Review IT system training by asking the following questions:

- What is the timetable for training, and what kind of training is provided? Is attendance obligatory? Does everyone have the option to attend? Do those holding the training course have the correct expertise?
- How is participation in and the quality of IT training documented?
- How are new employees introduced to the workplace and how is their digital competence ensured?

Review system error/crash routines by asking the following questions:

- Who do you contact if you have a problem?
- Are there written procedures in the event of system errors/crashes?
- Where are backups kept of personal codes, manual Dictaphones and paper forms, for example sick certificates?
- How is submitted documentation saved during a system crash?

Introduce crash exercises if none exist!

After the inspection

Action plan and arrangement of follow-up meeting

- Compile a list of current improvement requirements and issues.
- Propose improvement measures, including risk assessments for the work environment and quality assurance for the organisation, and if it is relevant from a client/security perspective.
- Establish an action plan for improvement measures
- Distribute responsibility for ensuring that the measures are implemented.
- Compile a list of issues that need to be discussed or referred to another part of the organisation.
- A comprehensive follow-up meeting can be held after a couple of months. It is important that everyone is aware of the timetable and their responsibility for realising the proposed improvements.
- Don't forget the importance of report the results back to the users/employees at workplace. Worker participation is a key role when improving the digital aspects of occupational health and safety.

Learn more about IT safety inspections and digital work environments at vision.se/arbetsmiljo.

Let IT disruption show you the way

This is how to implement an IT safety inspection to improve your digital work environment

vision.se/arbetsmiljo

On average, Vision's members lose almost 30 minutes of each working day due to IT disruption. This means that almost one working day is lost each month. By implementing IT safety inspections, you can identify where this time is being lost and where in your digital work environment improvements are needed. By involving staff, compiling improvement proposals and requirements to develop usability, and increasing competence as a client prior to the organisation's next IT procurement process.

Why should you implement IT safety inspections?

The primary purpose is simple; to improve the digital work environment and usability by identifying necessary improvements and problems in the existing IT system. Certain issues can then be rectified while others can be taken into account during the next procurement process. By working with IT safety inspections, you increase contact between operational management, system providers and users/employees within your organisation, to obtain a common picture of how your digital solutions are working in practice. Your client expertice in the procurement work will increase. Employees and management who are able to influence the development of the organisation's IT system experience less disruption and stress, and deliver better quality work. The employer also benefits from involving staff at an early stage, in that they will obtain an IT system in good working order and better health among the employees.

What is an IT safety inspection?

An IT safety inspection is performed in a similar fashion to a traditional safety inspection, although it also involves users/employees and IT developers. It is a method for systematically reviewing the digital aspects of the occupational health and safety environment.. It covers everything from flaws in the usability of the IT system and practical problems such as logging in, to training and crash procedures, etc.

This is how to carry out an IT safety inspection

Preparation

- Appoint those who are to participate, e.g. users/employees, manager, safety representative, IT developer, procurement manager
- Book time for both an IT safety inspection and for a follow-up meeting. Decide which activity/process is to be reviewed.
- Decide which programs/software are to be included.

Implementation

Review the activity/process with regard to:

- Hardware
- Software
- Ancillary equipment, e.g. printers, terminals, etc. Systematically inspect the program/activity in question. Which parameters should be assessed?

Points for assessment during the inspection:

- Potential safety risks
- Clarity
- Intuitiveness, e.g. graphic interface, design of forms
- Usability – the level of utility that the system provides for a user in a given situation.
- Communication with other relevant systems
- Different types of modules that may exist
- Number of printouts done/required
- Time required for typical case
- Concrete problems with the system, proposed improvements
- Any information from previous safety inspections/system evaluations