Annexes

Annex A. Control-Based Method Experimental Results

This annexe presents the implementation of the control-based method experiment.

Information Security implementation costs for both organizations were calculated according to the proposed methodology. Calculation results are presented in Table A.1, where the calculation equation is provided as well as related comments on each step.

Table A.1. Control-based method calculation steps

Formula	ACME	EMCA	Comments
Complexity and maturity coefficient $\varphi = \frac{Complexity\_level}{Maturity\_level}$	$\frac{3}{2} = 1.5$	$\frac{3}{4} = 0.75$	Higher organization maturity level let decrease the Information Security implementation and Assurance costs for EMCA

Continue of the Table A.1

Critical asset analysis $C_{Asset\_analysis} = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t)$ $C_{Consultant}(t) = Hour\_price * t$ $C_{Personal}(t) = Hour\_price * t$	$C_{Asset\_analysis} = (30 * 5) + (11 * 5) + (11 * 5) = 206$ €	$C_{Asset\_analysis} (30 * 2) + (11 * 2) + (11 * 2) = 104$ €	Critical asset analysis took: 5 hours in ACME and 2 hours in EMCA Two organization employees have participated in asset analysis.
Vulnerability analysis $C_{Vulnerabilities\_analysis} = \alpha C_{consultant}(t) + (\beta C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t))$ α and β are coefficients which define the percentage of time spent for discussion with organization employees and information evaluation.	$\alpha = \frac{2}{5} = 0.4$ $\beta = \frac{3}{5} = 0.6$ $C_{Vulnerabiliti} = (0.4 * 30 * 2) + (0.6 * 30 * 3 + 11 * 3 + 11 * 3) = 144$ €	$\alpha = \frac{1}{3} = 0.33$ $\beta = \frac{2}{3} = 0.66$ $C_{Vulnerabilities} = (0.66 * 30 * 2) + (0.33 * 30 * 1 + 11 * 1 + 11 * 1) = 84.56$ €	Vulnerability analysis took: 3 hours in ACME and 1 hour in EMCA 2 hours consultant spent to identify summarize vulnerabilities Two organization employees participated in asset analysis.
Threats analysis $C_{Threat\_analysis} = C_{Consultant}(t)$	$C_{Threat\_analy} = 30 * 4 = 120$ €	$C_{Threat\_analysi} = 30 * 4 = 120$ €	Threat analysis took 4 hours for both organizations.
Impact analysis $C_{Impact} = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t)$	$C_{Impact} = (3 * 30) + (3 * 11 + 3 * 11) = 156$ €	$C_{Impact} = (3 * 30) + (3 * 11 + 3 * 11) = 156$ €	Critical asset analysis took: 3 hours in ACME and 2 hours in EMCA

Continue of the Table A.1

Penetration testing $C_{Penetration\_testing}(N)$ $= C_{consultant}(t)$ $+ \sum_{i=1}^{n} C_{Personal_i}(t)$ $+ Fix\ cost, defined\ by\ contrac$	$C_{Penetration\_}$ $= 30 * 1$ $+ 11 * 1$ $+ 1250$ $= 1291$ €	$C_{Penetration\_te}$ $= 30 * 1$ $+ 11 * 1$ $+ 1250$ $= 1291$ €	Penetration testing requires 1-hour activities from consultant and employee. And cost 1250 € During test was tested one system (Logging and Monitoring)
Gap analysis $C_{Gap\_analysis} = C_{Consultant}(t)$	$C_{Gap\_analysis}$ $= 2 * 30$ $= 60$ €	$C_{Gap\_analysis}$ $= 2 * 30$ $= 60$ €	Threat analysis took 2 hours for both organizations.
Risk assessment process $C_{Risk\_assessment}$ $= C_{Asset\_analysis}$ $+ C_{Vulnerabilities\_analysis}$ $+ C_{Threat\_analysis}$ $+ C_{Impact}$ $+ C_{Penetration\_testing}(N)$ $+ C_{Gap\_analysis}$	$C_{Risk\_assessm}$ $= (206$ $+ 144$ $+ 120$ $+ 156$ $+ 1291$ $+ 60)$ $= 1977$ €	$C_{Risk\_assessmer}$ $= (104$ $+ 84.56$ $+ 120$ $+ 156$ $+ 1291$ $+ 60)$ $= 1815{,}56$ €	Sum of calculations done above Risk assessment cost depends on organization configuration and assessment scope.
$m_i(Risk_i)$ is Control criticality coefficient $Risk_i = Vulnerability_i$ $* Threat_i$ $* Impact_i$	$m_i - 0.7$	$m_i - 0.3$	This coefficient will be identified during the risk assessment process. Because of that for ACME: $m_i - 0.7$ and for EMCA: $m_i - 0.3$

Continue of the Table A.1

$C_{Mitigation\_strategy} = \begin{cases} -C_{Action}, \ where \ \frac{\Delta T(t)}{T(l_j)} * \bar{W} \ \leq Risk\_apetite \ and \ C_{Action} \ is \ HIGH \\ 0, \ where \ \frac{\Delta T(t)}{T(l_j)} * \bar{W} \ \leq Risk\_apetite \ and \ C_{Action} \ is \ ACCEPTABLE \\ C_{Metrics\_control}, \ where \ \frac{\Delta T(t)}{T(l_j)} * \bar{W} \ > Risk\_apetite \ and \ C_{Action} \ is \ ACCEPTABLE \\ C_{insurance} + C_{Metrics\_control} - C_{Action}, \ where \ \frac{\Delta T(t)}{T(l_j)} * \bar{W} \ > Risk\_apetite \ and \ C_{Action} \ is \ HIGH \ (Ris \end{cases}$			
$\Delta T(t)$ - Amount of security incidents during defined time t $T(l_j)$ - Amount of impacted systems lj – asset affected by a security incident, j – asset number, $\bar{W}$- Impact the average amount	$\frac{\Delta T(t)}{T(l_j)} * \bar{W} = \frac{136}{17} * 137 = 1096$ For ACME risk is below Risk appetite, so depending on the cost of mitigation controls ACME could ACCEPT risk or AVOID it Let predict, that ACME will Avoid risk.	$\frac{\Delta T(t)}{T(l_j)} * \bar{W} = \frac{136}{17} * 137 = 1096$ For EMCA risk is above Risk appetite, so depending on the cost of mitigation controls EMCA could REMEDIATE risk or TRANSFER it Let predict, that EMCA will Remediate their risk	This information is taken from statistic data for the market area or historical organization data. For ACME and EMCA, market statistics were taken: $\Delta T - 136$ incidents for Finance insurance and credit sector T – 17 assets for both organizations $\bar{W}$ – 137€ Risk appetites: for ACME is 1500 for EMCA is 1000

Continue of the Table A.1

Security Control implementation costs $C_{Security\_control\_implementation} = \sum_{i=1}^{n} (m_i\,(Risk_i) * (C_{Mitigation\_strategy_i} + C_{Action_i}))$ $C_{Metrics\_control}$ - Cost of metrics control operations, which could involve $C_{personal}$ and C_{Action} for additional specific tools, $C_{insurance}$ – Cost of insurance, according to signed off contract with 3rd party	$C_{Security\_con}$ 0.7 * C_{Action_i} = 0.7 * 352 = 246.4 €	$C_{Security\_contr}$ 0.3 * ($C_{Metrics\_contr}$ C_{Action_i}) = 0.3* (500 + 878 + 10860) =	Calculations of security implementation costs for ACME and EMCA will be different because they chose different mitigation strategy
Action Costs $C_{Action} = C_{Implementation}(t) + C_{Operation}$	C_{Action} $= C_{Operation}$	C_{Action} $= C_{Implementa}$ $+ C_{Operation}$	ACME to avoid risk, will decommissioned legacy systems from their environment. In that case, Actions cost are equal to Operation costs, needed to remove the legacy environment. EMCA will deploy logs gathering tool (Splunk), create a monitoring team.
Action implementation costs $C_{Implementation}(t) = C_{Environment\_purchase} + C_{deployment}(t)$ $C_{Environment\_purchase}$ –are hardware and software procurement costs	-	$C_{Implementatio}$ $= 500$ € $+ C_{deployment}$	Splunk tools for EMCA with all needed environment will cost 500 €

End of the Table A.1

Deployment project costs $C_{deployment}(t) = \sum_{i=1}^{n} C_{Personal_i} + C_{configuration} + C_{Training/Awareness}$ $C_{configuration}$ – is Configuration costs, $C_{Training/Awareness}$ – is Training/Awareness costs.	-	$C_{deployment}(t) = (3 * 11 * 16) + 250 + 100 = 878$ €	In Splunk deployment will participate 3 EMCA employees.And they will need 16 hours to deploy it fully. Configuration costs are defined in the contract with Splunk organization and will cost 250 €. Training will cost EMCA 100 €
Operation costs $C_{Operation} = C_{Environment\_support} + \sum_{i=1}^{n} C_{Personal_i} + C_{Other\_services}$ $C_{Environment\_support}$ is Environment support costs, $C_{Other\_services}$ – is the cost of additional services needed for effective control functionality.	$C_{Operation} = \sum_{i=1}^{n} C_{Perso} = 4 * 11 * 8 = 352$ €	$C_{Operation} = 150 + (2 * 2 * 11 * 20 * 12) = 10860$ € annually	ACME will need to decommission the legacy environment. Four employees will do it for 8 hours. Splunk environment supports cost organization 300 € annually. Splunk maintained by two employees ~2 hours during the day. EMCA do not have other services.
Information Security implementation costs $C_{Security} = \varphi(C_{Risk\_assessment} + \sum_{i=1}^{n} C_{Security\_control\_implementation}$	$C_{Security} = 1.5 * (1977 + 246.4) = 3355.1$ €	$C_{Security} = 0.75 * (1815.56 + 3671.4) = 4115.22$ €	Additional controls implementation costs depend on Risk mitigation decision and from environment configuration.