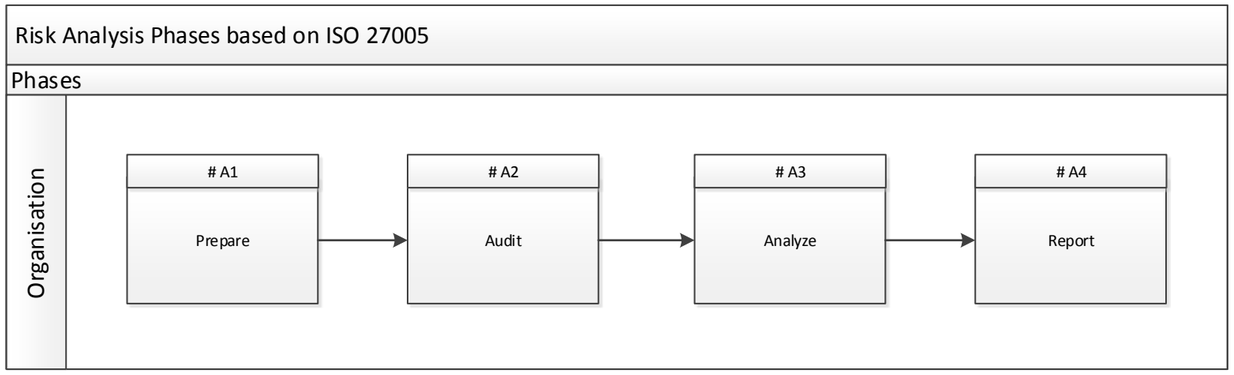
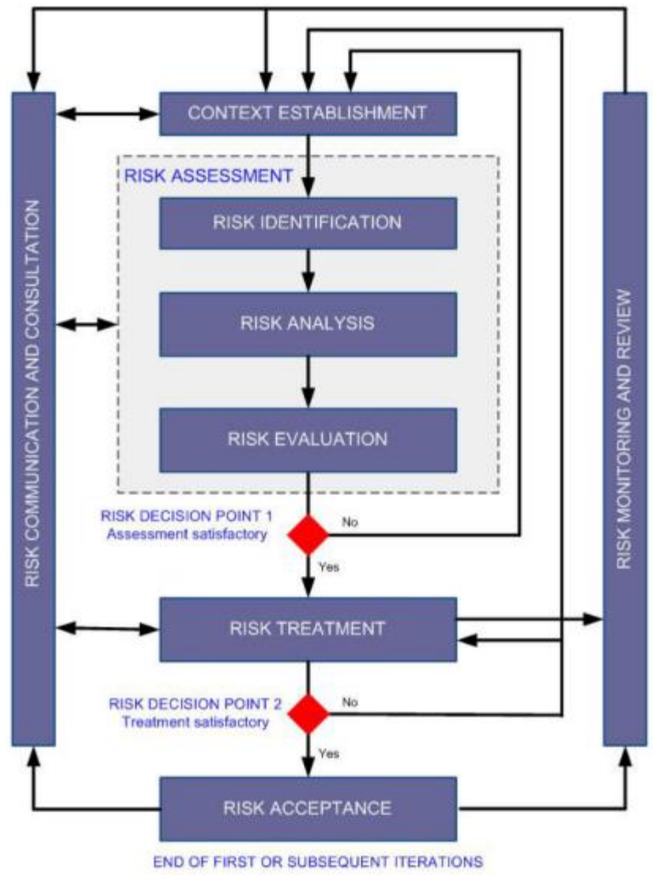


Version mai 2017, Author: Christophe Jolivet – PR4GM4 inc. 418-261-6320

(ISO 27005 measures in red)

PARTICIPANTS:
Shareholders
CTO: chief technology officer and other officer
CIO: Chief information officer
CISO: Chief information security officer and ***Analyst/auditor***
Respondents/Experts

ISO 27005



Risk Analysis Phases based on ISO 27005

A1 - Prepare

Shareholders

CEO/CIO/CTO/CFO

CIO

CISO

Analyst/Auditor

A1.2
Provide approval

A1.8
Help identify and classify assets

A1.3
Send a memorandum to the entire organization to formalize the project

A1.7
Designate/ identify respondents and experts

debut

A1.1
Get approval from upper level management

A1.4
Decide on the method and tool to be used

A1.10
Decide on the precision of the analysis

A2

A1.5
Participate in the decision-making process

A4

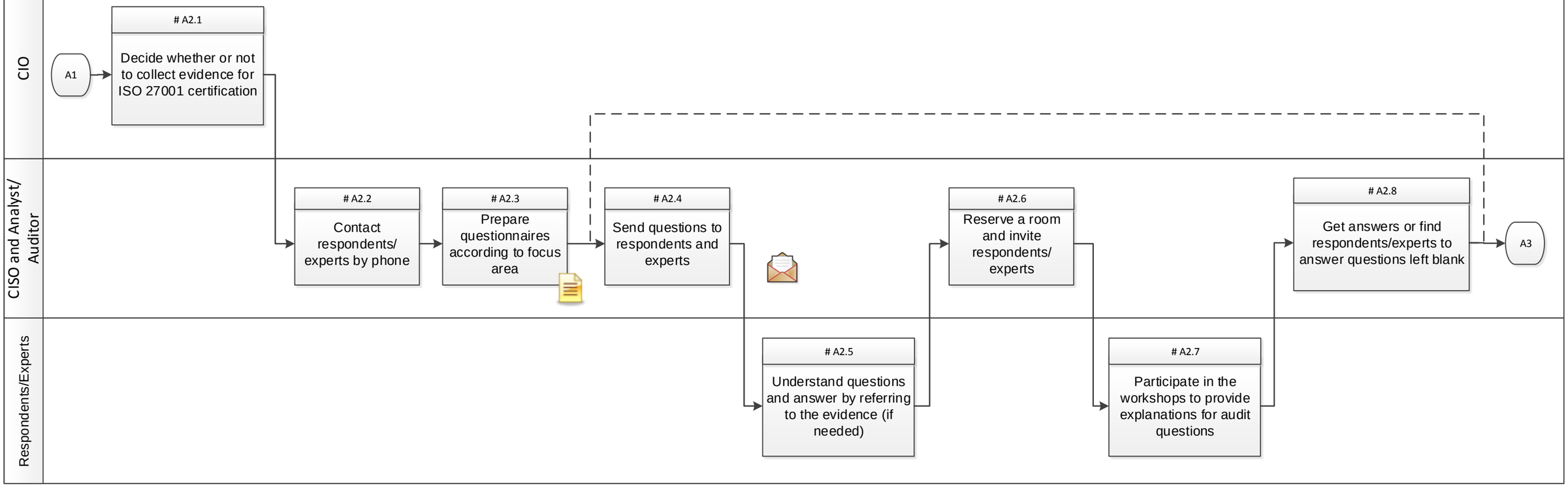
A1.6
Define the scope and range of the analysis (establish context)

A1.9
Obtain inventory and classification of primary and secondary assets

No.	Tasks	Description	Deliverable
Phase: Prepare			
A1.1	Get approval from upper level management	To facilitate collaboration between parties, it is preferable to get authorization from management	
A1.2	Provide approval	Provide approval	
A1.3	Send a memorandum to the entire organization to formalize the project	Approval from management must be validated using a memorandum sent to all those concerned and solicited	Official memorandum
A1.4	Decide on the method and tool to be used	Decide on the method and tool that will be used. There are in fact, several tools and methods available	
A1.5	Participate in the decision-making process	Help make decisions through a preliminary analysis, get demonstrations and make lasting choices	
A1.6	Define the scope and range of the analysis (establish context)	Define the scope and range of the analysis (establish context). Is the analysis being completed as part of a project? For a service, management or any other type of organization?	
1.7	Designate/ identify respondents and experts	Designate/ identify respondents and experts according to sector, industry, management and area of expertise	
A1.8	Help identify and classify assets	Help identify and classify assets (starting with businesses processes)	
A1.9	Obtain inventory and classification of primary and secondary assets	Help identify and classify assets from owners/holders (if not already done) who are often the CEO/CIO/CTO/CFO, etc.	Classification of assets
A1.10	Decide on the precision of the analysis	Decide on the precision of the analysis. Do you prefer yes/no answers or do you want to assess the security measures based on a maturity scale such as ISO 15504	

Risk Analysis Phases based on ISO 27005

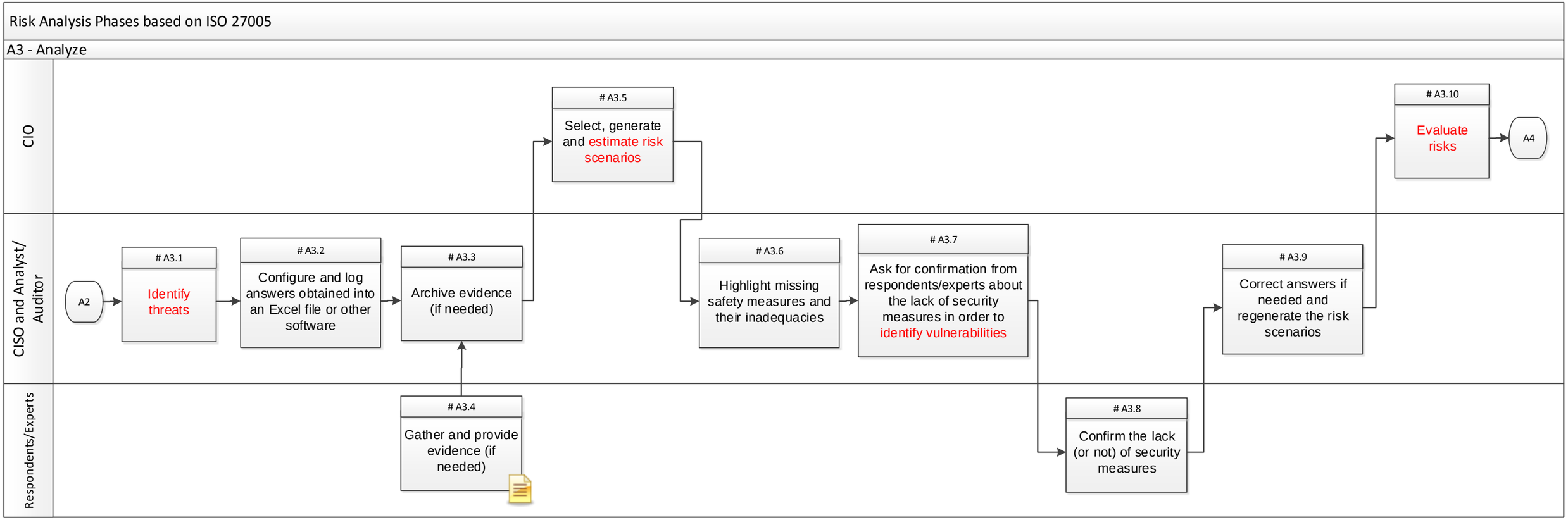
A2 - Audit



Phase: Audit			
A2.1	Decide whether or not to collect evidence for ISO 27001 certification	Decide whether or not to collect evidence for ISO 27001 certification. The external auditor will ask to see this proof in the form of procedures, processes, guidelines, screenshots, etc.	
A2.2	Contact respondents/experts by phone	Contacting respondents/experts by phone will make it easier to conduct follow-ups and ensure that the designated respondents/expert can answer the questions	
A2.3	Prepare questionnaires according to focus area	Prepare questionnaires according to focus area and the respondents/experts identified based on the organization's organizational chart	
A2.4	Send questions to respondents and experts	Send questions to the respondents/experts before the workshop so that they can read them in advance.	
A2.5	Understand questions and answer by referring to the evidence (if needed)	Understand questions and ideally, answer by referring to the evidence (if needed)	
A2.6	Reserve a room and invite respondents/experts	Reserve a room and invite respondents and/or experts to workshops lasting maximum one to two hours. Schedule many workshops if necessary.	
A2.7	Participate in the workshops to provide explanations for audit questions	Participate in the workshops to provide explanations for audit questions	
A2.8	Get answers or find respondents/experts to answer questions left blank	Get answers to questions asked, if some are left blank, get answers from other respondents/experts. There is a chance that some questions will have to be answered by other people.	

Risk Analysis Phases based on ISO 27005

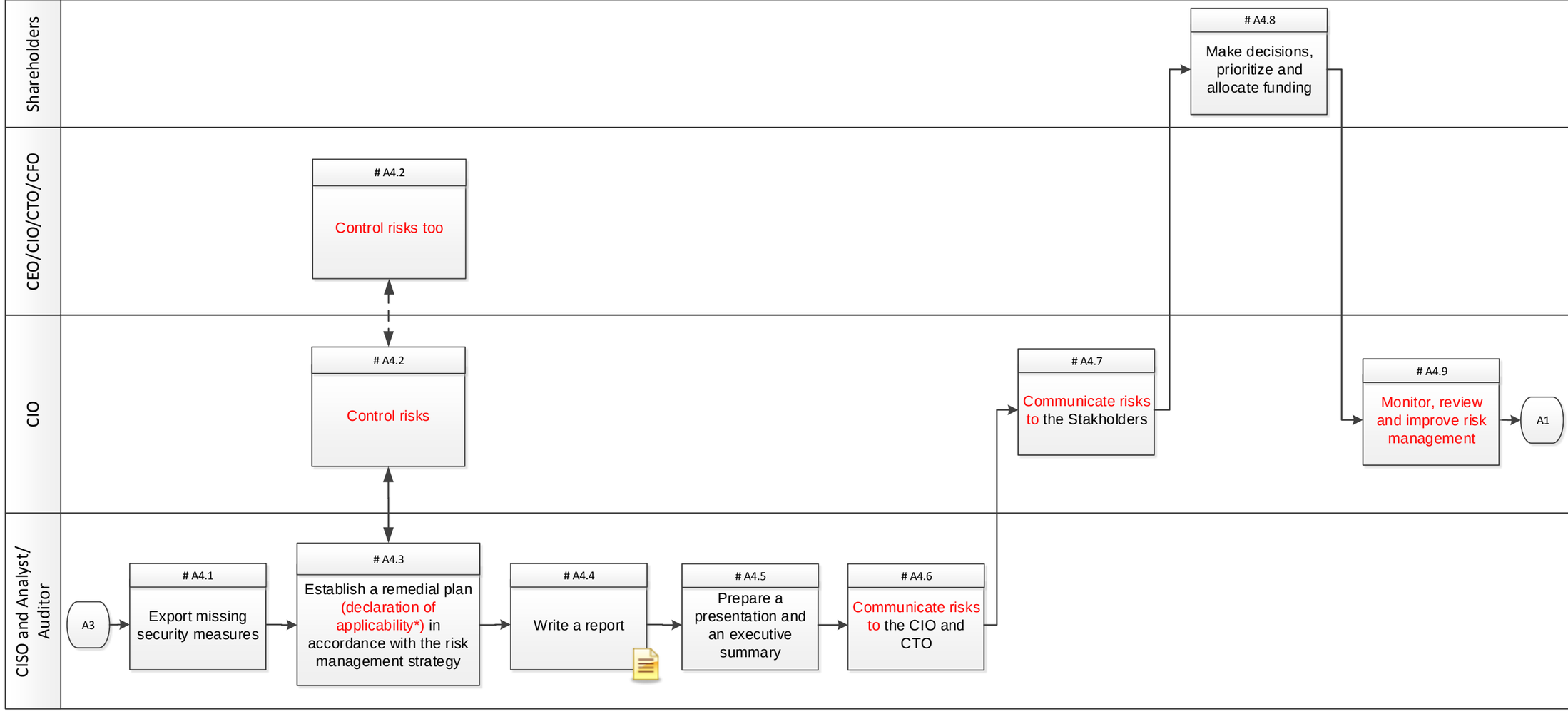
A3 - Analyze



Phase: Analyze			
A3.1	Identify threats	With ISO27005, you are required to identify threats	
A3.2	Configure and log answers obtained into an Excel file or other software	Configure and log answers obtained into an Excel file or other software	
A3.3	Archive evidence (if needed)	Archive evidence (if needed)	Evidence 
A3.4	Gather and provide evidence (if needed)	Gather and provide evidence (if needed)	
A3.5	Select, generate and estimate risk scenarios	Select, generate and estimate risk scenarios according to the scope of the project, starting with business lines	
A3.6	Highlight missing safety measures and their inadequacies	Highlight missing safety measures and their inadequacies	
A3.7	Ask for confirmation from respondents/experts about the lack of security measures in order to identify vulnerabilities	Ask for confirmation from respondents/experts about the lack of security measures in order to identify vulnerabilities. In fact, it's not uncommon that by demonstrating the missing measures, respondents/experts will reconsider their answers so they can contextualize the deficiencies. This avoids presenting risks that could be deemed "alarming"	
A3.8	Confirm the lack (or not) of security measures	Confirm the lack (or not) of security measures	
A3.9	Correct answers if needed and regenerate the risk scenarios	Correct answers if needed and regenerate the risk scenarios	
A3.10	Evaluate risks	Evaluate risks. This can be done automatically using an Excel spreadsheet or other software	

Risk Analysis Phases based on ISO 27005

A4 - Report



*(declaration of applicability if seeking an ISO 27001 certification)

Phase: Reporting			
A4.1	Export missing security measures	Export missing security measures from the Excel spreadsheet and use that information to deal with the risks	
A4.2	Control risks	Control risks by selecting and prioritizing the measures that will mitigate as many risks as possible	
A4.3	Establish a remedial plan (declaration of applicability*) in accordance with the risk management strategy	Establish a remedial plan (declaration of applicability if seeking an ISO 27001 certification) according to the corporate risk management strategy	Remedial plan 
A4.4	Write a report	Write a report in the appropriate format and according to the organization's practices	Report 
A4.5	Prepare a presentation and an executive summary	Prepare a presentation and an executive summary for senior management	Presentation and executive summary 
A4.6	Communicate risks to the CIO and CTO	Communicate risks to the CIO and CTO	
A4.7	Communicate risks to the CSAI	Communicate risks to the CSAI and shareholders	
A4.8	Make decisions, prioritize and allocate funding	Make decisions, prioritize and allocate funding	Meeting minutes 
A4.9	Monitor, review and improve risk management	To meet ISO 27005 standards, it is recommended to monitor, review and improve risk management	