DATA PROCESSING CONTRACTS

Owning Department: Information Management

Department SPOC: Compliance and Data Protection Officer

Risk Rating: Medium Low

Legal Sign Off: 21/06/2022

JNCC: June 2021

Published Date: 12/01/2024 (v1.1)

Review Date: 11/02/2027

Index

Legal Basis

Legislation specific to the subject of this policy document:

- Statutory Code of Practice for the Management of Police Information issued under The Police Act 1996
- Data Protection Act 2018 (Chapter 4, section 55-71)
- General Data Protection Regulation (GDPR) Article 28(3)
- European Union (withdrawal) Act 2018 (Section 3)

Other relevant legislation which you must check this document against (required by law) *(Delete as applicable for each policy)*

- Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
- Equality Act 2010
- Crime and Disorder Act 1998
- Health and Safety at Work etc. Act 1974 and associated Regulations
- Freedom Of Information Act 2000
- The Civil Contingencies Act 2004

Other documentation which you must check this document against:

- College of Policing – Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour
- College of Policing – Authorised Professional Practice – Information Management, Data Protection
- NPCC Community Security Policy
- ACPO National Vetting Policy

1. Introduction

1.1 Information is a valuable resource that requires adequate protection to be provided by the Controller and any Processors. All processing by both Controller and Processor is to be compliant with the Data Protection legislation (UK GDPR[1] and the Data Protection Act 2018).

1.2 This policy is supported by interrelated policies and procedures that further detail how matters connected with the management of information takes place, such as provision of access to information and security of information.

1.3 The Data Protection legislation places certain obligations on police forces when they use third party businesses/organisations to process personal data and special data on the Controller's behalf, which are known under the act as 'Processors'.

1.4 A 'Processor' is responsible for processing personal data on behalf of a controller.

1.5 Prior to a Processor processing personal data on behalf of a controller, the Controller must ensure that adequate arrangements are in place to protect the data from misuse, accidental loss or damage.

1.6 The purpose of the processing, the Processor's engagement in providing the information as well as any safeguarding measures which are in place to protect the information, are documented in a Data Processing Contract which is signed by both Controller and Processor.

2. Statement of Policy

2.1 This policy has been formally agreed via the approved policy development/review process. It will be maintained by the Information Management Department in conjunction with the Central Policy Unit.

2.2 The policy is intended to promote equality, eliminate unlawful discrimination and actively promote good relations regardless of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, economic or family status.

2.3 Managers have a responsibility to ensure this policy is applied fairly, and unless otherwise stated, all policies and procedures are non-contractual.

[1] UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4))

3. Applicability

3.1 This policy applies to, fixed term and permanent staff, seconded staff, temporary and agency staff, contractors, self-employed consultants and associates etc.

3.2 There are no known exemptions.

4. Data Processing

4.1 There are many reasons and areas with the police where the use of a Processor is required, some examples of which are:

- Payroll suppliers;
- Hardware/software/suppliers & maintenance companies;
- Confidential waste disposal contractors;
- University research for the police;
- Other persons working with the police, including volunteers where necessary.

4.2 A Data Processing Contract is required to oblige with the Data Protection legislation. A Data Processing Contract will specify exactly what the Processor is and is not permitted to do with the police information. For example, a Processor is required to maintain records of personal data and processing activities. The Processor will have legal liability if responsible for a breach. At the same time, the Controller is responsible for ensuring the Processor complies with the Data Protection legislation.

4.3 A Data Processing Contract will detail the following areas:

- Purpose, use and disclosure;
- Security;
- Staff training;
- Vetting of staff;
- Confidentiality agreements;
- Weeding/Retention/Disposal;
- Subject access and freedom of information provisions;
- Audit/inspection of the processor by the Constabularies;
- Indemnity.

5. Data Processing Contract Process

5.1 Where it is identified that a Processor is going to be used or required, the Data Processing Contracts Central Record should be checked to see if a Data Processing Contract, with the relevant business/organisation and for

the same purpose/processing, already exists. All current Constabularies Data Processing Contract and known National Data Processing Agreements can be found on the W drive at:

W:\Collaboration\Information Management\Information Compliance\Data Protection\Org\Reports and Publications\DPC Central Record

5.2 If a Data Processing Contract exists that appears to fully meet the requirements of the new processing, contact either the Designated Officer for the Constabularies listed on the agreement who will advise whether the existing contract is identical and adequate. If any uncertainty exists, contact the Information Sharing Officer for advice on compliance@suffolk.police.uk

5.3 If it is adequate, no further action beyond advising the Processor is necessary.

5.4 Where 7 Force Procurement is involved with any financial implications, the 7 Force Procurement Contracts Officer will have responsibility for the production of any agreements/contracts, the Information Sharing Officer will be consulted and will provide advice and guidance on the terms and conditions to be included to ensure compliance with the Data Protection legislation requirements.

5.5 If there is a procurement contract, there will be no need for a standalone Data Processing Contract and will be routed through the 7 Force sign off under Contract Standing Orders.

5.6 If there is no procurement or financial implications and there is no existing Data Processing Contract or the existing contract does not fulfil the requirements, it will be necessary to draft a new Data Processing Contract. Contact should be made to the Information Sharing Officers.

5.7 The Information Sharing Officer will liaise with Information Security and other relevant departments and perform a risk assessment to ensure the proposed Processor is able to satisfy the technical and organisational standards required by the Constabularies. This will include an assessment of the security arrangements of the data Processor, how the information will be used, vetting of staff etc.

5.8 With regards to security, all Chief Constables are committed to compliance with the NPCC Community Security Policy, and they and the Processor are expected to ensure that all data and information is handled in line with the HMG Security Policy Framework, specifically meeting the Mandatory Requirement:

- Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process to prevent unauthorised access, use, disclosure, modification, disposal, or

impairment, whether intentional or unintentional, through appropriate technical and organisational security measures.

5.9 See Appendix A the Constabularies' Information Security Policy Statement, which details the security requirements the forces expect the processing business/organisation to have in place to ensure the forces information is kept secure when they are processing it, and it is included in all Data Processing Contracts. If you have any queries or need advice regarding security please contact Information Security on the below e-mail address:

- InformationSecurity@suffolk.police.uk

5.10 Where necessary, the Project Officer will complete a Data Protection Impact Assessment (DPIA) to identify and reduce the privacy risks of a project or system. The Norfolk and Suffolk Constabularies' Compliance and Data Protection Officer can provide advice: compliance@suffolk.police.uk

Guidance is also available in the following document:

- Data Protection Impact Assessment Policy

5.11 When all of the above matters have been satisfactorily addressed and the Information Sharing Officer, Information Security and other relevant departments agree the proposed Processor is able to satisfy the technical and organisational standards required by the Constabularies, the Information Sharing Officer will draft the Data Processing Contract.

5.12 The process for new Data Processing Contract will be followed. The Information Sharing Officer will liaise with key stakeholders in the Data Processing Contract process until each are satisfied.

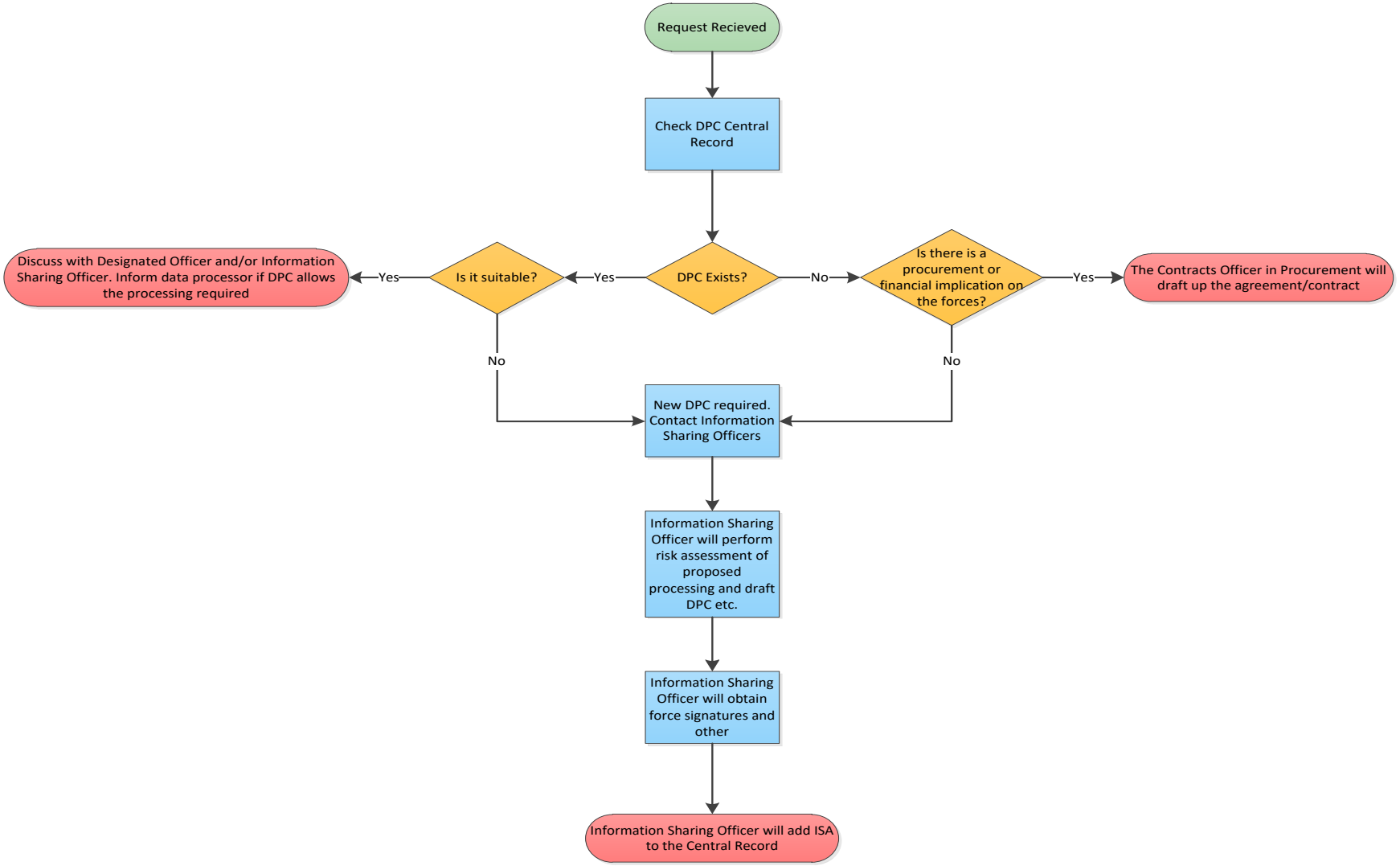
- Information Asset Owner(s)
- Designated Officer
- Compliance and Data Protection Officer
- Information and Cyber Security Officer
- Vetting Manager
- Processor(s)

5.13 When the final version of the Data Processing Contract has been agreed by the Compliance and Data Protection Officer and signed off by the Deputy Chief Constables, the Information Sharing Officer will acquire the Processor's signatures, inform the relevant business area and record the agreement on the central register.

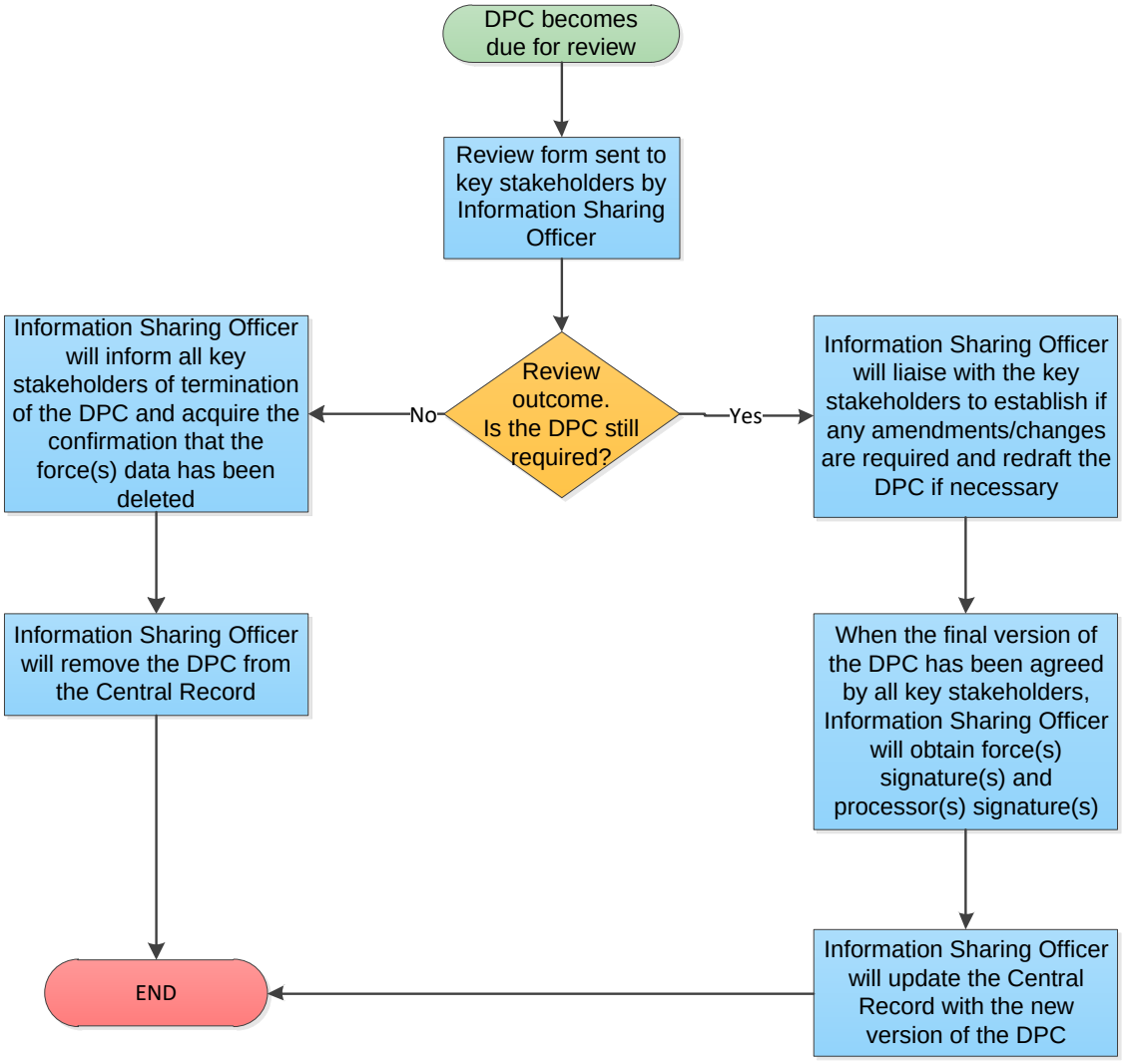
5.14 The Information Sharing Officer will initiate a review of the Data Processing Contract on an annual basis, and will liaise with the key stakeholders to establish if the Data Processing Contract is still required and if it is, any changes to the information being processed, the processes, the Designated Officers etc.

5.15 The process to review existing Data Processing Contracts will be followed in the same order as for new Data Processing Contracts (as per paragraphs 5.11 – 5.14).

6. Data Processing Contract Flowchart



7. Review of Data Processing Contract Flowchart



Appendix A: Information Security Policy Statement

All Chief Constables are committed to compliance with the Community Security Policy, and they and Partner Organisations are expected to ensure that all data and information is handled in line with the HMG Security Policy Framework, specifically meeting the following Mandatory Requirement:

'Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process (including electronic and paper formats and online services) to prevent unauthorised access, disclosure or loss. The policies and procedures must be regularly reviewed to ensure currency.'

Scope

These Information Security Requirements and Objectives apply to the following:

- Roles & Responsibilities

  All persons or parties conducting work for either Signatory regardless of any form of employment, including contractors providing services, agency workers and trainees on vocational or work experience.

- Data & Information
  - Whether stored, copied, duplicated or transmitted, all 'soft' (electronic, digital and virtual) data, information and communications on servers, networks, connectivity, ICT kit such as PCs, workstations, laptops, and authorised multimedia devices including USBs, mobile phones, tapes and CDs.
  - Also 'hard' information printed or written on paper or other medium such as whiteboards and flipcharts, and transmitted by any method whatsoever, such as fax or scanner.
  - Additional safeguards should be considered, specified and documented according to the sensitivity and classification of the data, information, and/or circumstances of the Agreement, for example observing operational security, such as precautions against eavesdropping.

- Data: The Data Protection Act & Information Commissioner's Office
  - Where Signatories process personal data defined by the Act, they agree to apply security measures, commensurate with the principles of the General Data Protection Regulation 2016/679 and the Data Protection Act 2018, and in particular by applying that personal data shall be: "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')
  - These Information Security Requirements and Objectives should evidence this principle.

Information Security Requirements & Objectives

To that end, Signatories to this agreement should ensure, document and be able to evidence, that they have in place common technical and organisational security arrangements, evidencing the following appropriate, proportionate and reasonable Information Security Requirements and Objectives:

- Information Security risk assessments to establish, evaluate and accept risks, and put in place appropriate controls to manage them.
- Information Security Policies, Guidelines, Processes, Controls and Practices in place to protect, and ensure the confidentiality, integrity and availability of data and information and systems under their control.
- An Information Security Review process at planned intervals, so that should significant changes occur this will ensure their continued suitability, adequacy, and effectiveness; i.e. for technological, legal, contractual and regulatory requirements and organisational changes.

Specifically, they should address the Information Security Requirements and Objectives below.

- **Information Security Policy** - A documented Information Security Policy should provide governance, management direction and support for information security according to relevant business and organisational requirements, contractual obligations, laws, statutes, regulations and best practices.
- **Organisation of Information Security** - Internal Organisation & External Parties to manage information security within the organisation, and maintain the security of information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
- **Asset Management** - Responsibility for Assets & Information Classification to achieve and maintain appropriate protection of organisational assets, and ensure information receives an appropriate level of protection.
- **Human Resources Security** - Prior to, During & After Employment. Training & Awareness to ensure that employees, contractors, third parties, and other users understand their responsibilities, and are suitable for the roles they are considered; reducing the risk of theft, fraud or misuse of facilities; and are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support security policy in their normal work, reducing the risk of error; and to ensure that all users exit or change employment in an orderly manner. Information security programmes should be available and imparted to all relevant users.
- **Vetting** - As an organisation Suffolk and Norfolk Constabularies have given an undertaking as part of their PSN(P) accreditation that all Police Staff and others who have access to Police data will be vetted in line with ACPO vetting policy, which defines non-police staff as requiring vetting to a minimum of NPPV2.
- **Physical & Environmental Security** - Secure areas & Equipment Security to prevent unauthorised physical access, damage and

interference to the organisations' premises and information; and prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.

- **Communications & Operations Management** - Operational Procedures, Responsibilities & Third Party Service Delivery Management to ensure the correct and secure operation of information processing facilities; and implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements;
- **System Planning** - Acceptance & Protection against malicious & mobile code to minimise the risk of systems failures; and protect the integrity of software and information;
- **Back-up & Network Security Management -** To maintain the integrity and availability of information and information processing facilities, and ensure the protection of information in networks and the protection of the supporting infrastructure.
- **Media Handling** - Exchange of Information & Monitoring to prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities; maintain the security of information and software exchange internally and with any external entity; and detect unauthorised information processing activities.
- **Electronic Commerce Services** - To ensure their security, and secure use.
- **Access Control**
    - Business Requirement for Access Control & User Access Management to control access to information, ensuring authorised user access, preventing unauthorised access to information systems.
    - User Responsibilities & Network Access Control to prevent unauthorised access, compromise, theft of information and information processing facilities; and access to networked services.
    - It is imperative that user accounts are unique to enable the tracking of specific activity to named individuals.
    - User activity must be correlated to a user via the use of a unique identifier. Each user connected to the network shall be assigned a unique user ID in order that it can be used for authentication of that individual user.
    - The access control will be covered by the Information Security policies and therefore will be sufficient to manage the risk to the organisation.
    - Operating System, Access, Application, & Information Access Control to prevent unauthorised access to operating systems; and information held in application systems.

  - Mobile Computing & Teleworking to ensure information security when using mobile computing and teleworking facilities.

- **Information Systems Acquisition, Development & Maintenance**
  - Security Requirements of Information Systems & Correct Processing in Applications to ensure that security is an integral part of information systems, and prevent errors, loss, unauthorised modification or misuse of information in applications.
  - Cryptographic Controls & Security of System Files to protect the confidentiality, authenticity or integrity of information by cryptographic means, and ensure the security of system files.
  - Security in Development, Support Processes & Technical Vulnerability Management to maintain the security of application system software and information, and reduce risks resulting from exploitation of published technical vulnerabilities.
- **Information Security Incident & Breach Management -** To report information security threats, events and weaknesses ensuring those associated with information systems are communicated to allow timely corrective action; and manage incidents and improvements, ensuring a consistent and effective approach is applied to information security incidents.
- **Business Continuity Management** - To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
- **Compliance with Legal Requirements** - To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements, and that they are met wherever applicable; and to ensure compliance of systems with organisational security policies and standards, and to maximize the effectiveness of and to minimise interference to/from the information systems audit process.