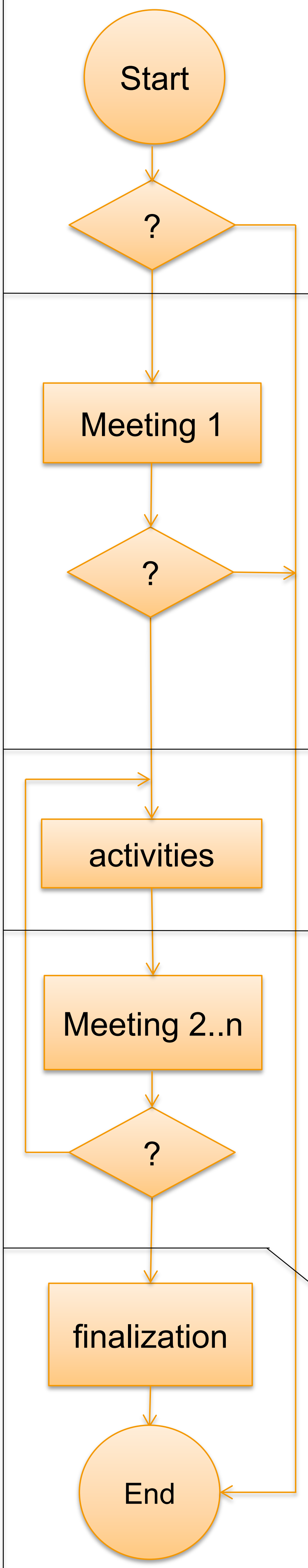
Course of action during an incident / evaluation of state

Goal: coordinated actions during an incident



Step	Description	Input ← / Output →
	Information abut an incident - Relevant for our customers or is it all over all media? (get 2nd opinion in the team) - **Decision: ad-hoc meeting** to decide on coordinated actions - **Yes:** set up ad-hoc meeting - **No:** no activity, further supervision? One time information?	← **Examples:** important vulnerability (Heartbleed); Data leakage (millions of usernames, passwords), etc.
	Ad-hoc-Meeting Participants: all available team members (when useful) **Goal:** evaluation of situation/state and coordination of actions - What do we know? Is it relevant for our customers? - **Decision: coordinated actions needed?** - **Yes:** - plan of actions - Next meeting (e.g. in 1h) - Appoint roles (coordinator, incident handler) - **No:** - no actions? One time info? Further surveillance (who)?	← Activity checklist → ToDoList (what, who, until when) → roles → Next meeting
	Perform decided activities - If the situation changes essentially, discuss impact, evt. Ad-hoc meeting	← **ToDo-List** ← **Templates** (e.g. Security-Advisory) → (what is listed in the ToDo-list)
	Update-Meeting Participants: incident coordinator, hotline coordinator, incident handler **Goal:** state of actions and situation, coordinate following steps - State of the activities? - New information? - How do we respond upon it? New activities (e.g.. Update Security-Advisory)? Change existing activities? - **Decision:** next meeting or final actions	→ Updated **ToDo-List** → Evt. Next update meeting
	Finalization - Open points from ToDo-List e.g. - Lessons learned - Optimize processes - Recommendations (articles, etc.) - Update of statistics, work reports	← **ToDo-List** → (points from ToDo-List)

Activity checklist Incident / evaluation of state

Goal: make sure, don’t forget any important activity
Output: ToDo-List

A. At start during the first ad-hoc meeting	**ja***	**nein**	**?**
• Direct information of customers? Heads-up or advisory? • Heads-up: There’s something, we don’t know the details yet, links/articles • Advisory: there’s something, this are our recommendations; links/articles • Information to • Own organization • Helpdesk • Management • Peers / neighbour organizations • … • Do we need further information? Where from? Who gets them? • Preparing scripts, configurations? What? Who? • Who’s keeping an eye on the media / sources? • Can we get information from partners? What? Who? • **Can the incident handler handle the case? Help needed?** • **Re-prioritization of other tasks?** • Who’s coordinating? (is also owner of the ToDo-List), who’s the incident handler? • Are Social-Media activities or marketing activities adequate? Heads up? Who’s coordinating this activities? • **Next meeting**			
B. Update meeting			
• New facts, change of situation which we should pass to our customers/peers? • Which activities need a change / update? New ToDos • **Next update-Meeting**? When?			
C. Finalization			
• All ToDos finished? • Lessons learned • Regarding the incident • Regarding our proceedings • Next steps useful? Final report etc.			