Oneconsult 360 Degree Checklist

to Manage Cyber Incidents

Follow us & stay informed!

oneconsult.com

/oneconsult-ag

/OneconsultAG

Newsletter

Oneconsult

Zurich | Bern | Munich | Auckland

The Oneconsult 360 Degree Checklist

to Manage Cyber Incidents

Instructions and Structure

The 360 Degree Checklist consists of a list of tasks to think about during a cyber incident. The goal is to provide an overview of what needs to be considered and the responsibilities and tasks of each individual, so that nothing is forgotten during the stressful situation.

The 360 Degree Checklist is modeled after the six phases of the SANS Institute‘s Incident Response (IR) process (Preparation, Identification, Containment, Eradication, Recovery, and Learnerd Lessons) and is presented in the form of a RACI matrix. The tasks listed are in a rough order, because the IR process is a cycle with many feedback loops.

To ensure that the 360 Degree Checklist is appropriate for your own company, it is essential to adapt it to the specific conditions.

Legend

- R: Responsible - Who (which person, role, organizational department) performs the task?
- A: Accountable - Who decides and has overall responsibility or will report to performing the task correctly?
- C: Consulted – Who can advise and support with expertise?
- I: Informed – Who must be informed, who can request information?

Themengebiete

The checklist includes the following five topics:

- Technical: relevant for the technical departments (e.g., IT)
- Organization: taskforce
- Personnel: mainly HR
- Legal topics: lawyers, attorneys
- Experts/external parties: IT partners, IR/forensics partners (e.g., Oneconsult)

Example

The table is read in the following way, e.g. for the first row (network plan):

- The IT department (technical) creates a network plan during the preparation phase to achieve an overview.
- The network plan is made available to the task force (organization) and the experts/external parties during the assignment.

The Oneconsult 360 Degree Checklist

to Manage Cyber Incidents

Legend: R: Responsible | **A:** Accountable | **C:** Consulted | **I:** Informed

IR-PHASES	TASKS	TECHNICAL	ORGANIZATIONAL	PERSONNEL	LEGAL TOPICS	EXPERTS/ EXTERNAL PARTIES
Preparation	Network plan	R	I			I
	Inventory of assets	R	I			I
	Classify assets according to their importance for the existence/operation of the company	R	I			I
	Protection solution (e.g. AV)	R	I			R/C
	Logging and monitoring solutions (e.g. EDR/NDR)	R	I			R/C
	Security/Vulnerability Scans	R	I			I/R
	AD overview (PingCastle)	R	I			I/R
	Patch/vulnerability management	R	A			R/C
	Securing data from logging and monitoring solutions	R	I			R/C
	Authorizations for data collection and analysis	I	I		R	C
	Backup concept	R	A			R/C
	Access concept (keys, etc.)	I	R			
	Contact list (employees, management, IT partners, etc.)	I	R	(I)	(I)	I
	Communication plan	I	R	(I)	(I)	I/C
	Define communication channels and tools for conversations, meetings and data exchange	I	R	(I)	(I)	I
	Communication towards employees, partners, public, authorities (if obligated)	I	A	R	I	C
	Define roles and responsibilities	I	R	I		I
	Clarify and review contracts and terms (IT partner, IR/forensics partner, cyber insurance, etc.)	I	R			I/C
	Incident Response Plan	R	I	I	(I)	R/C
	Strategy in case of extortion (e.g., ransomware/data disclosure)	I	R		C	C
	Legal restrictions (e.g., other countries)		I		R	C
	Personnel consequences/compensation to institutions/partners.		I		R	C
	Notification requirements (GDPR, association requirements, industry-specific requirements, etc.)		I/R		R	C
	Informing insurance company		I/R		R	C
	Report to the police		I/R		R	C
Identification	Performing AV scans everywhere	R				R/C
	Determining the crisis level	I	R			C
	Inquiry of the incident history (suspects, clues, traces, etc.)	(R)	I			R
	Detection of potential damage		R			C
	Are other companies affected?		R			I/C
	Define and run through worst- and best-case scenarios and derive necessary measures from them and implement them if necessary	I	R			I/C
	How often and who should assess the situation?	I	R			I/C
	Holding status meetings and taking minutes	I	R			I
	Communicating daily objectives	I	R			I/C
	Setting priorities and strategy	I	R			C
	Division of tasks	I	R			I
	Creating a ToDo list and checking completion or processing of tasks	I	R			I
	Identifying conflict potential (with other people/companies)		R	(I)		
	Identifying knowledge sources/key persons	I	I	R		
	Defining contact persons for the systems/areas	R	I	I		I
	Planning availability of resources (who, when, how)	R	A	R	R	R
	Resource planning of technical means (storage, computers, etc.)	R	A/I			
	Providing a "War Room"	I	R			I
	Organizing materials (office supplies, flip charts, etc.)		R			
	Catering (food and drinks)	I	R	I		I
	Care team for affected persons (personal or psychological/ stress)	I	I	R		

The Oneconsult 360 Degree Checklist

to Manage Cyber Incidents

Legend: R: Responsible | **A:** Accountable | **C:** Consulted | **I:** Informed

IR-PHASES	TASKS	TECHNICAL	ORGANIZATIONAL	PERSONNEL	LEGAL TOPICS	EXPERTS/ EXTERNAL PARTIES
Containment	Isolating systems	R				C
	Shutting down network and cutting connections to/ from external parties	R	A			
	Protecting unaffected systems	R				C
	Backing up relevant data and creating Images	R				R/C
	Blocking malicious IP addresses and domains	R				C
	Disabling accounts	R				C
	Forensic analysis	(R)	I			R
	Providing and securing emergency operation	R				C
Eradication	Determining process for setting up clean systems	I	R			C
	Checking backups for infections	R				C
	Preparing a clean and isolated environment for the restoration	R				C
	Resetting all passwords (including admin, services and Kerberos)	R				C
	Verifying accounts for legitimacy	R				C
	Updating and patching externally accessible services	R				C
Recovery	Restore (Restart, from backups, etc.)	R	I			C
	Restore network traffic	R	A			
	Enabling services	R	A			R/C
	Hardening of systems, GPO, etc.	R				C
	Firewall management	R	I			C
	Creating logpolicies	R	I			C
	Increased monitoring	R	I			C
Learned Lessons	Documentation (final report)	R	I	I	I	R/C
	Lessons learned meeting/debriefing of the incident	I	R	I	I	R/C
	Keeping minutes of the meeting	I	R	I	I	R/C
	Reviewing and adjusting processes, implementing measures	R	A/R	(R)	(R)	C

Oneconsult AG
Giesshübelstrasse 45
8045 Zurich
Schweiz

+41 43 377 22 22
info@oneconsult.com
www.oneconsult.com

oneconsult
together against cyberattacks