FSOR

FINANCIAL SECTOR FORUM
FOR OPERATIONAL RESILIENCE

28 August 2020

# Handbook of methodology for FSOR's risk analysis

# 1 Introduction

One of FSOR's tasks is to ensure a comprehensive overview of operational risks that could affect the entire sector and potentially threaten financial stability. FSOR therefore prepares a risk analysis to identify relevant risks and ensure a comprehensive overview. The risk analysis forms the basis for deciding and implementing joint actions to strengthen the resilience of the financial sector to major operational events, including cyber attacks.

The methodology used to prepare and maintain FSOR's risk analysis is described in the following. The work is carried out by the FSOR-RISK working group. The group's current members and contact details can be found in Appendix 3.

# 2 Purpose and limitation of the risk analysis

FSOR's risk analysis aims to identify and address operational risks, including cyber risks, which have the potential to threaten financial stability. As part of the risk analysis, critical infrastructure in the financial sector is identified. This will provide FSOR with a comprehensive overview of critical business activities, systems, suppliers, contexts and dependencies in the financial sector.

Financial stability is a state where the financial system as a whole is so resilient that any problems in the sector do not spread and prevent the financial system from acting as an effective provider of capital and financial services. In terms of operational resilience, financial stability could potentially be under threat by serious incidents causing a lengthy breakdown or compromising of critical business activities and/or affecting trust in the financial system. The risk analysis criteria for assessing whether a risk could threaten financial stability are shown in Box 1.

In selecting mitigating actions to address the risk identified, FSOR focuses on actions where the financial sector can usefully coordinate and cooperate to increase operational resilience for the sector as a whole.

Every financial institution is responsible for risk management in relation to its own operational resilience and IT security. FSOR's risk analysis does not replace the individual players' own risk management and mitigating actions. FSOR's risk analysis complements the

players' own risk management and can provide input to it. Similarly, FSOR's risk analysis complements the risk analysis of the Risk Forum for Interdependencies (RGA), which focuses on risks associated with dependencies between Kronos2, VP and retail payment systems.

## 2.1 Financial stability criteria

The following criteria are used to assess whether financial stability may be under threat by an operational incident, including a cyber attack.

### Criteria for assessing whether financial stability could potentially be under threat — Box 1

Financial stability could potentially be under threat when one or more of the following criteria are met:

Critical business activity unavailable or compromised.

- A breakdown affects several critical players during a critical time period or at a critical point in time.
- The confidentiality of critical assets is compromised, for example as a result of a cyber attack.
- Doubts arise about the integrity of critical data, for example as a result of a cyber attack.

Citizens'/businesses' trust in the financial system is under threat.

- A critically large share is directly or indirectly affected via media.

Investor confidence in Danish assets/markets is under threat.

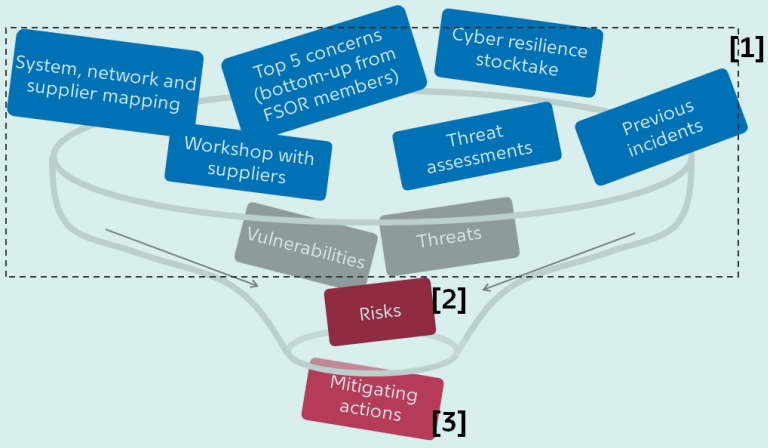
- Many investors are directly or indirectly affected through media or rating agencies.

# 3 Risk management process

FSOR's risk assessment is prepared as illustrated in the 'funnel' in Chart 1.

1. First, a broad assessment is made of the risks that could potentially threaten financial stability, see **[1]** in Chart 1. This is first and foremost done by maintaining a foundation for the risk analysis consisting of a mapping of critical business activities and critical infrastructure as described in section 4.1, and secondly by continuously obtaining information about threats and vulnerabilities from various sources, see section 4.2.
2. Once threats and vulnerabilities have been assessed, **risks are identified**, see **[2]**. **Risks are assessed** on a scale of 1 to 5 based on likelihood and impact, see section 5. The initial assessment is carried out by the FSOR-RISK working group.
3. The results are then **reported** to FSOR at the biannual FSOR meetings. Based on input from FSOR, FSOR-RISK also proposes mitigating actions, see **[3]. Implementation of mitigating actions** is initiated by FSOR, and the status of the implementation is discussed at the FSOR meetings, see sections 6 and 7.

**FSOR risk analysis workflow** **Chart 1**




Note: The risk analysis is prepared by collecting input which is placed in the funnel at the top, after which risks are identified and addressed, resulting in a number of recommendations for FSOR on how to proceed with mitigating actions.
Source: FSOR.

# 4 Risk identification

Risks are identified on the basis of a number of sources that highlight vulnerabilities and threats to financial stability. The sources are described below.

## 4.1 Foundation and limitation – re [1]

The foundation of FSOR's risk analysis is a mapping of critical business activities in the financial sector and critical infrastructure, which provides a comprehensive overview of critical business activities, systems, suppliers and contexts in the financial sector. The risk analysis is limited to the risks that could potentially affect critical business activities and thus threaten financial stability.

The foundation for the risk analysis consists of:

- Gross list of business activities in the financial sector.
- Selection of the most critical business activities, i.e. the activities where a breakdown may have consequences that could potentially threaten financial stability within the shortest time period. At present, five critical business activities have been identified.
- Business Impact Analysis (BIA) for each of the critical business activities. The BIA assesses the consequences of breakdowns and identifies the processes, systems and suppliers that support the business activity. The BIA format is shown in Appendix 1.
- Mapping of critical infrastructure that supports critical business activities and shows interdependencies between critical financial infrastructures.

The mapping provides input to potential vulnerabilities associated with, for example, the use of few or the same suppliers of critical systems and networks as well as dependencies on public infrastructure, i.e. shared official digital services and registers such as NemID, e-Boks, the land registry, the Danish Civil Registration System etc.

The foundation is revisited and updated at least once a year or more frequently if conditions require it.

## 4.2 Other sources of threats and vulnerabilities – re [1]

In addition, when the risk analysis is updated, input for threats, and vulnerabilities in relation to the stable operation of the five critical business activities is collected. Input is collected from the following sources, among others (the list is not exhaustive):

- Study of FSOR members' top-5 concerns
- Input from Risk Forum for Interdependencies (RGA)
- Input from FSOR-RISK, including on future system changes and new regulation

- Threat assessments from the Danish Centre For Cyber Security, CFCS
- Other threat assessments such as the National Threat Picture, TIBER-DK's generic threat landscape, NFCERT's quarterly threat assessment report and the Cyber Information and Intelligence Sharing Initiative (CIISI-EU)
- Vulnerabilities identified in FSOR's cyber stocktake
- Relevant incidents.

The study of the FSOR members' top-5 concerns is carried out annually by FSOR's secretariat. The study captures the FSOR members' 3-5 main concerns in relation to the stable operation of critical business activities in the financial sector. The concerns are grouped and ranked in an ISF threat catalogue and compared with the results of the previous year(s). This study, together with other sources, provides input on the risks to be focused on in FSOR's risk analysis.

### 4.3 Risk descriptions – re [2]

All risks are described with a risk cause, risk incident and risk effect (the bowtie concept is used). In addition, each risk is categorised into one of the five risk categories below (the risk category is shown in the risk register):

1 – Operational disruptions
2 – Supplier management
3 – Cyber resilience
4 – Compliance risk
5 – Other.

Based on the risk descriptions, each risk is assigned a score on a scale of 1 to 5 for likelihood and impact, respectively, and ranked in a risk matrix, see the next section.

# 5 Risk matrix and risk appetite – re [2]

The ranking of risks in the risk matrix is based on a scale for likelihood and impact, respectively. Likelihood (vertical axis) is assessed according to how often an incident is expected to occur, but it can also be assessed on the basis of, for example, maturity and complexity in different areas. Impact (horizontal axis) reflects the criteria for assessing whether financial stability is potentially under threat, see Box 1. The risk matrix with all scales is shown in Appendix 2.

**FSOR's risk matrix** **Chart 2**


Note: The figures indicate likelihood (1-5) times impact (1-5).
Source: FSOR-RISK.

FSOR's risk matrix is divided into the colours red, orange, yellow and green, see Chart 2. The colour distribution is slightly skewed towards the lower right corner, so that FSOR pays extra attention to high-impact risks, even when likelihood is low.

# 6 Mitigating actions – re [3]

All risks are reported to FSOR. The colour category of the risks reflects FSOR's risk appetite and guides FSOR's treatment of the risks:

Risks in **red**: FSOR discusses all risks in red, and FSOR-RISK proposes mitigating actions to FSOR.

Risks in **orange**: FSOR discusses all risks in orange, including whether mitigating actions should be taken. FSOR-RISK provides input on which mitigating actions would be the most appropriate.

Risks in **yellow**: FSOR discusses whether selected risks should be mitigated. FSOR-RISK provides input on the most important risks to address.

Risks in **green**: As a general rule, FSOR-RISK does not propose mitigating actions.

It may be necessary to obtain more information about a risk before FSOR takes a final position on mitigating a risk.

# 7 Continuous update of the risk analysis – annual wheel

The 'funnel' in Chart 1 illustrates how a single update of the risk analysis is carried out. In practice, it is an ongoing process in which the risk analysis is generally updated twice a year by the FSOR-RISK working group which meets every six months; approximately 2 months before each FSOR meeting. The working group reports the result of the update to FSOR for discussion at the next FSOR meeting, see the annual wheel illustrated in Chart 3. The status of mitigating actions initiated and how to proceed are also discussed at the FSOR meetings.

## 7.1 Working group meetings in FSOR-RISK

The following tasks are addressed at the working group meetings:

- Input to threats/vulnerabilities/concerns is discussed, see **[1]** in Chart 1.
- The ranking of the existing risks is revisited, and any changes are made, see **[2]**. The status of mitigating actions initiated is addressed in the discussions when appropriate.
  - New risks are discussed and, where appropriate, added to the risk analysis, see **[2]**. Major upcoming system changes in infrastructure and new regulation to be implemented in the financial sector are also routinely discussed when appropriate.
  - Input to mitigating actions to be presented to FSOR is discussed, see **[3]** in Chart 1.
  - Every 2-3 years in **September**, the gross list of business activities in the financial sector is revisited, and the scope of the risk analysis, i.e. critical business activities, is reconsidered. Moreover, the point of time where a business activity becomes critical and the the activation criteria for FSOR's Crisis Response Group are revisited.
  - In **March**, the foundation for the risk analysis (i.e. BIA for critical business activities and mapping) is revisited.

**Annual wheel** **Chart 3**


Source: FSOR-RISK.

- In **September**, the result of the study of the FSOR members' top-5 concerns in relation to the stable operation of critical business activities in the financial sector is discussed.
- In **September**, the methodology, processes and maturity of the risk analysis are evaluated and changes are decided upon as needed. This methodology description is updated when appropriate.

## 7.2 Conference calls

In between meetings, conference calls may be held as needed, with the working group discussing, for example, likelihood, impact and the need for mitigating actions to address an emerging risk.

## 7.3 Continuous input and handling

FSOR-RISK, FSOR members and FSOR's secretariat can report potential risks to the risk analysis on an ongoing basis. New risks will be discussed at the next working group meeting at the latest, during a conference call set up for the occasion or at additional physical meetings as needed.

Specific urgent situations are handled according to FSOR's crisis response plan.

# 8 Governance

## 8.1 FSOR-RISK working group

The risk analysis is maintained by the FSOR-RISK working group, which is composed of representatives from a wide range of FSOR members, including banks, financial infrastructures, data centres, authorities and CFCS. The working group is headed by FSOR's secretariat.

## 8.2 Document management

Documents relating to FSOR's risk analysis are stored in the 'FSOR risk analysis' section on Danmarks Nationalbank's extranet (confidential document management system) which can be accessed by the working group. The section is maintained by FSOR's secretariat.

The risk analysis is documented in a risk tool updated by Danmarks Nationalbank. The risk tool is stored on the extranet. The latest versions of the risk analysis foundation and methodology description are also stored on the extranet.

FSOR classifies material based on a 'Traffic Light Protocol', TLP. The material can be categorised into four classes: TLP:WHITE, TLP:GREEN, TLP:AMBER AND TLP:RED. Documents with information about threats, vulnerabilities, risks, mitigating actions etc. are typically classified as TLP:AMBER (limited disclosure), which applies to material of a sensitive nature that may have medium or serious negative consequences for FSOR or individual members in the event of a leak. Documents classified as TLP:AMBER are only shared via the extranet and may only be shared on a need-to-know basis inside the FSOR member's organisation. Documents containing information about the methodology are typically classified as TLP:GREEN (internal disclosure), which means that they can be shared inside the member's organisation with a work-relevant circle of people. TLP:GREEN documents are primarily shared via the extranet. An overview of the rules on confidentiality, classification and handling of material is provided in Appendix 4, which specifies what TLP:WHITE, TLP:GREEN, TLP:AMBER and TLP:RED covers.

## 8.3 Division of responsibilities

Different players may be relevant for dealing with the risks identified in the risk analysis:

- Risks where FSOR can contribute to increased operational resilience in the financial sector through joint actions are dealt with by FSOR.
- Risks related to dependencies between VP, Kronos2 and retail payment systems are transferred to and dealt with by the Risk Forum for Interdependencies (RGA).
- Risks affecting several critical sectors of society should be dealt with at national level.
- Some risks should be dealt with by individual players.

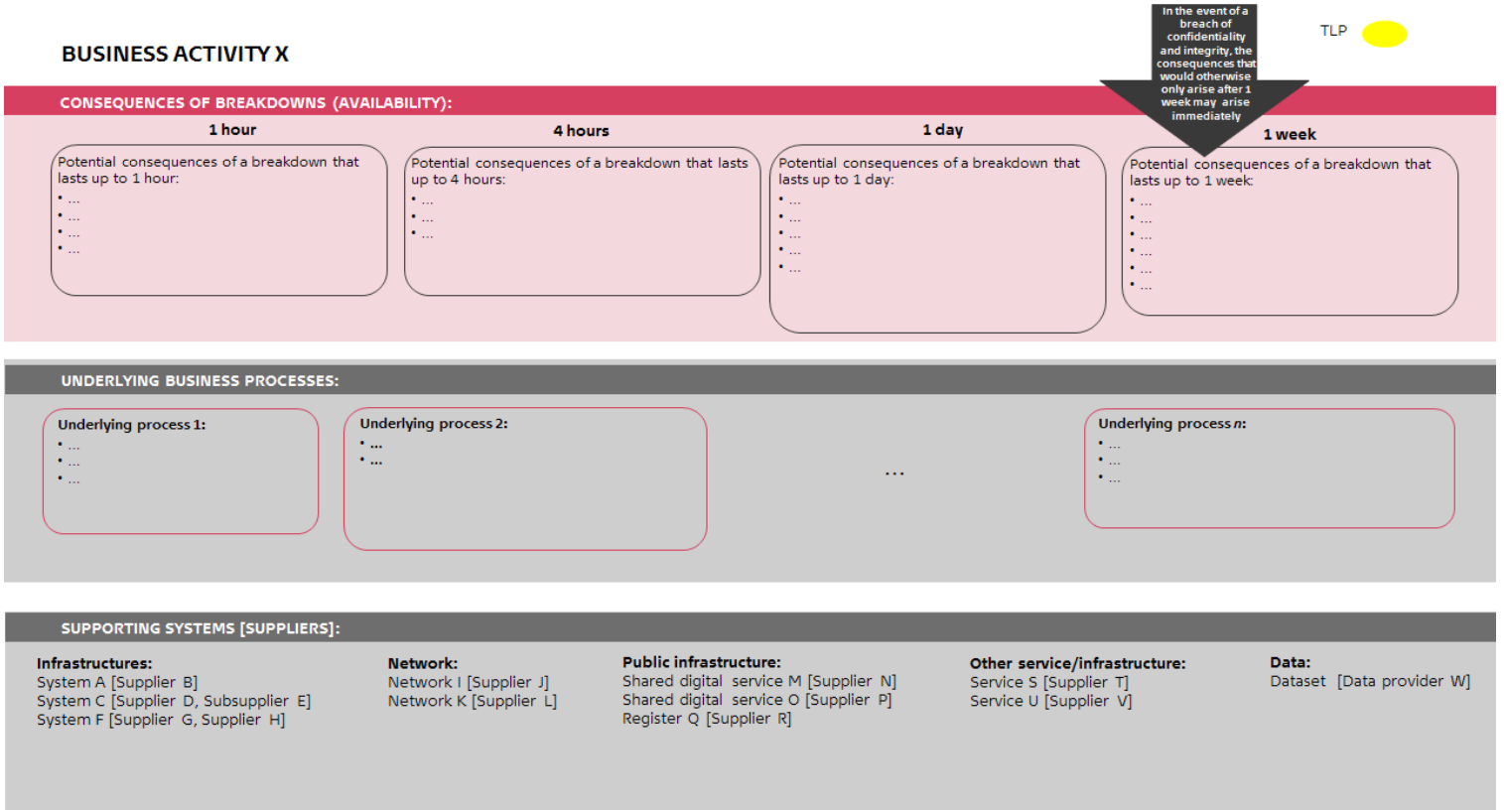
It may be necessary to deal with a risk at several levels. There is no actual risk owner of the risks dealt with by FSOR. Instead, a coordinator is appointed from among FSOR's members for each of the initiatives that FSOR decides to launch in connection with the risk analysis.

FSOR's secretariat has overall responsibility for:
- convening the working group to update the risk analysis
- preparing material and reporting it to FSOR
- coordinating the implementation of tasks related to mitigating actions
- coordinating the reporting on the status of mitigating actions.

FSOR's members are responsible for:
- discussing risks and approving risks ranked in the risk matrix
- deciding which mitigating actions to take
- discussing the status of mitigating actions, deciding on new tasks and making adjustments (if any)
- participating in or heading relevant sub-groups and task forces set up to implement mitigating actions
- incorporating risks into their own risk management.

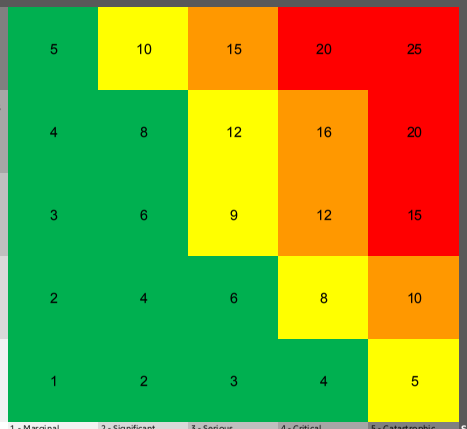
FSOR-RISK maintains and updates the risk analysis. Tasks related to maintenance of the risk analysis foundation are distributed among the members of the working group.

# Appendix 1: Business Impact Analysis, BIA



# Appendix 2: Risk matrix

| Threat level after mitigating actions | Knowledge sharing and cooperation | Sharing of information about threats etc. | Traceability | Supplier complexity | Maturity and control environment awareness of relevant players and/or suppliers | Lack of understanding of risk | Complexity of IT architecture | Overall |
|---|---|---|---|---|---|---|---|---|
| Very high | Players (and suppliers) work separately on operational resilience and do not share knowledge. | Players (and suppliers) withhold information about potential threats, threat groups, cyber attacks etc. | Almost impossible to detect. No evidence. | Extreme complexity and/or no governance. | No awareness of risks and controls. Incompetent and inadequate resources. Tests are seldom performed, if at all, and they are poorly documented. | There is a great deal of uncertainty about the level of risk. It is not possible to gain insight into the actual risk. | Extremely complex and unstable operations. | Event occurs once a year. |
| High | Some players (and suppliers) share knowledge in selected/random areas. | Players (and suppliers) seldom share information about threats, threat groups, cyber attacks etc. | Demonstrable, possible to collect evidence and documentation. | Very complex supplier picture. and weak governance | Poor awareness of risks and controls. Lack of competence and resources are often inadequate. Random testing and documentation. | There is a great deal of uncertainty about the level of risk. It is difficult to gain insight into the actual risk. | Very complex and varying operational stability. | Event occurs once within 1-3 years. |
| Medium | Some players (and suppliers) share knowledge and work together on solutions in selected areas. | Players (and suppliers) sometimes share information about threats, threat groups, cyber attacks etc. The sharing of information is not structured and may be somewhat random. | Can be demonstrated, destruction of evidence and documentation requires a lot of effort and is only possible for a short period of time. | Complex supplier picture and less robust governance. | Documents and uses standards. Limited awareness of risks and controls. Partially competent and not always adequate resources. Adequate systematic tests exist but are not carried out and they are partially documented. | The level of risk is unclear, but there are several opportunities for gaining insight into the scope of the risk. | Normal complexity and fairly stable operations. | Event occurs less frequently than every 3 years. |
| Low | Most players (and suppliers) work together on common issues, coordinate actions and share best practice experience and knowledge. | Players (and suppliers) share all relevant information about potential threats and threat groups. Cyber attacks etc. | Easily demonstrable, not possible to hide evidence and documentation. | Normal supplier picture and reasonable level of governance. | Follows and documents recognised standards. Strong awareness of risks and controls. Competent and adequate resources. Systematic tests exist and are carried out and they are documented. | There is some uncertainty about the level of risk but good opportunities for increasing insight into the risk. | Less complexity and fairly stable operations. | Event occurs less frequently than every 5 years. |
| No threat assessment | Players (and suppliers) work together on relevant issues, coordinate actions and systematically share best practice experience and knowledge. The players actively consider in which areas it is relevant to cooperate. | Information about threats, threat groups, cyber attacks etc. is immediately shared with other players. Information sharing is systematic and organised. | Full traceability and documentation exist. | Simple supplier picture and strong governance. | Follows and documents recognised standards. Strong awareness of risks and controls. Competent and adequate resources. Systematic tests exist and are carried out and they are documented. Fixed improvement routines are followed. | The level of risk is quite clear, and there are good opportunities for gaining insight into it. | Low complexity and stable operations. | Event occurs less frequently than every 10 years. |




| 1 - Marginal | 2 - Significant | 3 - Serious | 4 - Critical | 5 - Catastrophic | Scale |
|---|---|---|---|---|---|
| Consequences are internal, and critical business activities are not impaired. | Slight delay in delivery or slightly impaired quality of business activities. | Significant delay in delivery or significantly impaired quality of deliverables from critical business activities. | Lacking deliverables related to critical business activities. | Missing or compromised deliverables related to critical business activities. | Impact on critical business activities |
| Some citizens/ businesses/investors are briefly affected. | Citizens/businesses/ investors are directly or indirectly affected through media. Problems are quickly resolved. | Several citizens/businesses/ investors are directly or indirectly affected through media. Problems are resolved within a reasonable timeframe. There may be political attention. | Many citizens/ businesses/investors are directly or indirectly affected through media. There may be political attention. | A critically large share of citizens/businesses/ investors are directly or indirectly affected through media. There is likely to be political attention. | Share affected |
| Trust in the critical business activities of the financial sector is maintained. | Trust in the critical business activities of the financial sector is largely unaffected. | Trust in the critical business activities of the financial sector briefly drops. | Trust in the critical business activities of the financial sector is affected for a short period of time. | Trust in the critical business activities of the financial sector is reduced both in the short and long term. | Impact on trust |
| Unauthorised access to insignificant data. | Unauthorised access to significant data. | Compromising of insignificant data. | Compromising of significant data. | Data is compromised, business processes are corrupted. | Compromising of data |

IMPACT

# Appendix 3: Contact details

| Organisation | Participant | Email | Telephone |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Appendix 4: Confidentiality rules

Rules on confidentiality and handling of material from FSOR Table 1

| Colour code | Description | Information sharing | Dispatch, storage and destruction |
|---|---|---|---|
| White (TLP:WHITE) | Material is assigned the colour code TLP:WHITE when the content is not of an internal nature for FSOR or its members and its entry into the public domain has no negative impact on FSOR or individual members. | TLP:WHITE information and documents may be circulated inside the member's organisation and to external stakeholders or business partners. | *Electronic dispatch*: No special dispatch requirements.<br><br>*Storage*: No special treatment or physical storage requirements.<br><br>*Destruction*: In an ordinary office bin or rubbish bag. |
| Green (TLP:GREEN) | Material is assigned the colour code TLP:GREEN when the content has moderate negative consequences for FSOR or individual members in the event of a leak.<br><br>Confidentiality classification 'Internal disclosure'. | TLP:GREEN information and documents may be shared inside the member's organisation with a work-relevant circle of people. | *Electronic dispatch*: Sharing primarily via Danmarks Nationalbank's extranet.<br><br>*Storage*: Documents are assigned a classification and access restrictions in accordance with the colour code when filed electronically. Physical copies are stored in a cupboard or drawer.<br><br>*Destruction*: In an ordinary office bin or rubbish bag. |
| Amber (TLP:AMBER) | Material is assigned the colour code TLP:AMBER when the content is of a sensitive nature and may have medium or serious negative consequences for FSOR or individual members in the event of a leak.<br><br>Confidentiality classification 'Limited disclosure'. | TLP:AMBER information and documents may only be shared on a need-to-know basis inside the member's organisation. | *Electronic dispatch*: Sharing only via Danmarks Nationalbank's extranet.<br><br>*Storage*: Documents are assigned a classification and access restrictions in accordance with the colour code when filed electronically. Physical copies are stored in a cupboard or drawer.<br><br>*Destruction*: In an ordinary office bin or rubbish bag. |
| Red (TLP:RED) | Material is assigned the colour code TLP:RED when the content is of a particularly sensitive nature and may have very serious negative consequences for FSOR or individual members in the event of a leak.<br><br>Confidentiality classification 'Confidential' or 'Strictly confidential'. | TLP:RED information and documents may not be shared with parties outside the group of people, for example from a meeting or interview, with which they are originally shared. | *Electronic dispatch*: Sharing only via Danmarks Nationalbank's extranet.<br><br>*Storage*: Documents are assigned a classification and access restrictions in accordance with the colour code when filed electronically. Physical copies are stored in a cupboard or drawer.<br><br>*Destruction*: Using a shredder or a special closed container intended for confidential documents. |