

Risk and data handling policy

Attitude to risk¹ and data handling

1. The Competition Commission (CC) conducts in-depth inquiries into mergers, markets and the regulation of the major regulated industries. The CC's aims and objectives are set out in more detail in its corporate plan, published on the CC website.
2. As a public body the CC is committed to being as open and transparent as possible and publishes as much as it can within the constraints imposed by the nature of the CC's work and its legislative framework. The CC has continued to introduce a series of changes to embody greater transparency in its operations, following a major consultation with interested parties and the public generally. These changes are embodied in our publication scheme, on the CC website.
3. Measures to increase transparency must also be seen in the context of the overriding need to preserve the confidentiality of commercially-sensitive information, or personal data, in the conduct of our inquiries and the need to avoid prejudicing the discharge of our functions. Furthermore, information about businesses obtained during an inquiry is protected by the criminal law.
4. The nature and impact of the CC's work leads the CC to be necessarily risk averse in its policies and procedures. The CC actively identifies, assesses and manages key risks as set out in the CC risk registers,² and this policy defines the importance of managing these risks as a means of enabling the effective use of data for the public benefit.

Corporate governance of risk

5. The Operations Board (OB) includes the Senior Information Risk Owner (SIRO) and senior representatives from across the CC, and meets at least three times each year during the normal course of its meetings specifically to discuss risk and information risk management. In terms of risk management it has the following overarching objectives and is assisted by the Planning department:³
 - To ensure that the operational and other risks faced by the CC in carrying out its functions have been properly identified and are evaluated regularly and monitored by management at appropriate levels.
 - To ensure that appropriate and effective procedures have been established and are maintained by management to address the identified risks.
6. The OB seeks to ensure that risk management is embedded in the organization as a whole. It seeks to ensure that the existing management structures enable risk to be managed appropriately.

¹The term 'risk' in this policy includes all types of risk including information risk, such as personal data.

²Available in on the Planning page on the intranet: http://landscape/working/corporateservices/planning/risk_management.htm.

³As defined in the [Terms of Reference](#).

Risk and risk management process

7. Those with responsibility for managing risks at the CC are:
- **Council** to see a few 'high' level risks every meeting (every 2 months). Council takes decisions at a strategic level and feedbacks to the OB. It will also review the whole risk register once a year.
 - **Audit Committee** reviews the risk management process and ensures the mechanism is appropriate. Audit Committee reviews all committee risk registers at least once a year and highlights any concerns to Council or OB. Audit Committee also has responsibility for IT and data security.
 - The **OB** monitors the work stream 1 and 2 risk register, reviews and debates any changes, including when new risks are identified, or changes are made to the status of the risk. The OB approves the grade the risk is at. The OB reviews all other committees' risk registers at least once a year, and highlights strategic risks to Council. The OB owns the risk policy and its implementation. Any deviations from this policy should be approved by the OB.
 - **Remedies Standing Group, Practices & Procedures Group, Analysis Group and the Corporate Service Management Team** should review, monitor and update their work stream risk registers on a regular basis, and highlight any strategic risks to Council.
 - **Internal Audit**, RSM Bentley Jennison, assesses and reviews the CC's risk management processes and monitors the CC's compliance with the policy and its effectiveness.
 - **The Department for Business, Enterprise and Regulatory Reform (BERR)**, the CC's sponsor department is alerted to all high-level risks and the progress of those risks at a quarterly meeting by the CC's Accounting Officer.
 - **Accounting Officer** is the Chief Executive and will have to report explicitly on information risk as part of the Statement on Internal Control. The Accounting Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.
 - **The SIRO** is the Director of Corporate Services and is responsible for developing and implementing this policy and for reviewing it regularly to ensure that it remains appropriate to the business objectives and the risk environment. The SIRO acts as an advocate for information risk on the Council and in internal discussions, and provides written advice to the Accounting Officer on the content of the Statement on Internal Control relating to Information risk.
 - **Information Asset Owners (IAOs)** are the four Heads of Profession, all the Inquiry Directors and all Corporate Service managers. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. They also need to update the risk registers for work streams 1, 2, 3, 4 and 5.

- **HR** will implement a plan to introduce the necessary changes in culture at the CC to ensure that data is valued, protected and used for the public good. HR will also provide training to all those involved.
 - **IT** is responsible for having a policy of reporting, managing and recovering from information risk incidents, including losses of protected personal data and Information and Communications Technology (ICT) security incidents, defining responsibilities, and making sure staff are aware of the policy (which can be found at <http://landscape/working/corporateservices/security/resources.htm>). IT will report security incidents to HMG's incident management scheme (GovCERTUK for network security incidents and CINRAS for incidents involving cryptographic items). Significant actual or potential losses of personal data will be shared with the Information Commissioner and the Cabinet Office. IT will also ensure that the CC has the minimum requirements for continuing system accreditation and events that must trigger re-accreditation.
 - **Planning** is responsible for facilitating the risk process, and alerting Council, Audit Committee, the OB, and Internal Audit of any changes.
 - **Data users** should alert their line manager if they are aware of any risks facing the CC, alternatively they should contact the Planning team. All staff and members should report any data handling incidents to the IT helpdesk and then logged by IT. All staff, members and contractors with access to or involved in handling individual records containing protected personal data are referred to as 'users'. A list of all users has been identified and recorded by HR. Failure of users to apply CC handling of sensitive data procedure is a serious matter, and in some situations may amount to gross misconduct. HR will provide induction and annual training to help them to understand the importance of their role.
8. The Audit Committee reviews the following documents annually: all committees' updated risk registers; the risk policy document; and an annual report from the OB chairman. The Business Continuity Group discusses operational security issues and reports to the OB.

Risk awareness

9. The risk policy document and a non-confidential version of the CC risk registers are published on the CC intranet, as well as a point of contact for staff who identify risks or who want to talk about risk management at the CC. The Planning department may provide advice and support to staff with responsibilities for risk management. In addition, all staff are expected to engage in risk management as appropriate, through their day-to-day work, through the monitoring committees, or through participation in staff team discussions.
10. HR will ensure that all data users will successfully undergo information risk awareness training on appointment and at least annually. In addition, all IAOs must pass information management training on appointment and at least annually, and the Accounting Officer, SIRO and members of the Audit Committee will pass strategic information risk management training at least annually. Failure to apply the organization's policies and practices is a serious matter and may amount to gross misconduct. Risk management is also incorporated into the management and development programme. HR will also ensure that all those with responsibility for risk management, such as the IAOs, will have their responsibilities clearly identified in their role profile and appraisal objectives.

Glossary of terms

Delivery partners

All contracts with the CC include secrecy, confidentiality and data protection clauses. There is also a requirement for all members of a delivery partner's staff, who will be involved in any aspect of the service delivery, to sign a witnessed Confidentiality Undertaking.

Incidents

Incidents can cover a wide range of events and may be categorized as below, where examples of each type of incident are given:

- Physical: the loss of hard copy classified material; the breaching of access controls; the loss/theft of sensitive data or equipment; unauthorized access to, tampering with the use of ICT systems, equipment or accounts; unauthorized acquisition of privileges; unauthorized access to, use or disclosure of sensitive information; unauthorized changes to system hardware, firmware or software.
- Procedural: improper use of an ICT system, access or privileges (eg inappropriate use of email or accessing inappropriate websites); improper handling, distribution, accounting, storage and destruction of cryptographic items or sensitive information.
- Personnel: any unauthorized event involving insiders or ex-insiders (including members of staff, contractors, visitors, support staff or former members of any of these groups).
- Electronic: malware attacks (viruses, worms, Trojan horses); unauthorized disruption of service (denial or service and distributed denial of service attacks), receipt of spam, phishing attacks, etc.
- Operational: system failures, crashes, environmental failures and operator errors may have security implications and should be treated as incidents, in addition to their potential implications for business continuity. Some IT security incidents have been detected as a result of poorer system performance being detected.

Information risk

Information **risk** can take many forms—from data sets of confidential personal information through to records of sensitive meetings, personal records, policy recommendations, correspondence, case files and historical records. Information can be in many formats, from databases through to emails, paper and video. It is important to manage information **risks** as a means of enabling the effective use of data for the public benefit.

IT systems

Information technology systems: these are not the same as information. IT systems are platforms on which information is often exchanged and managed. Therefore, **information risks** are not necessarily the same as IT security **risks** (although

managing IT security is usually a critical component of any strategy to manage information **risks**).

Risk

A risk is an uncertainty of outcome—usually something which prevents the organization from meeting its objectives in some way. Good risk management allows stakeholders to have increased confidence in the organization's corporate governance and ability to deliver.

How to calculate risks

Risks are measured by multiplying the impact the risk would have on the organization, if the risk were to happen, by the probability of it happening. This score is then multiplied by '1' if the control is considered 'satisfactory', '2' if 'improvement is required' and '3' if the control is considered 'unsatisfactory'.

Table 1 shows the initial risk rating that is given when a risk is identified and scored, by inputting an impact score and a probability score into the risk register under the columns 'impact' and 'probability'. The risk register automatically calculates the 'rating' column, ie risk x probability = rating.

Tables 3 to 5 show how the risks change after considering the current controls that are in place to deal with the risk. Depending on whether the controls are considered 'satisfactory', 'improvement required' or 'unsatisfactory', a new overall rating will be given. This is represented in the risk register when inputting the 'effectiveness of mitigation' column with either 1 satisfactory, 2 improvements required, or 3 unsatisfactory. The new score is represented in the 'overall rating' column in the risk register, ie (risk x probability) x effectiveness = overall rating.

TABLE 1 Impact x probability = Risk rating

High score is red. Medium score is yellow. Low score is green.

Probability

5 Highly likely	5	10	15	20	25
4 Very likely	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Small	2	4	6	8	10
1 Unlikely	1	2	3	4	5
	1 No impact	2 Small	3 Moderate	4 Significant	5 Fundamental

Impact

(Impact x probability) x effectiveness = overall rating

TABLE 2 Effectiveness = Satisfactory (1)

Probability

5 Highly likely	5	10	15	20	25
4 Very likely	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Small	2	4	6	8	10
1 Unlikely	1	2	3	4	5
	1 No impact	2 Small	3 Moderate	4 Significant	5 Fundamental

Impact

TABLE 3 Effectiveness = improvement required (2)

Probability

5 Highly likely	10	20	30	40	50
4 Very likely	8	16	24	32	40
3 Moderate	6	12	18	24	30
2 Small	4	8	12	16	20
1 Unlikely	2	4	6	8	10
	1 No impact	2 Small	3 Moderate	4 Significant	5 Fundamental Impact

TABLE 4 Effectiveness = unsatisfactory (3)

Probability

5 Highly likely	15	30	45	60 Exposed	75 Exposed
4 Very likely	12	24	36	48 Exposed	60 Exposed
3 Moderate	9	18	27	36 Exposed	45 Exposed
2 Small	6	12	18	24	30
1 Unlikely	3	6	9	12	15
	1 No impact	2 Small	3 Moderate	4 Significant	5 Fundamental

Guidelines to choosing an impact and probability score

The tables below are provided to clarify and define how to choose the risk ‘impact’ and ‘probability’ scores. These guidelines should be used to ensure consistency when scoring a risk. They are examples of issues that arise at the CC and should give an indication of what the organization considers more important compared with something else. Some boxes give more than one example.

TABLE 5 **Impact guidelines**

<i>Category</i>	<i>Finance A loss of:</i>	<i>Media</i>	<i>Reputation CAT</i>	<i>Staff</i>	<i>Workload*</i>	<i>Operational Equipment</i>	<i>Timetable †</i>
No impact 1	< £5k	1 inquiry criticized in the media	Minor recommendation made by the CAT	Staff turnover is less than 20% per year	At any one time we have 9, 10 or 11 inquiries. Consistently over the year an average of 10 inquiries	5% of non-critical IT equipment fails for a few hours during office hours	The admin timetable is delayed by 1 week per inquiry. Overall there is one extension.
Small 2	£5k–£50k	1–3 inquiries criticized in the media	Some recommendations made by CAT	Staff turnover is 25% per year	At any one time 8 or 12 inquiries. Consistently over the year an average 9 or 11 inquiries	5–20% of non-critical IT equipment fails for up to half a day, during office hours	The admin timetable is delayed by 2–3 weeks per inquiry. Overall there are 2 extensions
Moderate 3	£50k–£500k	3–5 inquiries criticized in the media	Lose appeal on a technicality	Staff turnover is 30% per year	At any one time 13–14 or 6–7 inquiries. Consistently over the year 12–13 or 7–8 inquiries	Over 20% of IT equipment fails for more than half a day during offices hours. Critical systems fail for a few hours.	An extension is required on an inquiry. An extension is required on more than 3 inquiries in one year
Significant 4	£500k–£2m	More than 5 inquiries criticized in the media or a parliamentary report	Lose appeal and criticized publicly	Many staff leave at same time	At any one time 15–16 or 4–5 inquiries. Consistently over the year 14–15 or 5–6 inquiries	Serious equipment failure, many staff experience IT problems for more than 1 day during office hours	4+ inquiries require extension within the year
Fundamental 5	> £2m	Full public enquiry or severe criticism by the Government or NAO	Lose appeal and severely criticised	The CC ceases to operate	At any one time more than 16 or fewer than 4 inquiries. Consistently over the year over 15 or fewer than 5 inquiries	The CC ceases to operate	The statutory deadline is breached

*These are two options, one considers how many inquiries we might have at any point in time, and the next considers how many inquiries on average over the year.

†The first points relates to what impacts the individual inquiry, the second point relates to what impacts the organization.

Probability guidelines

Unlikely 1	May occur exceptionally	Can't believe it will happen
Small 2	Could occur	Don't expect, but possible
Moderate 3	Might occur	May occur occasionally
Very likely 4	Will probably occur	Will occur, not persistent occurrence
Highly likely 5	Expected to occur	Undoubted occurrence possibly frequent