Process Mining for Cyber Risk Assessment for Cyber Insurance

Thank you for taking your time to answer a short questionnaire about assessing internal processes for cyber risk assessment purposes.

The questionnaire should take between 25-30 minutes, and is meant to be followed by a short open interview.

* Required

1. Please select an option that best describes your role and area of expertise

Mark only one oval.

○ Underwriter Cyber

○ Underwriter (other P&C)

○ (Risk) Analyst

○ Actuarial / Risk Consultant

○ Insurance Broker / Agent

○ Reinsurance Underwriter

○ Product Manager / Specialist / other roles in Product development

○ Other Cyber Security Specialist / Expert

○ Other: ______________________________

Section 1: Business Process Perspective in Cyber Risk Assessment

In the following section, you will be asked a series of general questions regarding you views on cyber risk assessment methods and on the analysis of process perspective in the cyber security context.

2. How would you rate the importance of data mining and general log analysis in the context of cyber risk assessment of individual companies?

Mark only one oval.

	1	2	3	4	5	
Irrelevant	○	○	○	○	○	Critically Important

3. How would you rate the following statement: "Compared to qualitative methods (such as self-assessments, interviews, or analyses of policies), quantitative analyses of actual behavior (from productive systems) are more likely to reduce information asymmetries between the cyber risk analyst (e.g. IT Auditor, Cyber Underwriter, Regulator) and the organization subjected to the analysis."

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

4. How would you rate the following statement: "Investigating how internal processes of a given company operate is crucial for cyber risk assessment."

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Section 2: Process Discovery

In the following section, you will be asked to provide your cyber risk assessment based on visual analysis of process map generated by a process discovery algorithm.

Scenario 1: Insider-Threat Detection - Suspicious File Operations

Let's pose the following set up. As a risk analyst you are tasked with assessing the cyber risk associated with underwriting a Cyber, Privacy, and Network Security Liability coverage for a private bank. You decide to investigate the flow of sensitive data in the bank.

The IT Compliance responsible of the bank is convinced that their handling of sensitive data runs in a compliant way and provides you with a policy document with the following information on rules that should be followed, that he believes proves compliance:

Rule 0 (start event): Employees begin the day by retrieving the data they need for their responsibilities from a back-up machine. In the unit that you are analyzing, all data retrieved from the machine is considered sensitive.

Rule 1: Users that are part of the same team (e.g. team-1_user-1 and team-1_user-4) can share files with one another directly, but communication between teams needs to go through and be recorded in a communication hub of that team (e.g. communication-hub_team_1)

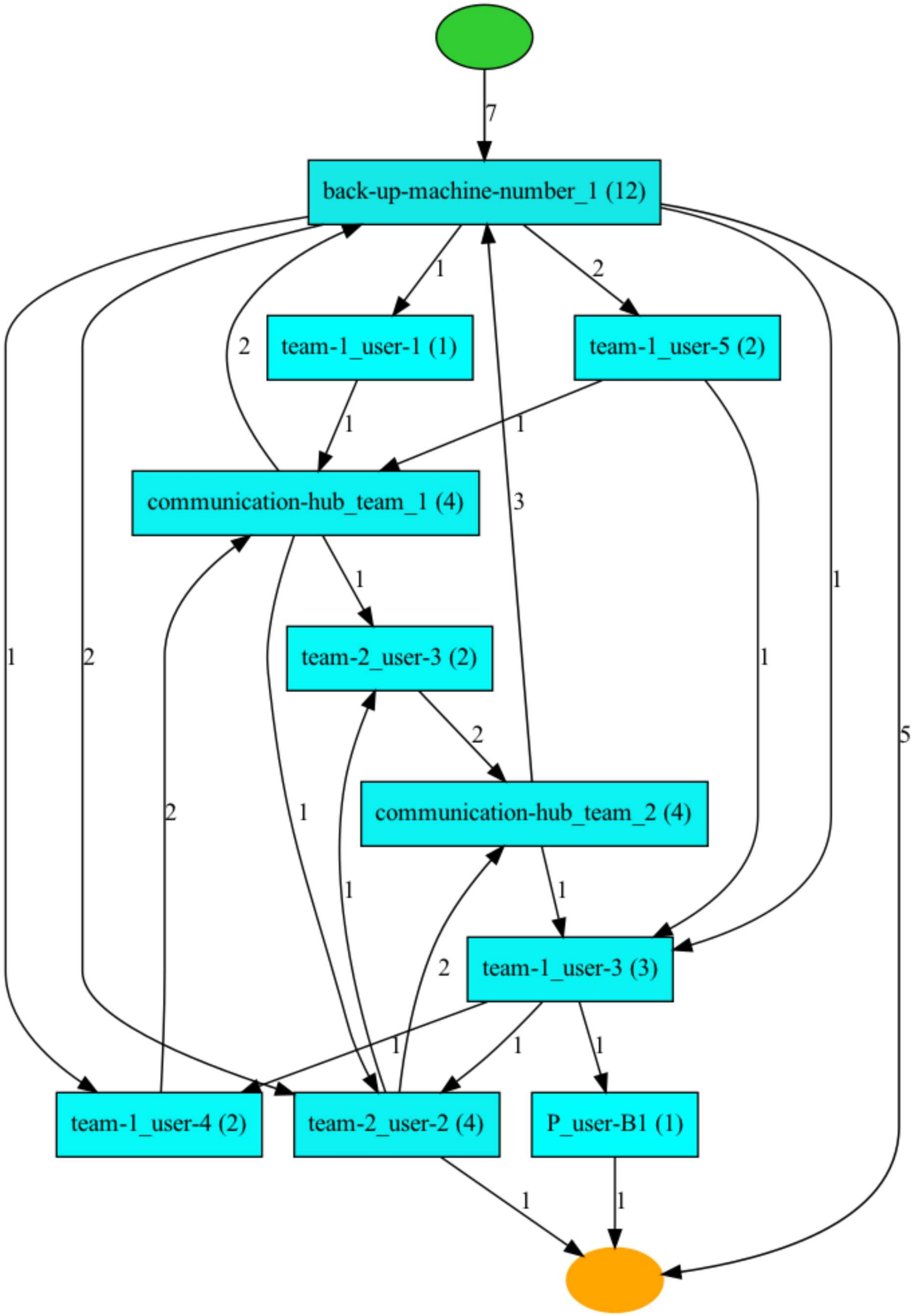
Rule 2: It is strictly forbidden to share sensitive data in a public system (denoted with 'P')

Rule 3: Data is eventually backed up from the communication hubs to the 'back-up machine'

As you want to verify the claim of the IT Compliance responsible, you decide to analyze the EventLog generated by mining the workstations of the employees.

You apply the process discovery method (heuristic miner) on the log and generate the following visualization (process map) of how files move across the organization. Please kindly review it and answer the questions below.

Process Map Discovered with Heuristic Miner



5. For which of the following rules can you identify violations, based on your interpretation of the process map

Check all that apply.

□ Rule 1: Communication between teams needs to go through and be recorded in a communication hub

□ Rule 2: No sharing of data in public systems

□ Rule 3: Mandatory eventual back-up of communication hubs

□ For none of them

6. In case you identified any of the violations outlined above, what (if any) influence does this have on your assessment of the following confidence factors (made available by the Chubb Reinsurance Company)? Note: A positive assessment would potentially lead to a premium discount, whereas a negative assessment to a premium increase. *

Mark only one oval per row.

	Positive influence	No influence	Slightly negative influence	Red flag	Would trigger further investigations
Handling of sensitive information	○	○	○	○	○
Backup/Mirror Procedures	○	○	○	○	○
Compliance with privacy regulations	○	○	○	○	○
Risk Management Controls	○	○	○	○	○
Employee Training	○	○	○	○	○
System Management	○	○	○	○	○

7. Please rate the following statement: "Providing visual abstractions of process flows is a viable way to enable business users to conduct simple cyber risk assessments based on rules."

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Section 3: Process Conformance

Conformance checking is a family of process mining techniques to compare a process model with an event log of the same process. It is used to check if the actual execution of a business process, as recorded in the event log, conforms to the model and vice versa.

Deviations identified using conformance checking may, for example, point at attackers acting in the system, malware, insider-threats, users using undesirable workarounds, or fraud.

In the following section, you will be asked to assess a simplified scenario in regard to the impact of the findings on your assessment of the cyber risk (modifiers) associated with the process.

Scenario 2: Identity Access Management

Let's assume the following scenario.

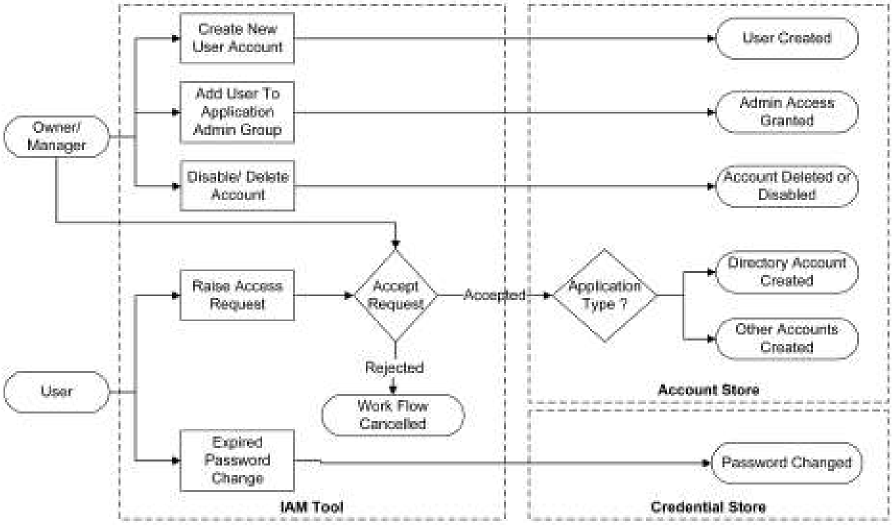
You are provided with the following reference process model by the IT Security team of a major hospital, that reflects their defined Identity Access Management (IAM) practice.

Your task is assessing their cyber security posture for the purposes of cyber insurance under time and resource constraints.
For the purpose of assessing their access controls, you decide to check whether the prescribed model holds in practice.

You therefore decide to extract an EventLog merging all events from the IAM Tool, Account Store (AD) and Credential store and to check whether that process holds in reality.

Please rate the series of statements below, which present you with findings generated by a conformance checking analysis.

Reference model of the IAM process provided by the company



Step 1: Checking fitness of the model against the EventLog

First, you decide to use an automated tool convert the prescribed model to a computer-readable format (i.e. petri net) and using automated conformance checking method (token-based-replay) test, whether the process instances in the EventLog conform to the model. You find out that only 40% of the process instances recorded in reality can be explained (replayed in) the model. In other words, the model allows for only 40% of the instances recorded.

8. What impact on your perception of the IAM process does the low fitness of the model have on your perception of the business process from the cyber risk perspective?

Mark only one oval.

	1	2	3	4	5	
No impact / inconclusive / not-interpretable	○	○	○	○	○	Points at increased risk

9. Please shortly comment on your perception of risk based on the metric

Step 2

You investigate further and, using conformance checking techniques, identify that the low trace fitness can be traced back to a high number of process instances skipping the steps in the IAM system altogether. You identify that 20% of the cases start with manual User Deletion, or manual User Creation events in the Account Store, which is in direct violation of the policy.

10. What impact does the information in step two have on you assessment of the IAM process from the risk perspective?

Mark only one oval.

	1	2	3	4	5	
No impact / inconclusive / not-interpretable	○	○	○	○	○	Points at increased risk

11. What (if any) impact would the limited information have on your assessment of risk modifiers that might have positive / negative impact on cyber insurance premiums? (modifiers by Chubb Reinsurance) *

Mark only one oval per row.

	Positive influence	No influence	Slightly negative influence	Red flag	Not decisive. Would trigger further investigations
Network Security	○	○	○	○	○
Risk Management Controls	○	○	○	○	○
System Management	○	○	○	○	○
Network Access Control	○	○	○	○	○

Section 3: Process Enhancement for Cyber Security

So far, we have focused on applying process mining to detect anomalies and identify threats. In the final scenario, we will focus on process enhancement.

Scenario 3: IT Incident Response - Major carmaker

For the final scenario, we will consider the Incident Management Process (containing events from Acceptance to Resolution) based on a real-life process model and EventLog. Details are intentionally abstracted away for the purposes of the scenario.

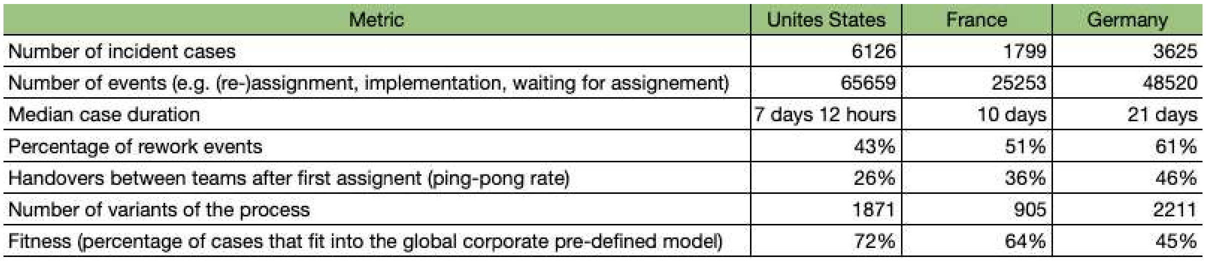
The car manufacturer has a globally defined Incident Management process, which is executed by subsidiaries across the world. In the scenario, we will observe three different countries, which are supported by dedicated local teams. Those teams, however, aim to follow the globally defined process and are otherwise independent of each other.

The set-up of the case study is that we want to rate the risk modifiers, taking the relative posture of other subsidiaries into consideration.In the scenario, we assume that the car manufacturer might arrange a separate cyber insurance agreement for each subsidiary.

The EventLog has been processed, discovery and conformance checking techniques applied, as well as process statistics generated.

Based on the summary of metrics generated below, please fill out the table below. In the open part of the interview, you will be asked on the reasoning behind your choices.

Summary of the metrics generated with automated process analysis



Metric	Unites States	France	Germany
Number of incident cases	6126	1799	3625
Number of events (e.g. (re-)assignment, implementation, waiting for assignement)	65659	25253	48520
Median case duration	7 days 12 hours	10 days	21 days
Percentage of rework events	43%	51%	61%
Handovers between teams after first assignent (ping-pong rate)	26%	36%	46%
Number of variants of the process	1871	905	2211
Fitness (percentage of cases that fit into the global corporate pre-defined model)	72%	64%	45%

12. Based on the information from the table. Please indicate how you would rate the risk modifiers (as per the Chubb cyber underwriting manual) for Germany relative to other subsidiaries. *

Mark only one oval per row.

	Significantly more favorable rating	Slightly more favorable rating	No influence / no difference in rating	Slightly less favorable rating	Significantly less favorable rating
Incident Response Planning	○	○	○	○	○
Risk Management Controls	○	○	○	○	○
Centralised Processes and Procedures	○	○	○	○	○
Employee Training	○	○	○	○	○
Training and Education	○	○	○	○	○
Disaster Recovery	○	○	○	○	○

Thank you!

This concludes the survey. Next, I would like to ask you to continue with a very brief semi-structured interview.