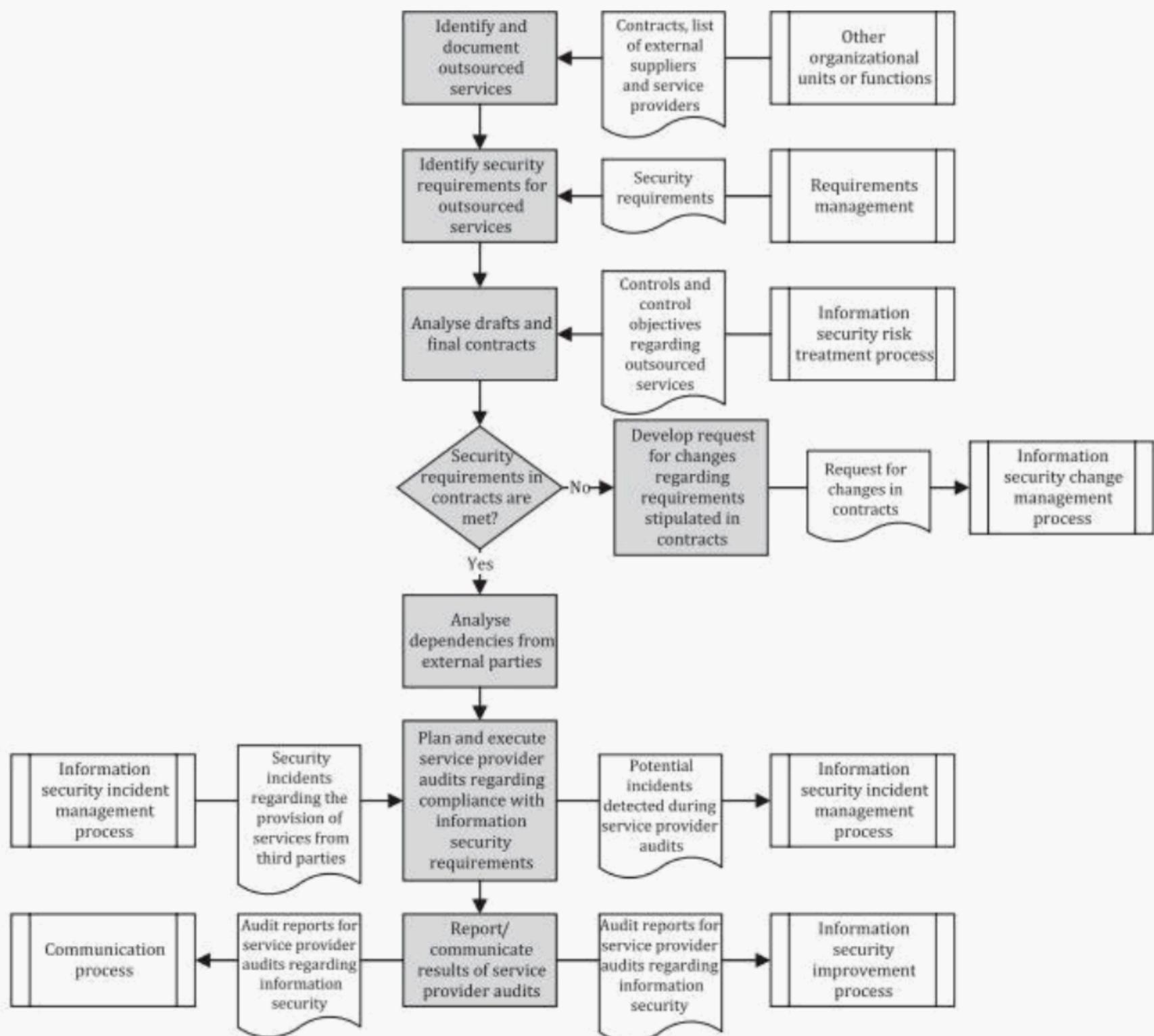


Figure 8 — Process flow chart — Process to control outsourced services

7.8 Process to assure necessary awareness and competence

Table 8 — Process profile — Process to assure necessary awareness and competence

Process name	Process to assure necessary awareness and competence
Process category	Core process
Brief description	The process to assure necessary awareness and competence should be the process to continuously develop and implement an information security awareness, training and education program.
Objective/purposes	The objective of this process is to ensure that all personnel receives the necessary security training and/or education. Employees should be aware of the information security policy, their contribution to the effectiveness of ISMS including the benefits of improved information security performance and implications of not conforming with ISMS requirements.
Input	<ul style="list-style-type: none"> — From the information security incident management process: Incidents. From information security risk treatment process: Risk treatment plan, controls, control objectives. — From the process to assure necessary awareness and competence itself: Information security awareness, education and training materials, plans, and records (also from preliminary results of the process to assure necessary awareness and competence).
Results	<ul style="list-style-type: none"> — For the process to assure necessary awareness and competence itself and records control process: <ul style="list-style-type: none"> — information security awareness education and training plans; — information security awareness education and training materials; — information security awareness education and training records.
Activities/functions	<ul style="list-style-type: none"> — Identify the level of information security awareness. — Derive training and education requirements for each unit/department. Develop training plans and materials – also integrate information security awareness in other training courses. — Execute training plans (training courses). — Document and analyse training records.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 7.3 — ISO/IEC 27003:2017, 7.3

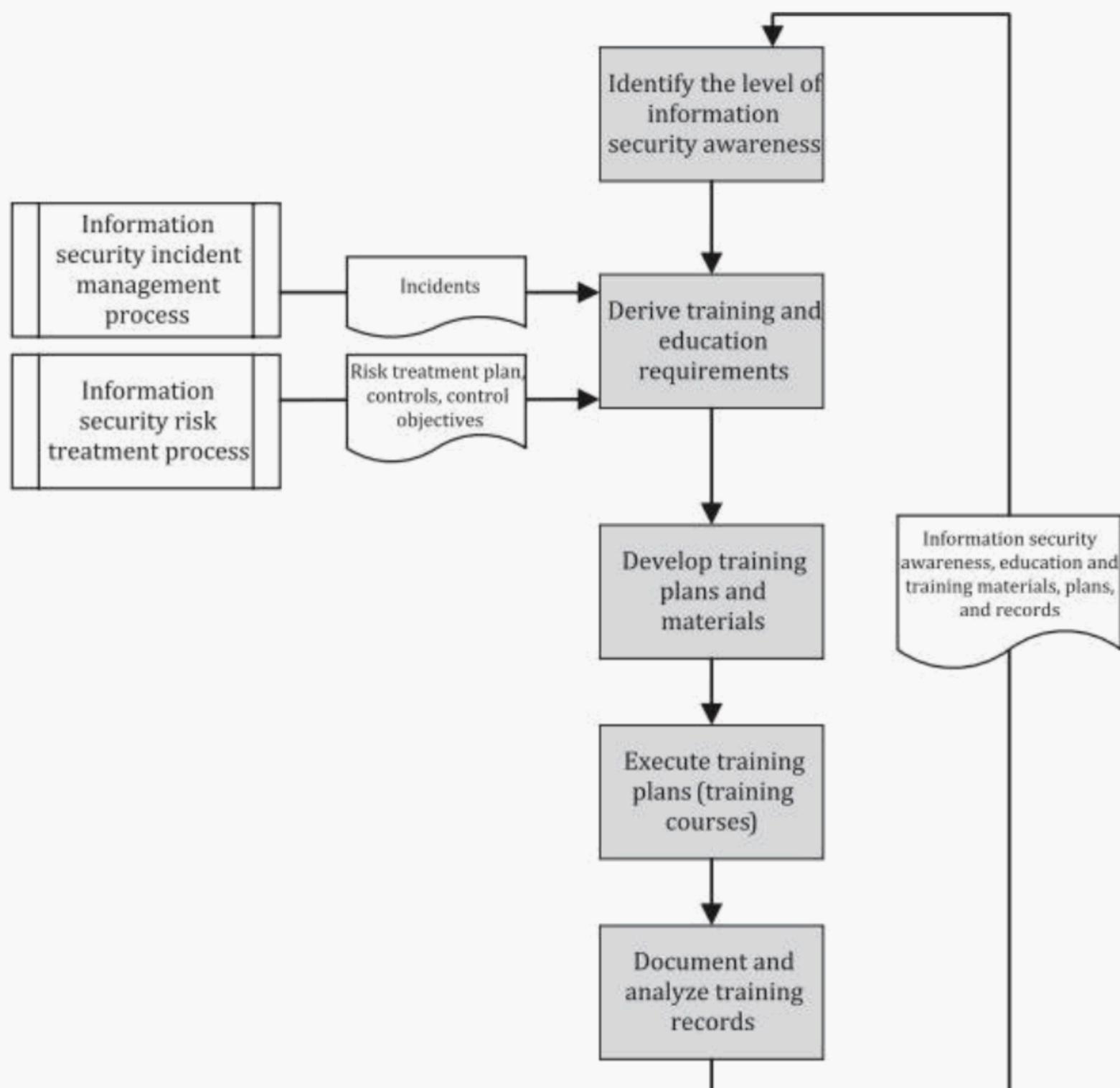


Figure 9 — Process flow chart — Process to assure necessary awareness and competence

7.9 Information security incident management process

Table 9 — Process profile — Information security incident management process

Process name	Information security incident management process
Process category	Core process
Brief description	An information security incident is a single or series of unwanted or unexpected information security events (possible breach of information security, policy or failure of controls) that have a significant probability of compromising business operations and threatening information security. The information security incident management process should be for detecting, reporting, assessing, responding to, dealing with and learning from information security incidents.
Objective/purposes	The objective of this process is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. Further objectives are to ensure a quick, effective and orderly response to information security incidents.

Table 9 (continued)

Process name	Information security incident management process
Input	<ul style="list-style-type: none"> — From help desk processes (employees), process to control outsourced services (contractors), internal audit and performance evaluation process: Potential incidents. — From records control process: Information needed to assess the incident (not displayed in the process chart). — From information security change management process: Status of requests for changes.
Results	<ul style="list-style-type: none"> — For communication process, internal audit process, performance evaluation process, information security customer relationship management process, requirements management process: Incidents. — For information security change management process: Request for changes to respond/ to deal with and to prevent further incidents. — For process to assure necessary awareness and competence: Information about incidents to learn from incidents. — For information security risk assessment process: Information about risks to be considered in the evaluation of risks. — For records control process: Information regarding the incident (evidence, results of incident assessment, etc. – not displayed in the process chart). Detect
Activities/functions	<ul style="list-style-type: none"> — and report potential information security incidents. — Recording, initial assessment and classification (classification as information security incident or not) of potential information security incidents. — Prioritize information security incidents. — Report information security incidents (as quickly as possible). — Respond to information security incidents: <ul style="list-style-type: none"> — collect evidence and conduct analysis of information security incidents; — escalate (if required) and communicate incident; — deal with information security incidents (resolution); — post incident analysis. — Closure and learn from information security incidents (reduce likelihood or impact of future incidents).
References	<ul style="list-style-type: none"> — ISO/IEC 27003:2017, 8.2 and 10.1 — ISO/IEC 27035-1:2016

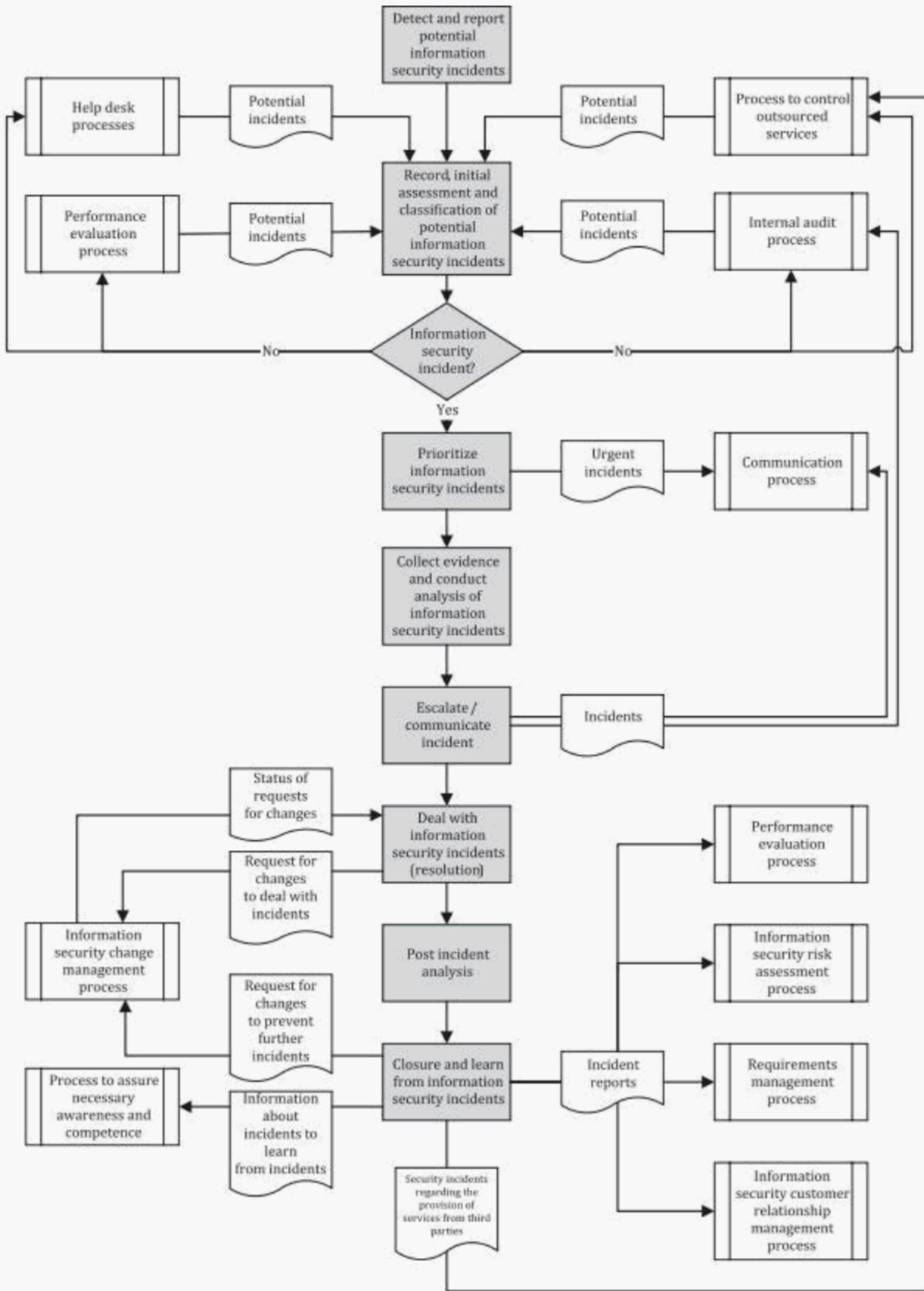


Figure 10 — Process flow chart — Information security incident management process

7.10 Information security change management process

Table 10 — Process profile — Information security change management process

Process name	Information security change management process
Process category	Core process
Brief description	Information security change management process should be the process to control changes of ISMS elements and review the consequences of unintended changes. This process only focusses on change management of the ISMS. This process should be linked with a general change management process of the organization, which provides input (proposed or realized changes) to this process.
Objective/purposes	Objective of this process should be to mitigate any adverse effects of changes as necessary. Relevant changes like changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled from the perspective of information security.
Input	<ul style="list-style-type: none"> — From information security risk assessment process: Evaluated risks of proposed changes. — From information security governance/management interface process (as part of the management reviews), information security customer relationship management process, information security risk treatment process, internal audit process (to correct nonconformities), process to control outsourced services (to correct nonconformities), information security improvement process (as results of the continual improvement), information security incident management process (to deal with incidents): Requests for changes. — From security implementation management process: Results of changes. — From change management process: Proposed or realized changes.
Results	<ul style="list-style-type: none"> — For information security incident management process: Status/results of changes. — For information security risk assessment process: Initiation of risk assessment when significant changes are proposed or occur; results of changes. — For security policy management process: Change requests for IS policies. — For records control process: Process results like control implementation plan. — For security implementation management process: Necessary changes (control implementation plan).
Activities/functions	<ul style="list-style-type: none"> — Identify and record necessary changes of controls, ISMS processes, ISMS documentation, ISMS scope, policy, standards procedures. — Plan changes including fall back procedures. — Obtain risk evaluation of proposed changes from risk assessment process (assessment of potential impacts). — Approve or decline changes. — Initiate changes via security implementation management process and security policy management process. — Obtain and record results of changes. — Communicate results of changes to risk assessment process as well as the information security incident management process.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 8.1 and 10.2 — ISO/IEC 27003:2017, 8.1 and 10.2

7.11 Internal audit process

Table 11 — Process profile — Internal audit process

Process name	Internal audit process
Process category	Core process
Brief description	Effectiveness and efficiency of the ISMS and implemented controls should be examined independently within the scope of internal audits to validate the ISMS against the needs of the business and to maintain the commitment of the business to the ISMS. The ISMS process of internal auditing contains only the part of auditing information security controls. The audit of the ISMS processes should be performed independent from the ISMS operation.
Objective/purposes	The internal audit process should determine effectiveness and performance of control objectives, controls as well as to identify nonconformities to the requirements – especially standards, legislation or regulations and identified security requirements.
Input	<ul style="list-style-type: none"> — From records control process: Results of former audits (not displayed in the process chart). — From security policy management process: IS policies. — From requirements management process: Information security requirements. — From information security risk treatment process: Risk treatment plan including list of controls, control objectives and control implementation plan. — From information security incident management process: Incident reports are used to verify/evaluate control functionality. — From performance evaluation process: Not continuously measured metrics.
Results	<ul style="list-style-type: none"> — For communication process: Reporting internal audit results. — For information security improvement process: Results of audits and suggestions for improvement. — For information security change management process: Request for changes regarding nonconformities of information security controls. — For records control process: Internal audit results (not displayed in the process chart). — For information security incident management process: Potential incidents.
Activities/functions	<ul style="list-style-type: none"> — Plan internal audits as part of an audit program. — Define audit criteria and scope of each audit. — Select auditors. — Perform internal audits. — Reporting internal audit results to communication process and information security improvement process, to information security incident management process (as results are possibly potential incidents) and to information security change management process (changes to correct nonconformities). — Optional: develop suggestions for improvement.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 9.2 — ISO/IEC 27003:2017, 9.2

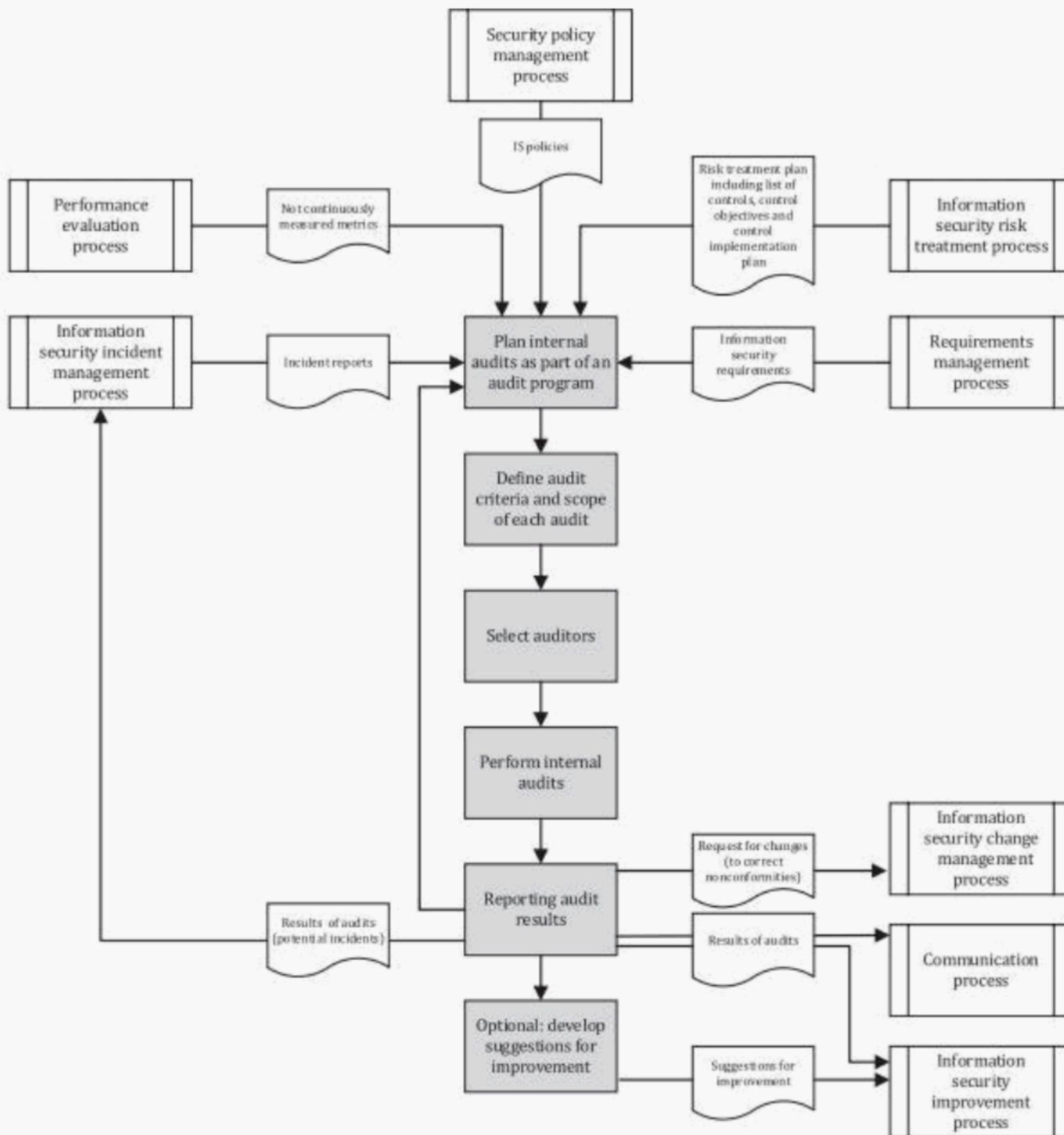


Figure 12 — Process flow chart — Internal audit process

7.12 Performance evaluation process

Table 12 — Process profile — Performance evaluation process

Process name	Performance evaluation process
Process category	Core process
Brief description	The performance evaluation process should contain monitoring, measurement, analysis and evaluation of two main criteria. First, the performance of the security controls and second the performance of the ISMS processes. Performance measurement differs from performance audit (internal audit) which should be performed independently. Performance measurement should be done by using key performance indicators (KPI) as well as key goal indicators (KGI) for every process of the ISMS.
Objective/purposes	The performance of ISMS needs to be monitored in terms of verification and reporting of security control implementation as well as the information security management processes. Objective of this process is to assess the performance against the policy and objectives of the organization to support management review.
Input	<ul style="list-style-type: none"> — From security policy management process: IS policies. — From information security risk treatment process: Risk treatment plan including list of controls, control objectives and control implementation plan. This process should especially integrated/linked with the information security risk treatment process because metrics for controls should be defined as soon as possible within the planning of controls to avoid unnecessary costs afterwards. — From information security incident management process: Incident reports are used to verify/evaluate control functionality.
Results	<ul style="list-style-type: none"> — For communication process and information security customer relationship management process: Reporting performance evaluation results. — For information security incident management process: Potential incidents. For information security improvement process: Suggestions for improvement. For records control process: Measurement results (not displayed in process chart). For the internal audit process: Where metrics are not continuously measured this process can also be linked with the internal audit process as it provides requirements to measure metrics within internal audits.
Activities/functions	<ul style="list-style-type: none"> — Determine and regularly review what needs to be measured as well as methods for analysis and evaluation of the measurement results. — Develop measurement system/program (what needs to be measured, using which methods, when should the measurement be done, who should do it). — Analyse and evaluate results of measurement. — Develop suggestions for improvement. — Reporting performance evaluation results and suggestions for improvement.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 9.1 — ISO/IEC 27003:2017, 9.1

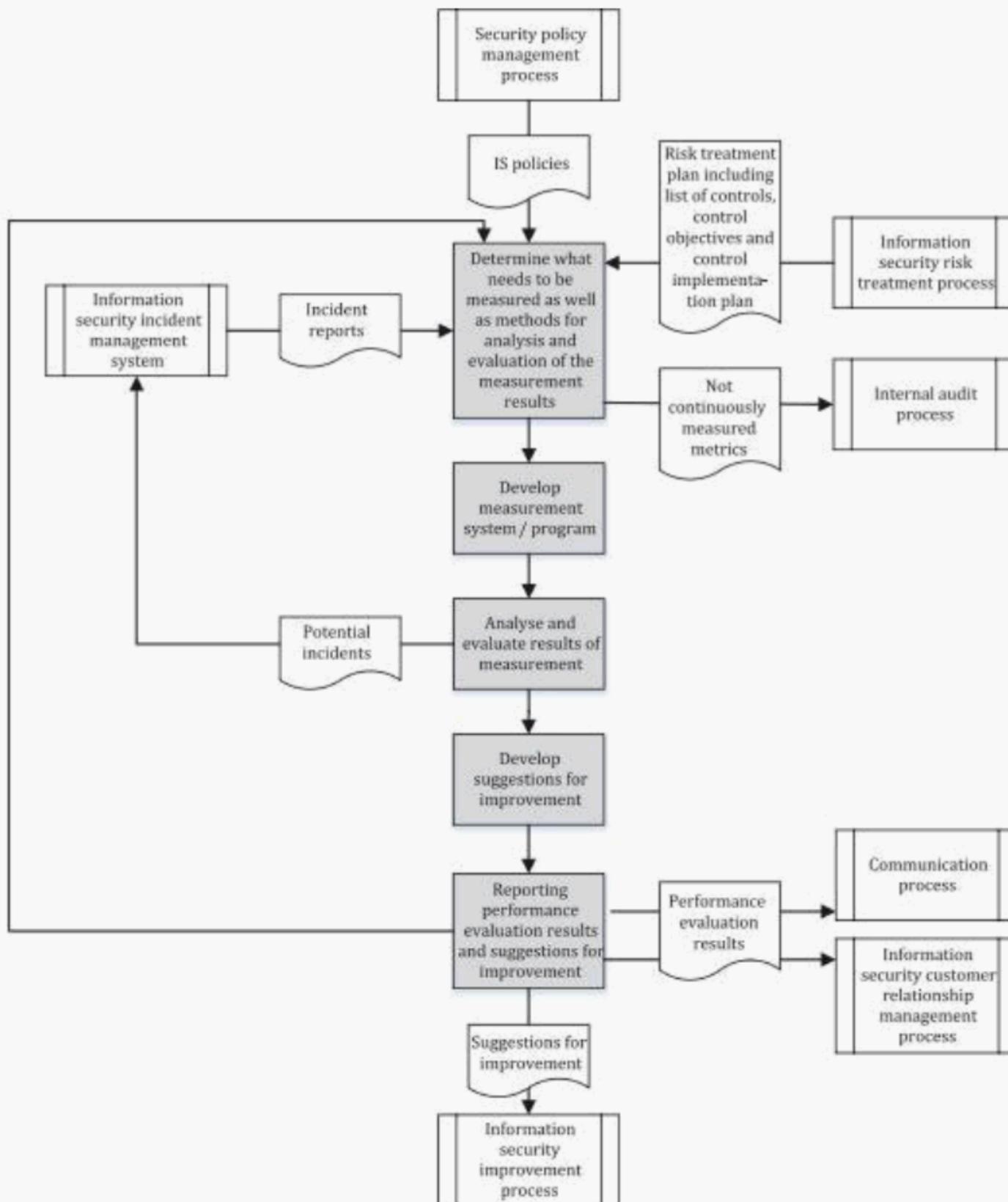


Figure 13 — Process flow chart — Performance evaluation process

7.13 Information security improvement process

Table 13 — Process profile — Information security improvement process

Process name	Information security improvement process
Process category	Core process
Brief description	The effectiveness, efficiency, suitability and adequacy of the ISMS need to be continually improved. A culture of continual improvement should be established. Emerging technologies and innovations also should be identified and assessed regarding potential ISMS-improvement possibilities.
Objective/purposes	The objective of this process should be to ensure and improve a continuing suitability, adequacy and effectiveness of the ISMS.
Input	<ul style="list-style-type: none"> — From internal audit process: Suggestions for improvement and audit results. — From process to control outsourced services: Audit reports for service provider audits regarding information security. — From performance evaluation process: Suggestions for improvement.
Results	<ul style="list-style-type: none"> — For records control process: Decisions related to continual improvement opportunities (not displayed in the process chart). — For information security change management: Change requests.
Activities/functions	<ul style="list-style-type: none"> — Continually identify trends, changes in the environment, emerging technologies and innovations. — Determine the effects and impact of trends, changes in the environment, emerging technologies and innovations for the ISMS. — Identify root causes of nonconformities. — Generate improvement opportunities as well as controls to eliminate root causes of nonconformities and evaluate them against the ISMS objectives. — Initiate changes to improve the ISMS.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 10.1 and 10.2 — ISO/IEC 27003:2017, 10.1 and 10.2

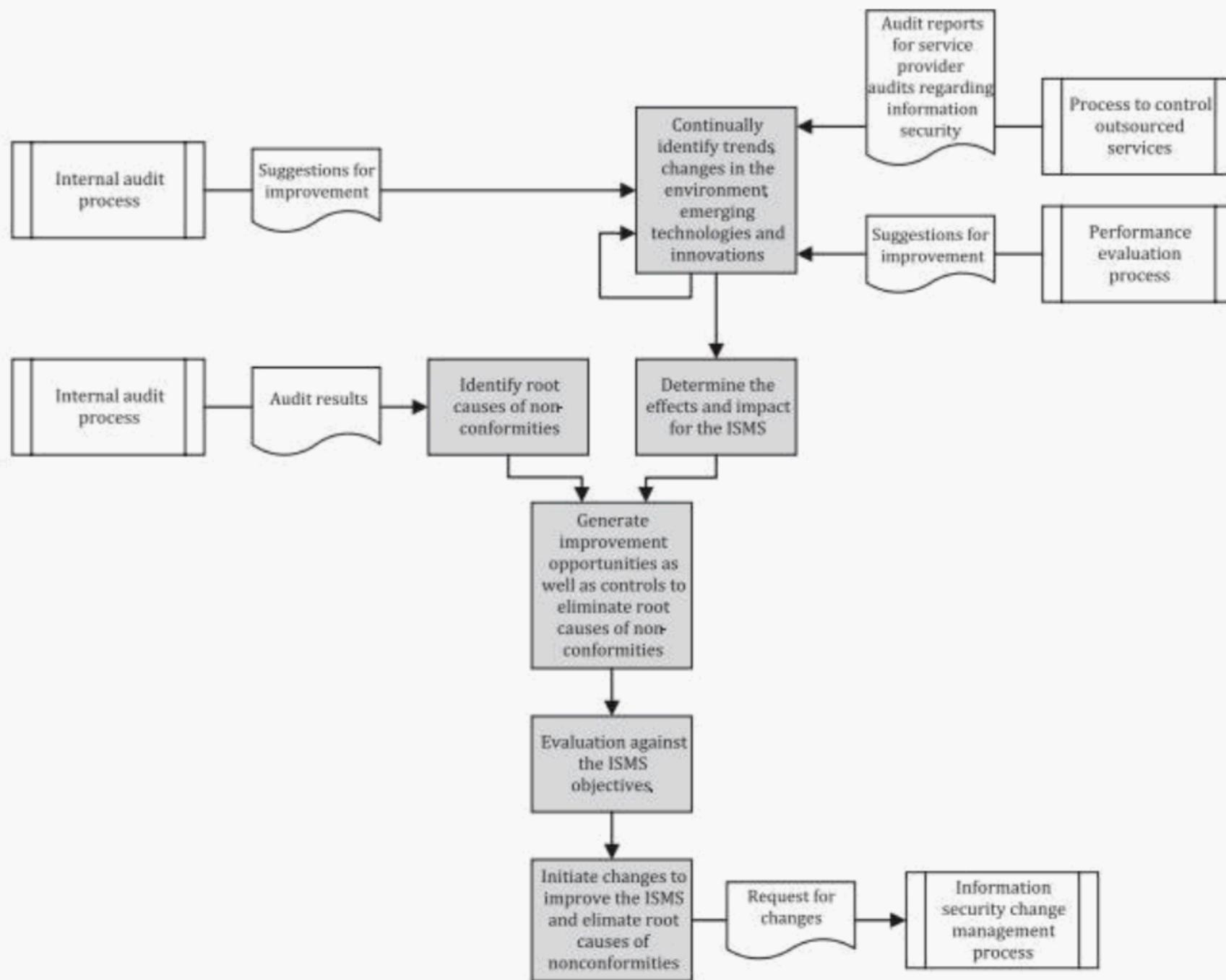


Figure 14 — Process flow chart — Information security improvement process

8 Support processes

8.1 General

This clause describes example support processes that can be found in an ISMS. The concepts and purposes embodied in these example processes should be considered during the process planning phase of an ISMS implementation project.

8.2 Records control process

Table 14 — Process profile — Records control process

Process name	Records control process
Process category	Support process
Brief description	Records control process should be the process to identify, create, update and control information determined to be necessary for the effectiveness of the ISMS.
Objective/purposes	<ul style="list-style-type: none"> — Ensure that all information determined to be necessary for the effectiveness of the ISMS are documented and recorded. — Ensure appropriate identification, description, format, review and approval for suitability and adequacy of records. — Ensure that the relevant recorded information is available for use, where and when it is needed, and it is adequately protected from loss, destruction, falsification, unauthorized access and unauthorized release.
Input	<ul style="list-style-type: none"> — From all other ISMS processes: Process results. — From requirements management process: Retention requirements.
Results	For all ISMS processes: Necessary records.
Activities/functions	<ul style="list-style-type: none"> — Obtain input from ISMS processes. — Define what should be recorded, to what extent. — Create/file records. — Access and protect records. — Identify period of retention (partially available as input from the requirements process). — Delete records after retention period.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 7.5 — ISO/IEC 27003:2017, 7.5

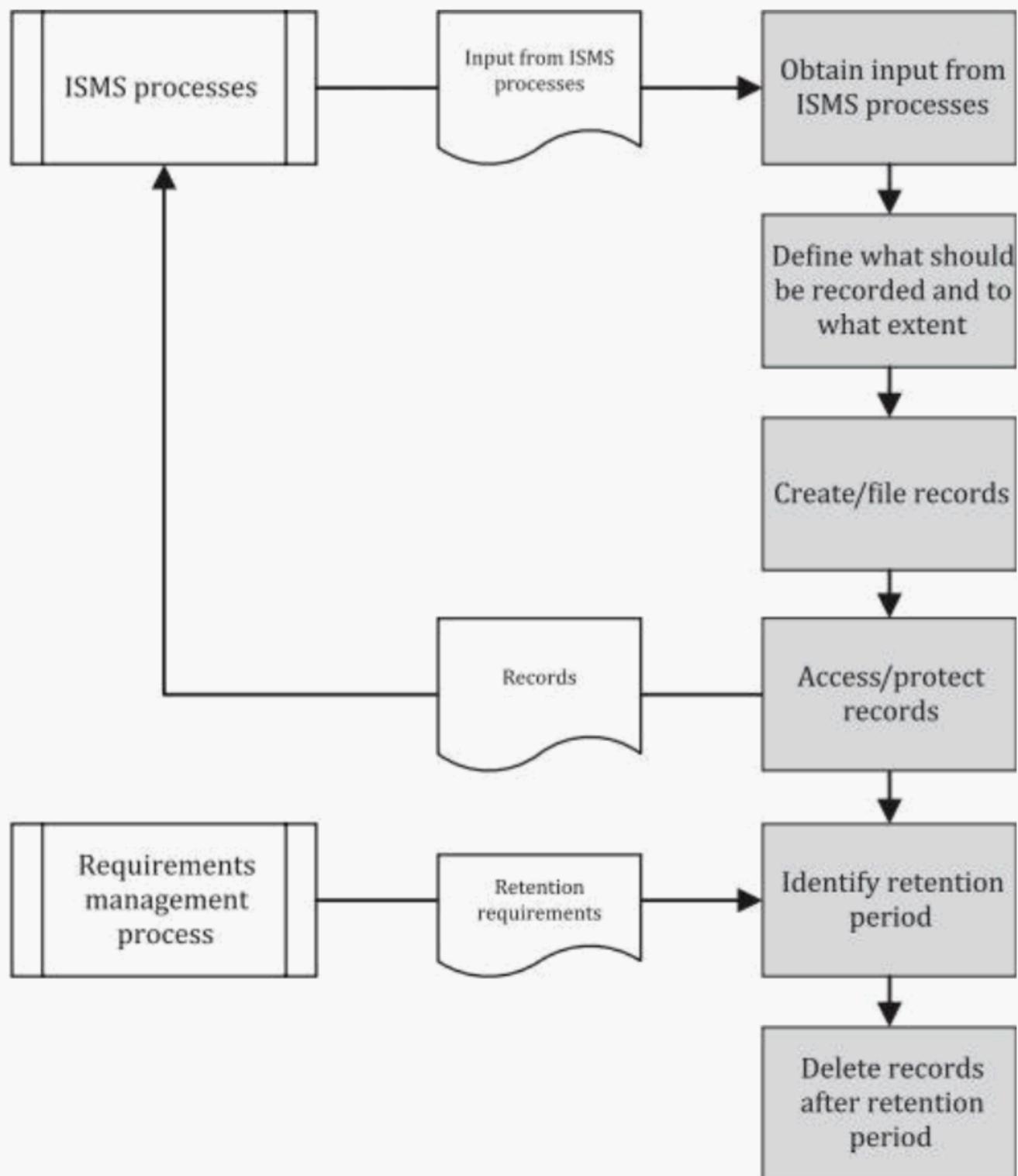


Figure 15 — Process flow chart — Records control process

8.3 Resource management process

Table 15 — Process profile — Resource management process

Process name	Resource management process
Process category	Support process
Brief description	The resource management process should be the process to identify, allocate and monitor required resources to run the ISMS processes as well as to implement and run the determined controls.
Objective/purposes	<ul style="list-style-type: none"> — Ensuring that the resources for the ISMS and the controls are available. — Appropriate management of ISMS resources and efficiency of resource usage.
Input	<ul style="list-style-type: none"> — From information security risk treatment process: Lists of determined and approved controls/control objectives. — From other organizational units or functions: List of suppliers, framework contracts, terms and conditions of purchasing, etc.
Results	<ul style="list-style-type: none"> — For information security risk treatment process: Estimation of necessary resources to implement controls. — For communication process: Estimation of necessary resources to operate the ISMS core processes and reports regarding resource usage of ISMS core processes. — For information security customer relationship management process: Reports on resource usage. — For records control process: Results of the process.
Activities/functions	<ul style="list-style-type: none"> — (Initially) plan necessary resources to implement and run the controls. — Categorize controls – a differentiation is made between controls funded by the ISMS budget and controls funded by other departments. — Communicate necessary resources to: <ul style="list-style-type: none"> — the information security risk treatment process to implement and run the controls – if necessary, repeat this step and the planning of necessary resources; — the communication process – regarding the ISMS controls. — Allocate necessary resources for approved controls funded by the ISMS. — Permanently monitor ISMS resource usage and update resource allocation. — Develop and communicate reports regarding resource usage of ISMS core processes to the responsible person for ensuring that the ISMS conforms to the relevant requirements.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 6.2 and 7.1 — ISO/IEC 27003:2017, 6.2 and 7.1

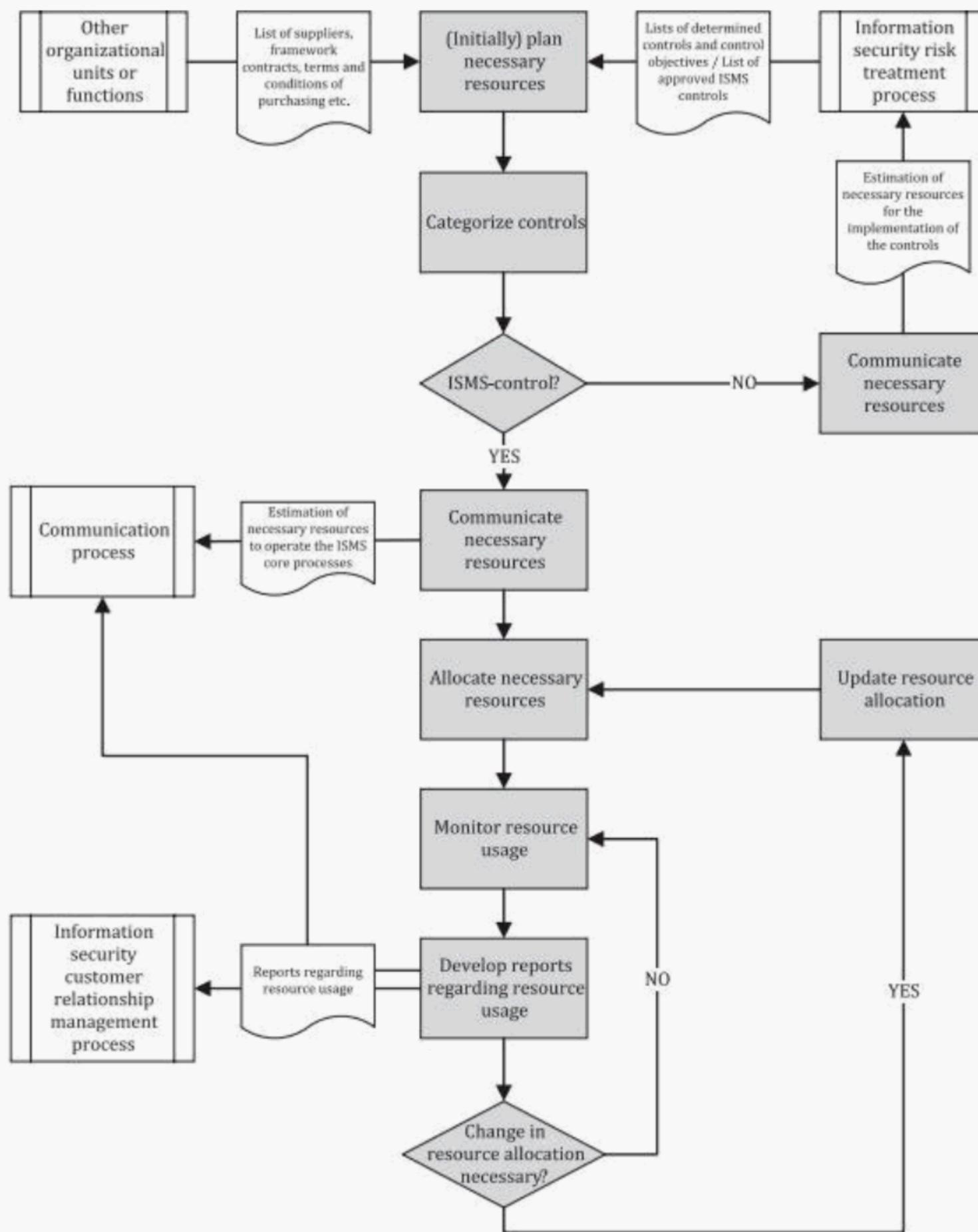


Figure 16 — Process flow chart — Resource management process

8.4 Communication process

Table 16 — Process profile — Communication process

Process name	Communication process
Process category	Support process
Brief description	Risk communication (communication process) should be the process to achieve agreement on how to manage risks by exchanging and/or sharing all information about risks between the decision-maker and other interested parties. This process is the interface/intermediary for all information leaving the ISMS.
Objective/purposes	Decision makers and other interested parties are adequately informed about information security risks and have a mutual understanding of these risks.
Input	<ul style="list-style-type: none"> — From information security risk assessment process: Documented risks and evaluation of risks in a list of prioritized risks. — From information security risk treatment process: Risk treatment and control implementation plan, list with determined controls and control objectives, acceptance of residual risks. — From security policy management process: IS policies. — From records control process: Appropriate documents and necessary records. — From resource management process: <ul style="list-style-type: none"> — reports regarding resource usage for ISMS controls; — estimation of necessary resources to operate the ISMS core processes. — From requirements management process: Assigned requirements regarding information security. — From internal audits and performance evaluation process: Audit and performance reports. — From process to control outsourced services: Audit reports. — From information security incident management process: Incident reports. — From information security customer relationship management process: Communication plan with customers and reports on information security performance and added value to the customers.
Results	<ul style="list-style-type: none"> — For information security governance/management interface process and records control process: information security management reports. — For records control process: <ul style="list-style-type: none"> — communication plan for normal operations and emergency situations; — information security management reports.
Activities/functions	<ul style="list-style-type: none"> — Develop/update risk communication plans for normal operations. — Develop/update risk communication plans for emergency situations. — Execute communication plans. — Learn from previous communication. — Regularly generate information security management reports.
References	<ul style="list-style-type: none"> — ISO/IEC 27001:2013, 7.4 — ISO/IEC 27003:2017, 9.4.1

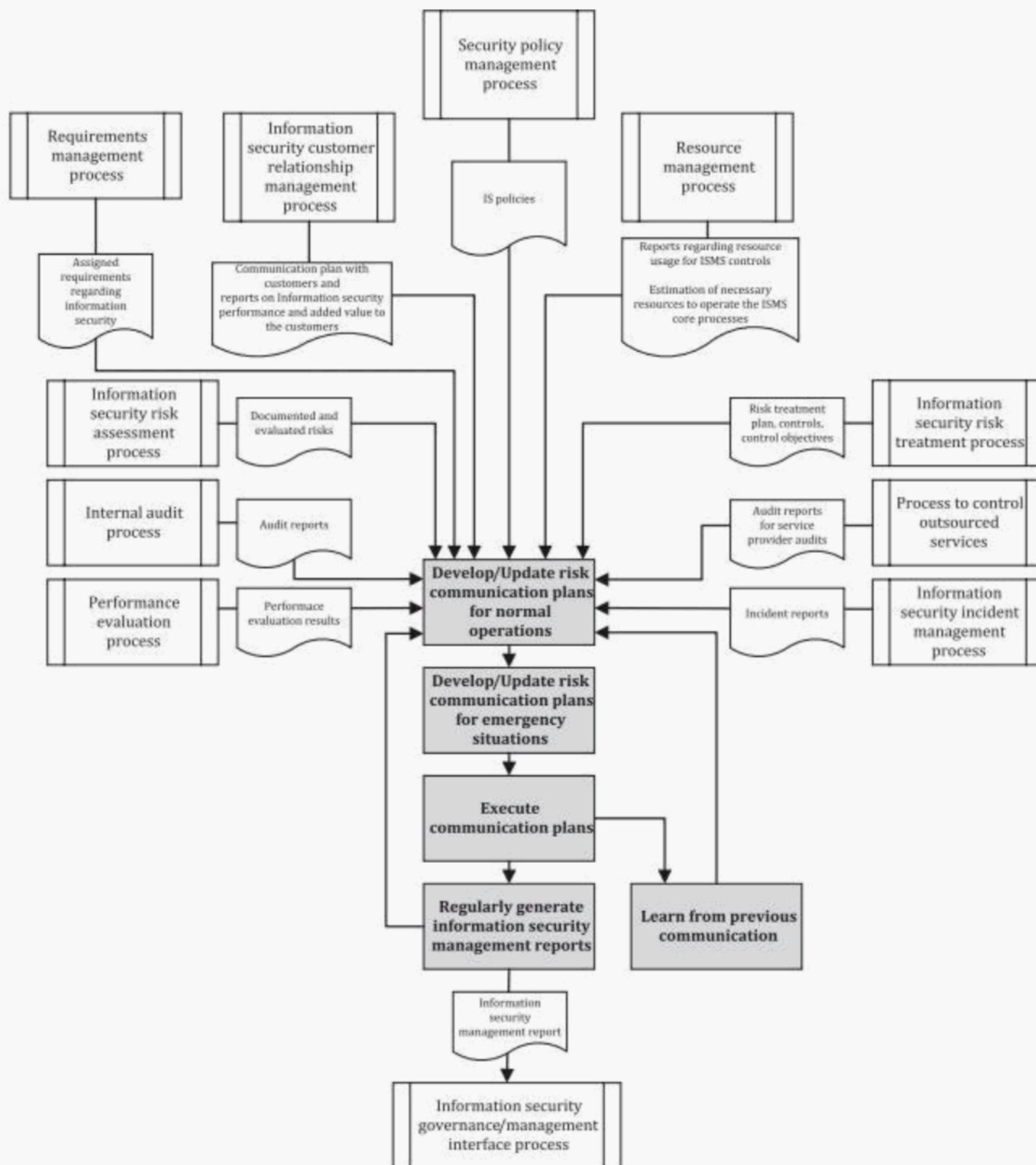


Figure 17 — Process flow chart — Communication process

8.5 Information security customer relationship management process

Table 17 — Process profile — Information security customer relationship management process

Process name	Information security customer relationship management process
Process category	Support process
Brief description	This process should enable the management of the customer satisfaction level and the continuous demonstration of the added value of investments in information security.
Objective/purposes	<ul style="list-style-type: none"> — Ensure an appropriate customer satisfaction. — Ensure an appropriate balance between benefits, and costs of information security investments as well as risks. — Continuously demonstrate the added value of the ISMS or information security controls.
Input	<ul style="list-style-type: none"> — From performance evaluation process: Performance evaluation reports. From — resource management process: Reports regarding the usage of resources. From — information security incident management process: Incident reports. For
Results	<ul style="list-style-type: none"> — records control process: <ul style="list-style-type: none"> — identified customers, users and interested parties including communication mechanisms with customers; — documented customer satisfaction levels, complaints and added value of information security investments. — For information security change management process: Change requests. — For communication process: Information security performance and added value to the customers and communication mechanism/plan with the customer. — For requirements management process: Requirements of customers.
Activities/functions	<ul style="list-style-type: none"> — Identification and documentation of customers, users and interested parties. — Establishment of a communication mechanism with the customer. Establish a method for measuring and demonstrating the value of information security and the efficient resource usage: <ul style="list-style-type: none"> — track results of information security initiatives and compare to expectations to ensure value delivery against business goals; — measurement of the customer satisfaction at planned intervals; — establish a documented procedure to manage information security complaints from the customer. — Initiation of changes to improve the customer satisfaction. — Communicate information security performance/added value to customers.
References	<ul style="list-style-type: none"> — ISO/IEC 27003:2017; 4.2, 7.4 and 10.1

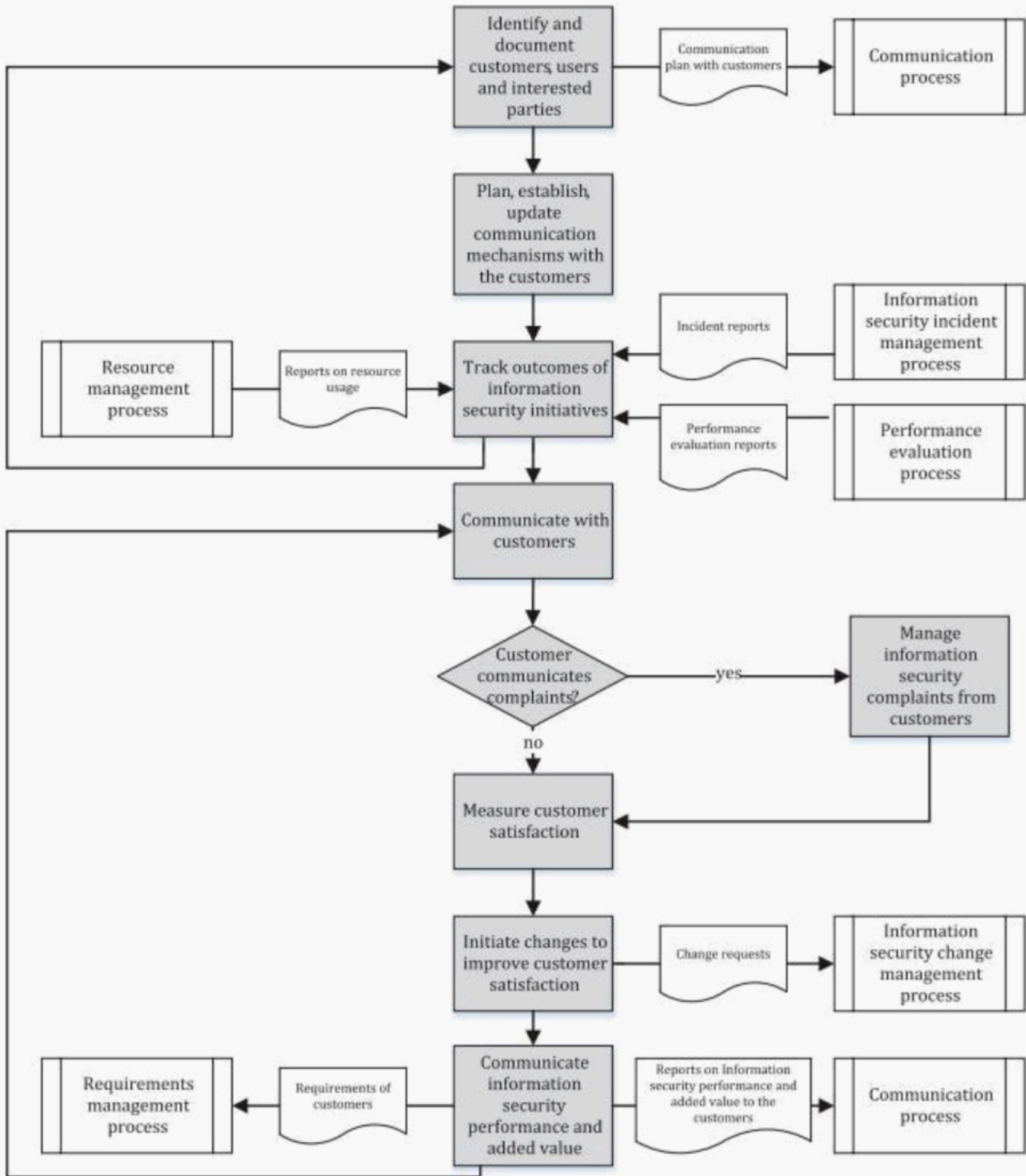


Figure 18 — Process flow chart — Information security customer relationship management process

Annex A (informative)

Statement of conformity to ISO/IEC 33004

This annex discusses whether the process model is a process reference model meeting the criteria defined in ISO/IEC 33004 for process reference models. According to ISO/IEC 33004: “The purpose of a process reference model is to define a set of processes that collectively can support the primary aims of a community of interest. A process reference model provides the basis for one or more process assessment models.” Criteria for process reference models defined in ISO/IEC 33004 are the following:

- 1) *A process reference model shall contain a declaration of the domain of the process reference model.*

The ISMS process reference model is clearly dedicated to the use within information security risk management, which is a domain.

- 2) *A process reference model shall contain a description of the relationship between the process reference model and its intended context of use.*

The processes of the ISMS process reference model are formulated in a general manner to fit for all organizations independent of their size, objectives, business model, location etc. The ISMS process reference model should be used in the context of a method to determine the necessary maturity level for each process contained in the framework. ISMS processes of the reference model should be tailored to the specific needs of the applying organization and must be used only as a starting point. A general focus on a process perspective rather than a measure perspective is intended. A measurement driven approach, like the understanding of information security as a one-time project, should be avoided and replaced by a process-oriented approach.

- 3) *A process reference model shall contain process descriptions, meeting the following requirements within the scope of the process reference model:*

- a) *A process shall be described in terms of its purpose and process outcomes.*

Process purpose and outcomes (results) are described within the process profiles.

- b) *The described set of process outcomes shall be necessary and sufficient to achieve the purpose of the process.*

The sets of process outcomes (results) were defined with the intention to be necessary and sufficient for the purpose of the process. Every process purpose and the process outcome set were validated to be necessary and sufficient.

- c) *Process descriptions shall not contain or imply aspects of the process quality characteristic beyond the basic level of any relevant process measurement framework conformant with ISO/IEC 33003.*

Every process description meets this requirement.

- d) *A process outcome describes one of the following: production of an artifact; a significant change of state; meeting of specified constraints, e.g. requirements, goals, etc.*

Every process outcome defined within the ISMS process reference model meets this requirement. In general, the guidelines of ISO/IEC TR 24774 were considered while defining and describing the ISMS processes.

- 4) *A process reference model shall contain a description of the relationship between the processes defined within the process reference model.*

A description of the relationships between the processes is described within the process profiles. For every process, input/results are defined. Those interfaces are also visualized within the process flow charts and [Figure 1](#).

- 5) *The process reference model shall document the community of interest of the model and the actions taken to achieve consensus within that community of interest:*
- a) *The relevant community of interest shall be characterized or specified.*

The community of interest is every person accountable or responsible (partially or overall) for the management of information security risks. Also, experts assessing an ISMS against ISO/IEC 27001 are included in the relevant community.

- b) *The extent of achievement of consensus shall be documented. If no actions are taken to achieve consensus, a statement to this effect shall be documented.*

The PRM is based on extensive scientific research documented in Reference [\[10\]](#).

Consensus was reached within extensive expert consultations with experts of the community of interest within the development of this document following the ISO standardization process. Also, consensus can be assumed taking into account that all processes were derived from internationally accepted standards.

- 6) *The processes defined within a process reference model shall have unique process descriptions and identification.*

Every process has unique process descriptions and identification.

As a result of the discussion above, the framework is meeting the requirements for process reference models defined in ISO/IEC 33004.

Bibliography

- [1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*
- [2] ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*
- [3] ISO/IEC TR 24774:2010, *Systems and software engineering — Life cycle management — Guidelines for process description*
- [4] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*
- [5] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*
- [6] ISO/IEC 27003:2017, *Information technology — Security techniques — Information security management systems — Guidance*
- [7] ISO/IEC 27035-1:2016, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*
- [8] ISO/IEC 33003:2015, *Information technology — Process assessment — Requirements for process measurement frameworks*
- [9] ISO/IEC 33004:2015, *Information technology — Process assessment — Requirements for process reference, process assessment and maturity models*
- [10] Haufe K., 2017). Maturity based approach for ISMS Governance. Available from https://e-archivo.uc3m.es/bitstream/handle/10016/25128/tesis_knut_haufe_2017.pdf?sequence=3

ICS 03.100.70; 35.030

Price based on 43 pages