DEMO (40% of full document)

RISK ASSESSMENT
(GENERAL RISK ASSESSMENT)

1. **The Context** should be established, i.e. the object of the risk assessment should be defined and the result of the inventory control taken into account. *For example, a paper file containing the employees' personal data stored in a wooden lockable cabinet in the headquarters as part of the employer's obligations*.
2. When assessing the risk, examining scenarios and deciding about separate resources, one must **take into account the entire "life cycle" of information – from its inflow or generation to its archiving or deletion.**
3. Before starting a risk assessment, it is necessary to establish who is the person directly responsible for a given information resource.
4. The value of an information resource must be established (e.g. on a scale of 1 to 4), depending on the type and importance of the information contained there – whether it contains health information, information on salary amount or just the address of residence and education, as specified in the table below:

Resource value	Information categories
(4) **Sensitive**	**Exclusively: data concerning health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for the purpose of identification), data concerning sex life or sexual orientation**
(3) **Financial**	**E.g. amount of salary, history of financial transactions, documents related to the use of banking services, investments, credit cards, invoices, insurance documents relating to the financial situation**
(2) **Behavioural** (pointing to certain behaviours)	**E.g. ordinary Web browser history, information on location (e.g. navigation applications), Web traffic information (billings, IP number), information on personal habits and routines**
(1) **Simple**	**E.g. name and surname, professional experience, qualifications, education, contact details (email, telephone number)**

5. Having established the context, we should examine the scenarios of possible risks, a list of which is included in **tables I–II (for paper records) and in III–IV (for electronic records).**
6. If we are able to show other risk scenarios with regard to our business activity than those included in the model risk scenarios, they should be added in subsequent lines in the relevant tables.
7. **The tables with exemplary entries** can be helpful in examining the scenarios; you should remember, however, that the tables should be examined with reference to your own business activity.
8. When examining the scenarios, we must take into account the **"supporting assets",** that is the tools, locations and the people directly using, for example, specific documents or programs for which an assessment is prepared.
9. A scenario examination should also account for the **currently applied** (at the time of the risk assessment) safeguards before the implementation of a specific scenario.
10. It is primarily the type of "**vulnerabilities**" of the "supporting assets" that determine the "**probability**" that a given scenario would become reality.
11.