GOV.UK

1. Home (https://www.gov.uk/)
2. Childcare and parenting (https://www.gov.uk/browse/childcare-parenting)
3. Schools and education (https://www.gov.uk/browse/childcare-parenting/schools-education)

The national curriculum

Contents

Key stage 1 and 2

Compulsory national curriculum subjects at primary school are:

- English
- maths
- science
- design and technology
- history
- geography
- art and design
- music
- physical education (PE), including swimming
- computing
- ancient and modern foreign languages (at key stage 2)

Schools must provide religious education (RE) (https://www.gov.uk/national-curriculum/other-compulsory-subjects) but parents can ask for their children to be taken out of the whole lesson or part of it.

Schools often also teach:

- personal, social and health education (PSHE)
- citizenship
- modern foreign languages (at key stage 1)

Tests and assessments

Year 1 phonics screening check

The check will take place in June when your child will read 40 words out loud to a teacher. You'll find out how your child did, and their teacher will assess whether he or she needs extra help with reading. If your child doesn't do well enough in the check they'll have to do it again in Year 2.

Key stage 1

Key stage 1 tests cover:

- English reading
- English grammar, punctuation and spelling
- maths

Your child will take the tests in May. You can ask the school for the test results.

You'll be sent the results of your child's teacher assessments automatically.

Key stage 2

Your child will take national tests in May when they reach the end of key stage 2. These test your child's skills in:

- English reading
- English grammar, punctuation and spelling
- maths

The tests last less than 4 hours. You'll get the results in July.

The school will send you the results of your child's tests and teacher assessments.

- ← Previous : Overview (https://www.gov.uk/national-curriculum)
- Next → : Key stage 3 and 4 (https://www.gov.uk/national-curriculum/key-stage-3-and-4)

Print entire guide (https://www.gov.uk/national-curriculum/print)

Related content

- Apply for a primary school place (https://www.gov.uk/apply-for-primary-school-place)
- Apply for a secondary school place (https://www.gov.uk/apply-for-secondary-school-place)
- Home education: get information from your council (https://www.gov.uk/home-schooling-information-council)
- School term and holiday dates (https://www.gov.uk/school-term-holiday-dates)
- Types of school (https://www.gov.uk/types-of-school)

Explore the topic

- Schools and education (https://www.gov.uk/browse/childcare-parenting/schools-education)
- Schools and curriculum (https://www.gov.uk/browse/education/school-life)
- Curriculum and qualifications (https://www.gov.uk/topic/schools-colleges-childrens-services/curriculum-qualifications)

GOV.UK

1. Home (https://www.gov.uk/)
2. Childcare and parenting (https://www.gov.uk/browse/childcare-parenting)
3. Schools and education (https://www.gov.uk/browse/childcare-parenting/schools-education)

The national curriculum

1. Overview

The 'basic' school curriculum includes the 'national curriculum' (https://www.gov.uk/government/collections/national-curriculum), as well as religious education and sex education (https://www.gov.uk/national-curriculum/other-compulsory-subjects).

The national curriculum is a set of subjects and standards used by primary and secondary schools (https://www.gov.uk/types-of-school) so children learn the same things. It covers what subjects are taught and the standards children should reach in each subject.

Other types of school (https://www.gov.uk/types-of-school) like academies (https://www.gov.uk/types-of-school/academies) and private schools (https://www.gov.uk/types-of-school/private-schools) don't have to follow the national curriculum. Academies must teach a broad and balanced curriculum including English, maths and science. They must also teach religious education.

Key stages

The national curriculum is organised into blocks of years called 'key stages' (KS). At the end of each key stage, the teacher will formally assess your child's performance.

Age	Year	Key stage	Assessment	
3 to 4		Early years (https://www.gov.uk/early-years-foundation-stage)		
4 to 5	Reception	Early years (https://www.gov.uk/early-years-foundation-stage)	Teacher assessments (there's also an optional assessment at the start of the year)	
5 to 6	Year 1	KS1	Phonics screening check	
6 to 7	Year 2	KS1	National tests and teacher assessments in English, maths and science	
7 to 8	Year 3	KS2		
8 to 9	Year 4	KS2		

Age	Year	Key stage	Assessment	
9 to 10	Year 5	KS2		
10 to 11	Year 6	KS2	National tests and teacher assessments in English and maths, and teacher assessments in science	
11 to 12	Year 7	KS3		
12 to 13	Year 8	KS3		
13 to 14	Year 9	KS3		
14 to 15	Year 10	KS4	Some children take GCSEs	
15 to 16	Year 11	KS4	Most children take GCSEs or other national qualifications	

Assessments

By the end of each summer term the school must write a report on your child's progress and talk it through with you.

2. Key stage 1 and 2

Compulsory national curriculum subjects at primary school are:

- English
- maths
- science
- design and technology
- history
- geography
- art and design
- music
- physical education (PE), including swimming
- computing
- ancient and modern foreign languages (at key stage 2)

Schools must provide religious education (RE) (https://www.gov.uk/national-curriculum/other-compulsory-subjects) but parents can ask for their children to be taken out of the whole lesson or part of it.

Schools often also teach:

- personal, social and health education (PSHE)
- citizenship
- modern foreign languages (at key stage 1)

Tests and assessments

Year 1 phonics screening check

The check will take place in June when your child will read 40 words out loud to a teacher. You'll find out how your child did, and their teacher will assess whether he or she needs extra help with reading. If your child doesn't do well enough in the check they'll have to do it again in Year 2.

Key stage 1

Key stage 1 tests cover:

- English reading
- English grammar, punctuation and spelling
- maths

Your child will take the tests in May. You can ask the school for the test results.

You'll be sent the results of your child's teacher assessments automatically.

Key stage 2

Your child will take national tests in May when they reach the end of key stage 2. These test your child's skills in:

- English reading
- English grammar, punctuation and spelling
- maths

The tests last less than 4 hours. You'll get the results in July.

The school will send you the results of your child's tests and teacher assessments.

3. Key stage 3 and 4

Key stage 3

Compulsory national curriculum subjects are:

- English
- maths
- science
- history
- geography

- modern foreign languages
- design and technology
- art and design
- music
- physical education
- citizenship
- computing

Schools must provide religious education (RE) and sex education (https://www.gov.uk/national-curriculum/other-compulsory-subjects) from key stage 3 but parents can ask for their children to be taken out of the whole lesson or part of it.

Key stage 4

During key stage 4 most pupils work towards national qualifications - usually GCSEs.

The compulsory national curriculum subjects are the 'core' and 'foundation' subjects.

Core subjects are:

- English
- maths
- science

Foundation subjects are:

- computing
- physical education
- citizenship

Schools must also offer at least one subject from each of these areas:

- arts
- design and technology
- humanities
- modern foreign languages

They must also provide religious education (RE) and sex education (https://www.gov.uk/national-curriculum/other-compulsory-subjects) at key stage 4.

English Baccalaureate (EBacc)

In performance tables, the EBacc shows how many students got a GCSE grade C or above in English, maths, 2 sciences, a language, and history or geography.

4. Other compulsory subjects

Children must also study:

- sex and relationships education (year 7 onwards)
- religious education (RE)

They may not have to take exams in these subjects.

Sex and relationship education

Sex and relationship education (SRE) is compulsory from age 11 onwards. It involves teaching children about reproduction, sexuality and sexual health. It doesn't promote early sexual activity or any particular sexual orientation.

Some parts of sex and relationship education are compulsory - these are part of the national curriculum for science. Parents can withdraw their children from all other parts of sex and relationship education if they want.

> All schools must have a written policy on sex education, which they must make available to parents for free.

Religious education

Schools have to teach RE but parents can withdraw their children for all or part of the lessons. Pupils can choose to withdraw themselves once they're 18.

Local councils are responsible for deciding the RE syllabus, but faith schools (https://www.gov.uk/types-of-school/faith-schools) and academies (https://www.gov.uk/types-of-school/academies) can set their own.

GOV.UK

1. Home (https://www.gov.uk/)
2. Education, training and skills (https://www.gov.uk/education)
3. School curriculum (https://www.gov.uk/education/school-curriculum)

Primary curriculum, key stage 2

Teaching and assessing the primary curriculum at key stage 2, primary school performance data, frameworks for teacher assessments.

Services

1. ISSP primary curriculum project application form (https://www.gov.uk/government/publications/issp-primary-curriculum-project-application-form)
   Application form for schools to propose new independent/state school partnerships (ISSPs) for specific subject teaching at primary level.

See all services (https://www.gov.uk/search/advanced?group=services&topic=%2Feducation%2Fprimary-curriculum-key-stage-2)

Guidance and regulation

1. National curriculum in England: primary curriculum (https://www.gov.uk/government/publications/national-curriculum-in-england-primary-curriculum)
   Statutory guidance
   6 May 2015
   Department for Education
2. Key stage 2: submitting teacher assessment data (https://www.gov.uk/government/publications/key-stage-2-submitting-teacher-assessment-data)
   Guidance
   18 May 2018
   Standards and Testing Agency
3. Key stage 2 tests: 2018 mathematics test materials (https://www.gov.uk/government/publications/key-stage-2-tests-2018-mathematics-test-materials)
   Guidance
   29 May 2018
   Standards and Testing Agency

1. **Key stage 1 and key stage 2 test dates (https://www.gov.uk/guidance/key-stage-1-and-key-stage-2-test-dates)**
   - Detailed guide
   - 16 October 2017
   - Standards and Testing Agency

2. **National curriculum in England: mathematics programmes of study (https://www.gov.uk/government/publications/national-curriculum-in-england-mathematics-programmes-of-study)**

- Statutory guidance
- 16 July 2014
- Department for Education

See all guidance and regulation (https://www.gov.uk/search/advanced?group=guidance_and_regulation&topic=%2Feducation%2Fprimary-curriculum-key-stage-2)

News and communications

STA assessment update: 3 July 2018 (https://www.gov.uk/government/publications/sta-assessment-update-3-july-2018)
3 July 2018

Standards and Testing Agency

Correspondence

1. **STA assessment update: 26 June 2018 (https://www.gov.uk/government/publications/sta-assessment-update-26-june-2018)**

    - 26 June 2018
    - Standards and Testing Agency
    - Correspondence

2. **STA assessment update: 19 June 2018 (https://www.gov.uk/government/publications/sta-assessment-update-19-june-2018)**

    - 19 June 2018
    - Standards and Testing Agency
    - Correspondence

3. **STA assessment update: 12 June 2018 (https://www.gov.uk/government/publications/sta-assessment-update-12-june-2018)**

    - 12 June 2018
    - Standards and Testing Agency
    - Correspondence

4. **STA assessment update: 5 June 2018 (https://www.gov.uk/government/publications/sta-assessment-update-5-june-2018)**

    - 5 June 2018
    - Standards and Testing Agency

- Correspondence

See all news and communications (https://www.gov.uk/search/advanced?group=news_and_communications&topic=%2Feducation%2Fprimary-curriculum-key-stage-2)

Policy and engagement

1. Regulating national assessments (https://www.gov.uk/government/consultations/regulating-national-assessments) 6 March 2018
   Ofqual
   Consultation outcome
   Date closed 20 December 2017
2. Primary school pupil assessment: Rochford Review recommendations (https://www.gov.uk/government/consultations/primary-school-pupil-assessment-rochford-review-recommendations)
   14 September 2017
   Department for Education and Standards and Testing Agency
   Consultation outcome
   Date closed 22 June 2017

1. **Primary pupil assessment: Rochford Review impact assessment (https://www.gov.uk/government/publications/primary-pupil-assessment-rochford-review-impact-assessment)**

   - 14 September 2017
   - Department for Education
   - Impact assessment

2. **Rochford Review: final report (https://www.gov.uk/government/publications/rochford-review-final-report)**

   - 19 October 2016
   - Standards and Testing Agency
   - Independent report

3. **Rochford Review: interim recommendations (https://www.gov.uk/government/publications/rochford-review-interim-recommendations)**

   - 5 February 2016
   - Standards and Testing Agency
   - Independent report

See all policy and engagement (https://www.gov.uk/search/advanced?group=policy_and_engagement&topic=%2Feducation%2Fprimary-curriculum-key-stage-2)

Transparency

1. **Observations on the consistency of moderator judgements (https://www.gov.uk/government/publications/observations-on-the-consistency-of-moderator-judgements)**

   - 29 March 2018
   - Ofqual

- Research

2. **National curriculum assessments: key stage 2, 2017 (revised) (https://www.gov.uk/government/statistics/national-curriculum-assessments-key-stage-2-2017-revised)**

    - 25 January 2018
    - Department for Education
    - National statistics

3. **National curriculum test handbook: 2016 and 2017 (https://www.gov.uk/government/publications/national-curriculum-test-handbook-2016-and-2017)**

    - 21 December 2017
    - Standards and Testing Agency
    - Research

4. **National curriculum assessments: key stage 2, 2016 (revised) (https://www.gov.uk/government/statistics/national-curriculum-assessments-key-stage-2-2016-revised)**

    - 14 December 2017
    - Department for Education
    - National statistics

5. **Key stage 2 national curriculum test review outcomes: 2017 (https://www.gov.uk/government/statistics/key-stage-2-national-curriculum-test-review-outcomes-2017)**

    - 2 November 2017
    - Department for Education and Standards and Testing Agency
    - National statistics

See all transparency (https://www.gov.uk/search/advanced?group=transparency&topic=%2Feducation%2Fprimary-curriculum-key-stage-2)

Organisations

1. Standards & Testing Agency (https://www.gov.uk/government/organisations/standards-and-testing-agency)
2. Department for Education (https://www.gov.uk/government/organisations/department-for-education)

1. Ofsted (https://www.gov.uk/government/organisations/ofsted)
2. Ofqual (https://www.gov.uk/government/organisations/ofqual)

Explore these sub-topics

1. **English (key stage 2) (https://www.gov.uk/education/primary-curriculum-key-stage-2-english)**

    Programme of study and research.

2. **Maths (key stage 2) (https://www.gov.uk/education/primary-curriculum-key-stage-2-maths)**

   Programme of study and research.

3. **Programmes of study (key stage 2) (https://www.gov.uk/education/primary-curriculum-key-stage-2-programmes-of-study)**

   National curriculum framework, attainment targets.

4. **Science (key stage 2) (https://www.gov.uk/education/primary-curriculum-key-stage-2-science)**

   Programme of study and research.

5. **Tests and assessments (key stage 2) (https://www.gov.uk/education/primary-curriculum-key-stage-2-tests-and-assessments)**

   Key dates, sample and test materials, administration, moderation, assessing and reporting, statistics, frameworks.

DfE Security Assurance Model - Triage Document

SYSTEM / SERVICE NAME:		SRO:		Project Manager:	

RISK ASSESSMENT QUESTIONS		RISK SCORES						PROJECT TRIAGE SCORES	ITSAT ASSESSED SCORES
		0	1	2	3	4	5		
INFORMATION & DATA PRIVACY IMPACTS NOTE: THIS ASSESSMENT IS FOR INFORMATION AT OFFICIAL ONLY; IF YOU NEED TO PROCESS INFORMATION AT A HIGHER CLASSIFICATION PLEASE CONTACT YOUR ITSAT-ADVISOR FOR ADVICE.	Estimated Number of Records	Tens of Records	Hundreds of Records	Thousands of Records	Tens of Thousands of Records	Hundreds of Thousands of Records	A Million Records and above	0	0
	Data Confidentiality (Type of Data being Stored or Processed)	DfE Information in the Public Domain	DfE Information Containing No Personal or Sensitive Business Information		Small amounts of Personal and/or Sensitive Business or Cross Government Information (Not exceeding 15% of the Data Stored / Processed)	Moderate amounts of Personal and/or Sensitive Business or Cross Government Information (Not Exceeding 50% of the Data Stored/Processed)	Significant amounts of Personal and/or Sensitive Business or Cross Government Information (Exceeding 50% of the Data Stored / Processed)	0	0
	Estimated Amount of Personal Data (DPA 1998-GDPR 2016)	None	Tens of Records	Hundreds of Records	Thousands of Records	Tens of Thousands of Records	Hundreds of Thousands of Records	0	0
TECHNICAL ENVIRONMENT	External Network Connectivity		DfE Express Route	PSN Connected Services	Supplier Connected Secure VPN (Dedicated)	Encrypted Internet Connection (Trusted Users)	**Internet Connected – Untrusted Users**	0	0
	Hosting Arrangements		Within a Government Owned Building	DfE Azure / O365 Cloud with OffShore Elements within the EEA (Near- Shore)	Third-Party Data Centre or Cloud Hosting within the UK	**Cloud Hosting with OffShore Elements Outside the EEA (Far-Shore)**	**Un-Assured Hosting Provider** **Un-Assured Cloud Provider**	0	0
	Solution Complexity		COTS with No Customisation	COTS with Minor Customisation	COTS with Significant Customisation		**Fully Bespoke or Untried Solution**	0	0
BUSINESS DEPENDENCY	Business Reliance on System		A Few Teams within the Department	Entire Directorate or Significant Portion of Department	Whole Department	More than One Department, or Organisation (Multiple SIRO)	**Pan Government** **National**	0	0
	User Types and Groups, including Suppliers, Using the System / Service	Single Organisation (DfE + Outsource Supplier) (Note:This option scores as a 1 in column (I))	1 Organisation / Groups (DfE + Outsource Supplier & One Other Approved Organisation, including LA's Schools & Academy's)	2 Organisation / Groups (DfE + Outsource Supplier & Two Other Approved Organisations, including LA's Schools & Academy's)	3 Organisation / Groups (DfE + Outsource Supplier & Three Other Approved Organisations, including LA's Schools & Academy's)	5, plus Organisations (DfE + Outsource Supplier & Other Approved Organisations, including LA's Schools & Academy's)	DfE, plus Organisations (DfE + Outsource Supplier & Publically Accessible)	0	0
	Business Criticality (How Important is the Integrity and Availability of the Data being Stored or Processed)	Not Critical to Delivery of Core Department Objectives	Supports Delivery of Core Department Objectives	Critical to Delivery of Core Department Objectives	Critical to Delivery of Cross Government Services.	Critical to Delivery of Public-Facing Services.		0	0
What is the projected life of the system?									
							Total:	0	0
							Assurance Type:		

Notes:

1. DSAM Triage scores within a range of 18 - 22 shall be reviewed by DSAT to assure that an appropriate security assurance path is being followed.

Assurance Type:	**A**	**20 to 44**
Assurance Type:	**B**	**4 to 19**

DfE Security Assurance Model - ITHC Remedial Action Plan

IT Health Check Remedial Action Plan for: [Enter Report Reference and System, Service or Application Name]

Report Date: [Enter Report Date]

DSAM Form 3 - v2.0

When changing the Status in column F just Type, Open, Closed or Accepted the Status will update accordingly

Risk Rating	Total Count	Open	Accepted (Unmitigated)	Accepted (Partial)	Closed
Critical	0	0	0	0	0
High	1	0	0	0	1
Medium	0	0	0	0	0
Low	0	0	0	0	0
Very Low	0	0	0	0	0
Information	0	0	0	0	0
Totals	1	0	0	0	1

When changing the Residual risk Indicator in Column O just Type, High, Medium, Low or Very Low the RRI status will update accordingly

Finding No.	Impact	Likelihood	Overall Risk	Status	Finding	Hosts	Recommendation	Planned Mitigation	Planned Completion Date	Actual Mitigation [Evidence of Change e.g. CAB reference should be provided]	Owner	Actual Closure Date	Residual Risk Indicator	Initial DSAT Assessment
			High	Closed									High	

Department for Education

[Insert System, Service, Application or Network Name] Security Assurance Report

Version X.X

This document is an OFFICIAL document and may contain sensitive information about the departments approach to security assurance and configuration of departmental systems, services and applications.

The information contained in this document should only be disseminated and retained by individuals within the Department for Education Digital, Data & Technology and trusted third party providers and their representatives.

The document and the information contained may only be shared with external personnel with a 'need to know' criteria who hold a minimum of UK BPSS security clearance or equivalent.

It is not to be shared with sub-contractors or organisations without explicit written authority from the Head of Systems Assurance or the Deputy Senior Information Risk Owner. It must not be shared with any offshore personnel or non-UK Nationals.

This document or the information contained must not to be sent across the Internet without appropriate protection, such as in an encrypted file using either a self-decrypting archive or encrypted zip file and must not be processed or stored on unmanaged devices.

All hard copies of this document are considered to be uncontrolled and when no longer required must be disposed of or destroyed by either cross-cut shredding or placing the document in a secure bin for shredding or other approved physical destruction method.

Table of Contents

1 Introduction

This document is presented as a statement of security assurance for the under-mentioned solution used by the department to store and process OFFICIAL information (including OFFICIAL--SENSITIVE – *delete, if not applicable*). The following sections will provide further detail on the requirements, acknowledged controls and assertions associated with this assurance.

[Insert System / Service Name Here]

1.1 IT Systems Assurance Team (ITSAT) Statement

ITSAT confirms that, on behalf of the SIRO, a review of the assurance evidence and risk management approach presented at Section 3 of this document has been carried out and, where necessary, relevant advisories have been added at Section 6 of the document. ITSAT accepts that the statements made in this document, based on the information to hand, are correct and that this document is an accurate reflection of the security assurance surrounding the documented solution.

Information from this and other documents shall be used by ITSAT to draw up and issue a Security Assurance Statement that will describe the assessed level of security assurance afforded to the system, service, application or network.

1.2 Assurance Review Conditions

This document shall be maintained as a "living" record of the assurance aspects of the *[Insert System / Service Name]*. Any security-relevant changes, such as those outlined below, shall initiate a review of the security assurance surrounding the system or service. These changes may include:

a. Any major changes to the system, service or application architecture, including the addition of any internal or external connectivity.
b. A change in the status of the user groups or their security clearances.
c. A change in the risk or threat profile associated with the system, service or application.
d. A major security concern, be it a single significant incident or an accumulation of minor incidents.
e. A change in business circumstances and opportunities, including service and support, outsourcing, offshoring or a change in circumstances within a supplier organisation, including a shortfall in the working practices of a supplier.
f. The introduction of a new business requirement or changes to the scope of use.
g. A change to the HMG Security Policy Framework (SPF), legislation or other overarching security polices and guidance, that materially affect the security and operation of the system, service or application.
h. Any alteration in or additional levels of remote access and administration.
i. A change in the supporting assurances, such as the loss of security assurance for a major supporting component.
j. A change which affects the physical security of one or more data centres or operational management centres, including disaster recovery, backup and archive storage, used to house and support the service, including changes to suppliers or locations.

The IT Systems Assurance Advisor (ITSAA) can advise on which changes would be considered as being of security relevance, and should be consulted if there is any doubt.

AWT

1.3 Assurance History

The following table maintains a historical record of the solution's security assurance[1]:

Date	SIRO	SRO	ITSAT	Proposed Review Date[2]
DD-MMM-YYYY	[Name]	[Name]	[Name]	[Enter Date]

2 Background Information

Documents on which the solution's security assurance is based:

Title	Reference (If Any)	Version Number	Document Date
[Document Name[	[Document Reference]	[Version Number]	[Date]

2.1 Solution High Level Overview

This section shall contain a high-level description of the system, service or application.

2.1.1 Architecture Overview Diagram

Insert Diagrams Here

Figure 1: Diagram of the System, Service or Application

2.1.2 Stakeholders[3]

The key stakeholders for this solution are:

Appointment	Name	Appointment	Name
Senior Information Risk Owner (SIRO)		Security & Information Risk Advisor (SIRA)	
IT Systems Assurance Advisor		System Architect	
Senior Responsible Owner (SRO)		System / Application Owner	
Project Manager (PM)		Cloud Operations / Cyber Security	

1 Note: If this is the initial systems assurance document, for the solution delete the existing text and table and replace these with the text stating that position.

2 The proposed review date does not indicate the expiry of the security assurance, but is intended as a simple check of the Assurance Review Conditions shown at Section 1.2 above.

3 Section 2.1.2 Stakeholders should be amended to show the appropriate key stakeholder; the example above is neither fixed nor exhaustive.

2.1.3 Solution Design Principles

Has the solution been designed using the following security and design principles guidance published by NCSC, if so detail the principles and other guidance used in designing the solution below:

- ***Cloud Security Principles**. These principles will be used later in the document to complete the risk assessment for the solution. https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles*
- ***Security Design Principles for Digital Services**. These security design principles are intended to inform systems architecture design where there is no precedent or architectural pattern to follow. https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main*
- ***Bulk Personal Data.** Has a Bulk Assessment been completed and have the required control groups been applied to the design of the solution? If so has the result of the assessment been reported to the IT Systems Assurance Advisor. https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main*
- ***End User Devices Security Guidance.** This guidance is for any organisation wishing to secure the End User Devices (EUD) they use, but it is primarily to help system administrators make informed decisions about the configuration, management and use of EUDs, and risk owners understand the overall risk to their networks presented by their use. https://www.ncsc.gov.uk/guidance/end-user-device-security*

2.1.4 Information Assets

Describe the information assets, including their classification and criticality to the business.

2.1.5 Geographical Locations

Provide details of the system, service or application locations covering the following bullet points:

- *Hosting locations, this should detail the physical location of any physical, virtual or cloud environments and any disaster recovery locations;*
- *Department or third party management and administration centres;*
- *User locations; e.g. departmental locations or, if a shared solution, other user groups.*

2.1.6 Users and Usage

Provide a bulleted list of the system, service or application's users, roles, security clearance(s) and location; this list should include any external users and third-party support and development providers.

2.1.7 Interconnections and Interfaces

Provide details of all internal and external system or network interconnections and interfaces used by the system, service or application.

2.1.8 Exchange of Information

Does the system facilitate the exchange of information either across the department or to external organisations, if so provide details of all such information exchanges and data sources used by the system, service or application? This should include a statement that all information exchanges and data sources are subject to content checking for viruses and malicious code.

3 Risk Assurance Summary

3.1 Business Impact Assessment (BIA)[4]

The department's stated Risk Appetite and Risk Tolerance ranges from "OPEN" to "CAUTIOUS" dependent of the information being stored or processed. This approach is aligned with a classification of OFFICIAL (including OFFICIAL–SENSITIVE) and is defined as having a "preference for safe delivery options that have a low to medium degree of residual risk". The forms of risk which, if realised, would be regarded as unacceptable to the department include, but are not limited to, the following:

Describe the business risks and potential impacts to the information being stored or processed should the risks be realised. For instance:

The forms of risk which, if realised, would be regarded as unacceptable include, but are not limited to, the following:

- ***Confidentiality**: Any exposure of financial information relating to the provision of funding to schools, academies and other educational institutes throughout the UK which is considered to be sensitive business information or, in the case of personal data (as defined by the Data Protection Act), any exposure of personal information that would cause unnecessary harm or distress to an individual or individuals.*
- ***Integrity**: Errors introduced to personnel records and financial information, or malicious modification of data or code by unauthorised individuals would be damaging to the department's operations.*
- ***Availability**: Any extended loss of service outside of planned maintenance windows.*
- ***Financial Impacts**: Mistakes likely to result in inaccuracies, or any malicious modification of data or code or fraudulent activity by any individual within the department's financial systems would be seriously damaging to the department's operations and must be avoided.*
- ***Reputation impacts**: Any visible breach of the service or a publicised failure to deliver against public commitments.*
- ***Legal and Compliance**: Any breach of HMG or departmental policy, any breach of the law, including the Data Protection Act 1998, or a lack of confidence in the security of the solution.*

3.2 Offshoring

Is the solution, together with any information being stored or processed subject to offshoring outside of the UK Mainland; this includes any support or development activities carried out on the solution. If so have you completed the Department's Offshoring Application and submitted this to your IT Systems Assurance Advisor for approval by the DfE SIRO?

3.3 Data Privacy Impact Assessment (DPIA)

Does the solution store or process personal data? If so, has the project conducted a DPIA pre-assessment or full DPIA assessment? Was the assessment reviewed and accepted by the department's legal team and/or business data controller? What were the findings and decision made?

[4] Further advice on how to value and assess departmental information can be found in "*OGSIRO Guidance: Information Risk Appetite v1.0; 4 June 2015*".

3.4 Overall Scope of Security Assurance

Describe the boundaries of the scope of assurance, including details of interfaces or interconnections, any components where a level of assurance can be drawn from, such as pre-existing certifications, accreditations or product assurances.

Insert the Scope of Security Assurance Diagram Here[5]

Figure 2: XXX System Assurance and Reliance Scope

3.5 Assurance Components[6]

Assurance of the solution has been derived from a number of sources, these 'assurance components' are listed under the headings below with a brief description of the attribute and assurance being claimed.

3.5.1 Policy, Procedures, Processes, Standards and Guidance

Provide details of the relevant HMG or departmental policy and guidance used in the development of the system, service or application confirming that the solution conforms to published HMG and departmental policy and guidance, such as the End User Device Guides. Provide a bulleted list with a brief description of the assurance attributes used.

3.5.2 Access Control:

Provide details of the solution's user provisioning approval and authentication processes, how are user accounts and privileges assigned and reviewed.

3.5.3 Password Management

Provide details of the solution's password management structure, including length, complexity, aging and lockout mechanism. Do any users, including any external users and third-party support and development providers access the system using two-factor authentication or any other secure access solution?

3.5.4 Legal and Regulatory Assurance

Provide confirmation that the system, service or application and its planned use meets applicable legal and regulatory requirements. If a project has a particular legal or regulatory impact reference this here.

3.5.5 Commercial Assurance

Provide confirmation that suitable contractual terms are in place for the deployment and use of the system, service or application.

---

5 This diagram should be based on either the HMG IS1&2 Domain or DBSy Domain Models and must clearly show the system components that are inside the scope of assurance.

6 Note the section headings below are provided as an example of assurance component that may be used to show compliance, these heading are not exclusive and can be replaced or supplemented by other components. Security Assurance Components that should be considered are shown within the DfE Security Assurance Component Guidance on the DfE Intranet Pages.

3.5.6 Use of Certified Products[7]

Provide a list of products which have claimed certifications e.g. FIPS 140-2.

3.5.7 Compliance to Recognised Standards

Provide details of any certification or compliance to a recognised standard, such as ISO / IEC 27001 or other valid standard held by the supplier. Please include certificate reference and validity dates. A copy of the certificate should also be provided as supporting evidence for the claimed assurance.

3.5.8 Security Inspections and Validation Testing

3.5.8.1 System Testing

Confirm that the system, service or application has successfully passed through end-to-end system and operational testing and that all identified defects were resolved. Validation of the end-to-end system testing should be sought, verified where necessary and referenced here.

3.5.8.2 IT Health Check[8]

Confirm that the IT Health Check (ITHC) scope of testing was both appropriate and proportionate to the system, service or application, that all service-impacting controls were within scope of the testing and a qualified Cyber Certified Professional Security & Information Risk Advisor (CCP SIRA), or the IT Systems Assurance Advisor, validated the scope. The scope document should be referenced here.

The ITHC should be carried out by an independent certified ITHC provider, such as those registered in the NCSC CHECK scheme. The ITHC should address and report on all areas covered in the ITHC scope. The ITHC report, not the content, should be referenced here.

A qualified CCP SIRA should review the ITHC report. All risks and issues should be clearly identified and, where action is deemed necessary, a remedial action plan to address the notified risk and issues shall be drawn up and referenced here. Note: it is the responsibility of the project and the assigned SRO to ensure that appropriate, proportionate IT Health checks have been complete, and all findings remediated.

4 Risk Assessment and Treatment[9]

The risk assessment approach preferred by the department is the application of the fourteen (14) published NCSC Security Principles which set out a common approach to implementing security assurance as detailed by the documents below. This approach also allows for the use of a more defined risk assessment using an acceptable methodology to be overlaid:

- *Cloud Security Principles:*

  https://www.gov.uk/government/publications/cloud-security-guidance-introduction/cloud-security-guidance-introduction

- *Cloud Security Guidance - Risk Management:*

---

7 Note: Section 3.5.6 does not verify that the control components have been properly configured, or that the components are correctly or robustly implemented. This will be confirmed by relevant system and security testing, and IT Health Checks.

8 ITSAT has published an ITHC Guidance document to assist projects in the scoping of IT Health Checks.

9 The risk assessment process detailed above is predicated on the fourteen (14) published NCSC Security Principles. If a different assessment methodology is used then this should be briefly described at Section 4.5.

https://www.gov.uk/government/publications/cloud-security-guidance-risk-management

4.1 Risk Assessment

Describe the risk assessment methodology used in creating this assessment, e.g. the solution was assessed using the fourteen (14) published NCSC Security Principles, which provide a number of means by which the risks can be identified. Provide details of any review of the applied controls and their implementation by a suitably qualified individual, such as a CCP SIRA, or a recognised subject matter expert, who reviews the scope of the certification and the implementation of the controls. This approach provides a higher degree of confidence that the service meets the stated objectives through certification against an appropriate standard. If another risk assessment methodology has been used to supplement the security principles summarise this here by stating the number of risks and issues and levels of risk found and provide reference to the assessment report here.

4.2 Risk Treatment[10]

Provide details of any review of the controls applied following the risk assessment described at 4.1 and their implementation by a suitably qualified individual, such as a CCP SIRA, or a recognised subject matter expert.

Controls that are both appropriate and proportionate to the identified risk should be selected and implemented to treat the risk. These controls can be selected from a number of different sources, such as the ISO / IEC 27002, Centre for Internet Security Critical Security Controls, Cobit 5 or NIST standards which are recognised and widely used within industry. This approach provides a higher degree of confidence that the service meets the stated objectives through certification against an appropriate standard.

Cloud Security Principles

4.2.1 Data in Transit Protection

Principle	**Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption. If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

[10] The Centre for Internet Security Critical Security Controls can be found at: http://www.cisecurity.org/critical-controls.cfm

4.2.2 Asset Protection and Resilience

Principle	**Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure[11]. If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.3 Separation between Consumers

Principle	**Separation should exist between different consumers of the service to prevent malicious or compromised consumers from affecting the service or data of another. If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.4 Governance

Principle	**The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it. If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.5 Operational Security

Principle	**The service provider should have processes and procedures in place to ensure the operational security of the service. If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.**

[11] The protection of DfE information as an asset at rest or store will require the use of an approved encryption product, the protection of physical infrastructure storing or processing DfE information will require physical security measure to be implemented.

Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.6 Personnel Security

Principle	**Service provider staff should be subject to personnel security screening and security education for their role. If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.7 Secure Development

Principle	**Services should be designed and developed to identify and mitigate threats to their security. If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.8 Supply Chain Security

Principle	**The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement. If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.9 Secure Consumer Management

Principle	**Consumers should be provided with the tools required to help them securely manage their service. If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.10 Identity and Authentication

Principle	**Access to all service interfaces, for consumers and providers, should be constrained to authenticated and authorised individuals. If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data or denial of service may occur.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.11 External Interface Protection

Principle	**All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them. If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.12 Secure Service Administration

Principle	**The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*

Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.13 Audit Information Provision to Consumers

Principle	**Consumers should be provided with the audit records they need to monitor access to their service and the data held within it. If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.2.14 Secure Use of the Service by the Consumer

Principle	**Consumers have certain responsibilities when using a service in order for this use to remain secure, and for their data to be adequately protected. If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.**
Identified Risks	• *Provide a bulleted list any identified risks and shortfalls here. Each risk should have a unique identifier, a description of the risk and risk level.*
Controls Applied	• *Provide a bulleted list of the Controls applicable to this principle should display a unique control identifier, used for each instance of the controls implementation; a description of the control applied should be included.*
Residual Risks	• *Provide a bulleted list of the Residual risks identified here; any risks shown here must be included in the DSAM-5 – Residual Risk Statement. Each residual risk should have a unique identifier, a description of the risk, an initial risk level, the treatment approach and a final risk level.*

4.3 Additional Risk Assessment Overlay

The use of any additional risk assessment methodologies, such as; HMG IS1&2 or ISO 27005 used in the assessment or treatment of risks to this solution shall be summarised, and references to the full assessment provided here.

5 In-Service - Security Assurance Plan

An 'In-Service - Security Assurance Plan' should be drawn up and implemented to ensure the continued assurance of the system, service or application throughout its life-cycle. The plan shall contain details of the business accountability, task owner and frequency of the task. Areas to be covered as a minimum by this plan include, but are not limited to, the following:

- *Security Policy Reviews;*
- *Risk Reviews;*
- *Security Assurance Report Reviews;*
- *Security Control Reviews;*
- *IT Health Check / Penetration Testing, planning, completion and remediation;*

- *Protective Monitoring;*
- *Physical Security Inspections;*
- *System Audits,*
- *Software Updates and Patching*
- *Security Operating Instructions,*
- *Service Operating Manuals,*
- *Incident Reporting and Management,*
- *Supplier Reviews, etc.*

Department for Education

Residual Risk and Security Assurance Statement [Insert System, Service or Application Name] Issued [Insert Date]

Version X.X

This document is an OFFICIAL document and may contain sensitive information about the departments approach to security assurance and configuration of departmental systems, services and applications.

The information contained in this document should only be disseminated and retained by individuals within the Department for Education Digital, Data & Technology and trusted third party providers and their representatives.

The document and the information contained may only be shared with external personnel with a 'need to know' criteria who hold a minimum of UK BPSS security clearance or equivalent.

It is not to be shared with sub-contractors or organisations without explicit written authority from the Head of Systems Assurance or the Deputy Senior Information Risk Owner. It must not be shared with any offshore personnel or non-UK Nationals.

This document or the information contained must not to be sent across the Internet without appropriate protection, such as in an encrypted file using either a self-decrypting archive or encrypted zip file and must not be processed or stored on unmanaged devices.

All hard copies of this document are considered to be uncontrolled and when no longer required must be disposed of or destroyed by either cross-cut shredding or placing the document in a secure bin for shredding or other approved physical destruction method.

Table of Contents

1 Introduction

This document forms the residual risk and security assurance statement for the [Insert system, service, application or network name]. These risks are what remain following risk treatment.

2 Part 1 - Residual Risks and Issues (To be completed by CCP SIRA or Project Manager)

The following residual risks and issues pertaining to the system, service, application or network remain following implementation of available measures and security controls:

2.1 Non-ITHC Risks

2.1.1 [Insert Risk or Issue Identifier and Name]

- *Example Risk: There is a risk, due to an inability to purge individual sections of the storage medium, that data containing personal information may be retained beyond its business requirement leading to a risk of exposure if there is a security breach, leading to a potential breach of the Data Protection Act 1998. However, the likelihood of exposure of this retained data is minimal due to the protective controls applied to the overall solution and the Residual Risk Rating is Low.*

2.1.2 [Insert Risk or Issue Identifier and Name]

- *Example Risk: There is a risk that third party supplier will be unable to support the xxxx system due to a shortfall in linux knowledge within the current support team. Although a failure is possible the risk is minimal as the xxxx system is not a critical business asset and can be recovered within 24 – 48 hours the Residual Risk Rating is therefore considered to be Low.*

2.2 ITHC Risks

2.2.1 [Insert Risk or Issue Identifier and Name]

- *Example Risk: Medium rated risk. Testing identified that a weak user account lockout policy was configured on the server. There is a risk that an attacker could brute-force user passwords by making repeated attempts to logon until the correct password is found.*

3 Part 2 - Security Assurance Statement (To be completed by ITSAT)

The undermentioned system, service, application or network has been through a security assurance assessment for the storage and processing of departmental information. The purpose of the assessment is to measure the risks and assurance levels pertaining to the system, notify the business of those risks and assurances and provide the Senior Responsible Owner (SRO) with any necessary information on which to base their risk ownership decision. The assessment was based on the documents listed at Section 3.1 of this document.

System / Service Name	Classification
[Insert System / Service / Application or Network Name]	OFFICIAL (including OFFICIAL–SENSITIVE – *delete, if not applicable*)

3.1 Document Reference(s)

- [Insert bulleted list of referenced documents here, this should include; the document title, any reference, date and version number]

4 Observed Risk and Assurance Levels (To be completed by ITSAT)

Following assessment, it is the opinion of the IT Systems Assurance Team (ITSAT) that the residual and unmitigated risks surrounding the above system, are:

4.1 Risk Rating:

The observed residual risk rating following any risk mitigation for this system is: Critical / Significant / High / Medium / Low / Very Low*

The reason for this rating is…

4.2 Security Assurance Level:

The assessed security assurance level for the system is: High / Medium / Low*

This assessment is made based on…

5 ITSAT Security Advisories (To be completed by ITSAT)

The following ITSAT security advisories are made in respect of the *[Insert System / Service / Application or Network Name]:*

Advisory Number	Details
[Enter Advisory No.]	[Enter security advisory details here]

6 Part 3 - Risk Ownership[1]

As the Senior Responsible Owner / Information Asset Owner for the above-named system, service application or network; I confirm that I been briefed on the unmitigated or residual risks detailed above and that these risks and issues are understood and owned by me.

Name	Signature	Appointment	Contact Details (Email / Phone)

[1] Note: In all cases, a scanned copy of this document signed by the SRO / IAO or an email attributable to the SRO / IAO must be forwarded to ITSAT and retained.

Department for Education

DfE – Guidance - IT Health Check Requirements

Version 2.0.2

This document is an OFFICIAL document and may contain sensitive information about the departments approach to security assurance and configuration of departmental systems, services and applications.

The information contained in this document should only be disseminated and retained by individuals within the Department for Education (DfE) IT Systems Assurance Team and trusted third party providers and their representatives.

The document and the information contained may only be shared with external personnel with a 'need to know' criteria who hold a minimum of UK BPSS security clearance or equivalent.

It is not to be shared with sub-contractors or organisations without explicit written authority from the Head of Systems Assurance or the DfE Senior Information Risk Owner. It must not be shared with any offshore personnel or non-UK Nationals.

This document or the information contained must not to be sent across the Internet without appropriate protection, such as in an encrypted file using either a self-decrypting archive or encrypted zip file and must not be processed or stored on unmanaged devices.

All hard copies of this document are considered to be uncontrolled and when no longer required must be disposed of or destroyed by either cross-cut shredding or placing the document in a secure bin for shredding or other approved physical destruction method.

Table of Content

1 Introduction

The aim of the IT Health Check (ITHC) is to provide the Department for Education (DfE) with assurance that the organisations systems, services, applications and network infrastructure are properly configured and, as far as is possible, protected from unauthorised access or change, and that they do not provide an unauthorised point of entry into your network infrastructure. This is especially important for those systems, services and applications which process and store sensitive information and are externally facing, such as websites, or, systems having onward connection interfaces and interconnections to other systems or organisations.

All systems, services, applications and network infrastructure should be subject to an ITHC prior to their operational go-live and annually thereafter to provide assurance that no significant weaknesses exist on the network or individual systems, that could allow any device to intentionally or unintentionally affect the security of another. It is mandated that government departments shall use National Centre for Cyber Security (NCSC) CHECK Scheme ITHC Providers for all systems storing or processing information at OFFICIAL.

2 Objective

To assist in the development of an effective scope of work and conducting an appropriate ITHC to support the assurance of the systems, services, applications and network infrastructure. This is equally important if the ITHC is for a new service or the renewal of assurance for an existing system, service, application or network infrastructure.

To ensure that the business understands what constitutes 'sufficient assurance' in that suitable technical testing has been undertaken and the identified vulnerabilities have been adequately mitigated.

3 The CHECK IT Health Check Process

A typical ITHC is a six-stage process. These stages include:

- **Stage One - Decision**. The decision to conduct an ITHC will normally be taken in conjunction with the project and the IT Systems Assurance Team (ITSAT) and will be influenced by the sensitivity of the systems, services, applications or network infrastructure, the levels of information being processed and stored, and the potential for its exposure to unauthorised access.
- **Stage Two - Statement of Work**. This is the key process, ensuring that all elements of a system, which require testing, are identified to the ITHC Provider.
- **Stage Three - Confirmation of Scope**. This demonstrates that the ITHC Provider understands the requirement.
- **Stage Four - The ITHC Test**. The ITHC is conducted. It is important to ensure that the information processed and stored on any system is backed up and all necessary change controls are in place before testing commences.
- **Stage Five - The ITHC Report**. The findings and recommendations are reviewed and accepted.

- **Stage Six – The ITHC Remediation Process**. This is a key stage of the overall process, ensuring that sufficient assurance is obtained from the mitigation decisions identified for each risk or issue.

DfE has a call-off arrangement with an ITHC provider. As a certified CHECK provider and our trusted ITHC partner, the department will allow the connection of their laptops to DfE networks for the purposes of testing. If using other ITHC providers, you should discuss with the DDaT Security Operations Centre (SOC whether that supplier will be allowed to connect their devices or will be required to use a DfE provisioned device.

4 The IT Health Check Scope

Developing an appropriate ITHC Scope is an important first step to ensuring that the ITHC is a worthwhile exercise that will provide you with a correct level of assurance for the systems, services, applications or network infrastructures being tested.

It is strongly recommended that a qualified NCSC Certified Security Consultancy (CCSC) or Cyber Certified Professional (CCP) Security & Information Risk Advisor (SIRA), be retained to advise the project and develop the ITHC Scope to ensure it is both appropriate and proportional to the systems, services, applications or network infrastructures being tested.

If the business does not use the services of a qualified CCSC or CCP SIRA it should be recognised that if the ITHC Scope does not cover the required range of testing, then the IT Systems Assurance Advisor (ITSAA) or other Authority may require additional testing to be carried out to gain sufficient assurance on the security of the build and configuration of the systems, services, applications or network infrastructure.

4.1 Internal ITHC Testing

An internal ITHC, regardless of scale, is essentially a vulnerability scan to ensure the correct configuration of systems, services, applications and network devices. As a minimum an internal ITHC should include:

- A review of the desktop and server build and configuration; network management security check. This should include checks to ensure that user access permissions, including system to system accesses, are set accordingly; that the password system is configured correctly and events are being logged for audit purposes.
- Ensure default logon credentials have been changed for software down to server level.
- A review of security patches and software updates at the operating system, application and the firmware level.
- A review of all system, service or application interfaces and interconnections to ensure that these are configured as expected and unauthorised access is not possible.
- A review of the configuration of remote access solutions, this is particularly important if the device being tested is part of a mobile solution giving access to your internal network resources and information.
- Confirm the build and configuration of laptops and other mobile devices such as phones and tablets used to access DfE information and systems.

- Check the operation of any internal security gateways, ensuring that all components, such as firewalls, intrusion detection, content checking and anti-virus, plus any protocol breaks are operating as expected.
- Check any wireless network configuration; ensure that these are configured as expected and unauthorised access is not possible.

These scans will look to provide assurance that your internal systems have been configured in a secure manner and have been properly maintained. The ITHC or vulnerability scanning should cover the entire environment to be tested including end-points, thick and thin clients, servers, network devices and appliances.

4.2 System Sampling

It is normal for all components of the solution to be tested to be included within the scope of work. However, in areas with a large number of devices, a representative sample may be acceptable on the proviso that the sample covers all capabilities and functions of the solution. The size of the sample will normally be no less than **20%** of the environment to be tested.

4.3 Build Testing

Where a defined secure build exists that has been subject to its own ITHC, and not modified post testing, has been used in the build of the solution it is acceptable to reduce the scale of the ITHC to a randomly selected representative sample of the solution being tested. It is essential that the testing should capture at least one or two examples of each component or build type within the overall solution to validate the use of the build throughout the solution.

If, however, it is identified either before or during the ITHC, that the build has been modified or has not been universally applied, the ITHC scope of work shall be revised to encompass a much wider sample of the solution. This is likely to involve the cancellation of the test and re-scheduling with any additional days required added to the scope of work. The cost of any such revision of the scope shall be borne by the project.

4.4 Application Testing and Code Review

The primary objective of an application test and code review is the assurance that any security enforcing controls are effective, appropriate and proportionate. This may be through a combination of code and application reviews. A code review includes any bespoke code that has been written to provide security enforcing controls. These could include (but not limited to):

- The authentication model
- Security of credentials in transit and at rest
- Role Based Access Control (RBAC)
- Data leakage/customer data separation
- Database connectivity
- Where it is proposed to share code in a code repository such as Github or BitBucket, testing of access controls, exposure of sensitive code and code approval procedures e.g. code reviews and checks before new code is uploaded.

Application tests would normally include the following:

- Testing to validate application is free from known vulnerabilities and configuration errors
- Testing to validate that unauthenticated users cannot view, modify, or delete data in an unauthorised manner
- Testing to validate that authorised users cannot view, modify, or delete data in an unauthorised manner, gain access to unauthorised functionality or escalate their privileges
- Review of application logic, access controls and authentication mechanisms
- Alignment with security hardening best practice (CIS or equivalent)
- Vulnerability scanning of exposed surfaces
- Testing to validate https is enforced
- For web applications, assessment against the OWASP top 10 2013 and OWASP top 10 2017 critical application vulnerabilities. See https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Testing of interactive web pages within the application

4.6 External ITHC Testing

In addition to the internal testing an external ITHC or Penetration Test shall be carried out on all systems that provide access beyond the boundary of the environment or network infrastructure. The testing shall include any security enforcing controls or devices which are in place to protect the business from unauthorised access from its third-party connections. For example: the operation of any externally facing proxies or security gateways, ensuring that all components, such as firewalls, intrusion detection, content checking, malicious code and anti-virus devices and any protocol breaks are operating as expected.

All third-party suppliers with access to any departmental systems, services, applications and network infrastructures from their own offices or support locations as part of their provision of service must be considered as an external connection and tested accordingly. Further advice as to what should be included in an external test should be sought from a qualified CCSC or CCP SIRA or the ITSAA.

5 The ITHC Report

The output of the ITHC shall be a report by the ITHC Provider that contains a clear summary of the number, type and severity of the issues discovered during the testing of the target systems, services, applications or network infrastructures. As a minimum the ITHC Report shall contain the following:

- Details of the individuals involved in completion of the ITHC.
- The background, scope and context of the ITHC.
- A unique identifier for each risk or issue detailed in the report.
- Each risk or issue discovered should be accurately described and explained.
- Each risk or issue should be assigned an impact and probability score from which a risk value; normally expressed as being; high, medium, low or information, may be derived

- Where possible a Common Vulnerability Scoring System (CVSS) base score should be included. This requirement is mandated for ITHC reports covering the PSN.
- Each risk or issue discovered should be accompanied by a clear recommendation for remedial action; this recommendation may include a short-term fix which may be appropriate while a permanent solution is developed.

6 The ITHC Remedial Action Plan

An ITHC Remedial Action Plan (RAP) shall be compiled from the ITHC Report, using the format shown at Annex A to this document. It is expected that all Critical, High and Medium risks will be fully mitigated before any new systems, services, applications and network infrastructures are permitted to go-live.

The expectation for the remediation of risks and issue on any pre-existing systems, services, applications and network infrastructures is that full remediation of Critical, High and Medium risks shall be completed within two months of the report date.

Subject to agreement between the ITSAA and the Senior Responsible Owner (SRO), any Low and Very Low risks and issues on both new and pre-existing systems, services, applications and network infrastructures may be addressed by a suitable Business As Usual (BAU) Risk Action Plan (RAP) to be completed within three months of the date of the report. The acceptance or mitigation decisions designed to address the notified risks and issues at all levels of risk must be fully justified by the business within the RAP.

7 ITHC Provider Selection

The NCSC provides further details of the CHECK Scheme and information on suitably qualified ITHC Provider companies on their website. See CHECK providers listing

Annex A – ITHC Remedial Action Plan – Format[3]

DfE Security Assurance Model - ITHC Remedial Action Plan

IT Health Check Remedial Action Plan for: [Enter Report Reference and System, Service or Application Name]

Report Date: [Enter Report Date]

DSAM Form 3 - v2.0

When changing the Status in column F just Type, Open, Closed or Accepted the Status will update accordingly

Risk Rating	Total Count	Open	Accepted	Closed
Critical	0	0	0	1
High	1	0	0	0
Medium	0	0	0	0
Low	0	0	0	0
Very Low	0	0	0	0
Information	0	0	0	0
Totals	1	0	0	1

When changing the Residual risk Indicator in Column M just Type, High, Medium, Low or Very Low the RR status will update accordingly

Finding No.	Impact	Likelihood	Overall Risk	Status	Finding	Hosts	Recommendation	Planned Mitigation	Planned Completion Date	Actual Mitigation	Owner	Actual Closure Date	Residual Risk Indicator	Initial ITSAT Assessment
			High	Closed									High	

[3] Note: An electronic copy of this spreadsheet is available on the DfE Intranet.

Department for Education

Self-Assessment - Security Assurance Questionnaire

[Insert System, Service or Application Name Here]

Version X.X

This document is an OFFICIAL document and may contain sensitive information about the departments approach to security assurance and configuration of departmental systems, services and applications.

The information contained in this document should only be disseminated and retained by individuals within the Department for Education Digital, Data & Technology and trusted third party providers and their representatives.

The document and the information contained may only be shared with external personnel with a 'need to know' criteria who hold a minimum of UK BPSS security clearance or equivalent.

It is not to be shared with sub-contractors or organisations without explicit written authority from the Head of Systems Assurance or the Deputy Senior Information Risk Owner. It must not be shared with any offshore personnel or non-UK Nationals.

This document or the information contained must not to be sent across the Internet without appropriate protection, such as in an encrypted file using either a self-decrypting archive or encrypted zip file and must not be processed or stored on unmanaged devices.

All hard copies of this document are considered to be uncontrolled and when no longer required must be disposed of or destroyed by either cross-cut shredding or placing the document in a secure bin for shredding or other approved physical destruction method.

Self-Assessment - Security Assurance Questionnaire

This security questionnaire is applicable to information systems and services storing or processing Department for Education (DfE) information holding a lower level of risk and scoring 19 or less on the Security Assurance Triage (DSAM form 2). These are generally considered to be lower risk projects requiring less security assurance oversight.

This is a self-assurance process designed to enable projects to display sufficient confidence that their data is appropriately secured without having to undergo a full security assurance process.

The questions should be equally applicable to:

- An IT system or service designed to deliver a business function.
- A cloud based service procured to deliver a business function.

Some systems and services may be able derive security assurance from other sources, including pre-existing certifications, such as; certifications issued by another authority, certified products and industry standards , such as; FIPS140-2, ISO / IEC 27001 and 27002 or in the supplier's responses and supporting information provided for the G-Cloud security questionnaire. It is the project's responsibility to obtain this information.

Acceptable responses to the questions are **YES**, **NO** or **NOT APPLICABLE** with additional information being provided, as follows:

- If answering **NO** to any question you must provide further information in the box provided.
- If answering **NOT APPLICABLE** to any question you must state why you believe this control does not apply to you.

If all the questions are either answered as either; **YES** or **NOT APPLICABLE** with an appropriate explanation provided, the form should be copied to DSU for registration.

The Senior Responsible Owner (SRO) must sign as to the accuracy of the questionnaire.

Where the questionnaire answered by either; **NO** or **NOT APPLICABLE** with unclear or insufficient reasons given, IT Systems Assurance Team (ITSAT) may seek clarification, provide advice, or recommend further security controls. The SRO must 'wet' sign the form. The SRO will retain ownership of the identified risk as documented in the corresponding Residual Risk Statement (RRS) for the system, service or application.

1. Brief Description of the System / Service:

The description should provide an overview of the system / service, including details of the data to be stored or processed, the technology to be used, whether the system is public facing or has any internal or external connections, user groups and any intent to off-shore data.

2. System / Service Diagram:

A diagram of the system or service should be inserted in the box below; this diagram should show data flows, protocols used, interconnections and interfaces to other systems and services.

3. Secure Configuration:

3.1. Has the system, service or application been built to an approved design with all relevant security patches and updated applied as recommended by the manufacturer?

☐ YES	☐ NO*	☐ NOT APPLICABLE*

**Further comments.*

3.2. Is the system, service or application regularly maintained with all relevant security patches and updates being tested and applied to the system within a timeframe acceptable to the business?

☐ YES	☐ NO*	☐ NOT APPLICABLE*

**Further comments.*

3.3. Has the system, service or application been locked down to ensure only legitimate authorised users are able to access the system, service or application and have the correct level of access permissions been applied to ensure that no one can access information or functionality for which there is no business need?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

3.4. Are users prevented from attaching unauthorised devices such as USB sticks, external drives or smart phones to the system or service?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

3.5. Are the system, service or application users prevented from downloading, installing and running unapproved programs and software?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

4. Privileged Access Management

4.1. Do all system administrator roles have individual, unique accounts (not shared accounts)?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

4.2. Is all administration of the system carried out either on site, or across secure, encrypted channels?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

5. Access Control and Password Policy

5.1. Are all users and administrators of the system, service or application holding a minimum BPSS security clearance? https://www.gov.uk/government/publications/government-baseline-personnel-security-standard		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

5.2. Are all users of the system, service or application approved as having a legitimate business requirement before access is granted?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

5.3. Is there a process for removing user accounts which are no longer required?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

5.4. Are passwords either randomly generated, or, if user selected, are the rules on password length and complexity enforced?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

5.5. Are users, including administrators, forced to change their passwords at defined intervals, the recommended maximum expiry period is ninety (90) days?		
☐ **YES**	☐ **NO***	☐ **NOT APPLICABLE***
**Further comments.*		

5.6. Are accounts configured to lock out after a defined number of failed logon attempts?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*
**Further comments.*		

6. User Education and Awareness

6.1. Are all users, including system administrators, made aware of the policy for acceptable use of the system and their personal responsibility to comply with security procedures?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*
**Further comments.*		

7. Backing Up Data and Disaster Recovery

7.1. Is data regularly backed up at intervals appropriate to the business?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*
**Further comments.*		

7.2. Is the SRO satisfied that in the event of a major incident resulting in the complete loss of the system, operation and business functions could be restored within timeframes acceptable to the business?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*
**Further comments.*		

8. Incident Management

8.1. Is there an effective process for reporting of major security incidents which ensures DSU is kept informed?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*

*Further comments.

9. Malware Protection

9.1. Has Anti-Virus software been installed on the system, and is this anti-virus software regularly updated to ensure it remains current?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*
*Further comments.		

9.2. If data is imported into the system, is it scanned for malware / viruses either prior to or on upload of data?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*
*Further comments.		

10. Protective Monitoring

10.1. Are user actions on the system monitored and audit logs generated and retained?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*
*Further comments.		

10.2. Are incoming and outgoing traffic flows monitored and audit logs generated and retained?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*
*Further comments.		

10.3. Are audit logs being reviewed at regular intervals, if so who carries out the review and how often is this completed?		
☐ YES	☐ NO*	☐ NOT APPLICABLE*

*Further comments.

11. Data Encryption

11.1. Is data being encrypted if transmitted across the internet, if so does the encryption method conform, as a minimum, to the FIPS 140-2 standard?

☐ YES	☐ NO*	☐ NOT APPLICABLE*

*Further comments.

11.2. Is data located on hosted servers, databases or outsourced solutions being encrypted, if so does the encryption method conform, as a minimum, to the FIPS 140-2 standard?

☐ YES	☐ NO*	☐ NOT APPLICABLE*

*Further comments.

11.3. Is sensitive personal data and sensitive business data on removable media encrypted, if transferred outside the building, if so how will this be implemented does the encryption method conform, as a minimum, to the FIPS 140-2 standard?

☐ YES	☐ NO*	☐ NOT APPLICABLE*

*Further comments.

12. Home Working

12.1. Do all users who access the system remotely, either from home or other locations, do so using a method approved by the department; such as, a departmental issued laptop, tablet, smart phone or Desktop to Go?

☐ YES	☐ NO*	☐ NOT APPLICABLE*

*Further comments.

13. Testing & Assurance Processes

13.1. Have appropriate levels of IT Health Checks / Penetration testing been carried out, if so has a report and remediation plan been produced and shared with the DSU, have the remediation's been successfully completed?		
☐ **YES***	☐ **NO**	☐ **NOT APPLICABLE**
**The ITHC Report should be referenced here.*		

14. In Service - Security Improvement and Assurance Plan

14.1. An 'In Service - Security Improvement and Assurance Plan should be should implemented to ensure the continued assurance of the system, service or application throughout its life-cycle. The plan shall contain details of the security assurance activity, a task owner appointment of function and frequency of the task.		
☐ **YES***	☐ **NO**	☐ **NOT APPLICABLE**
**The Security Assurance Plan should be referenced here.*		

15. SRO Risk Acceptance Statement *to be signed by Senior Responsible Owner in all cases:*

(insert system / service name here)

As the Senior Responsible Owner for the above named system; I confirm that all exceptions have been documented above and the answers given above are true and accurate.

I am content that the system and my data are being appropriately protected and that any agreed remedial actions will be applied in a timely fashion. I understand that all risks as detailed in the accompanying Residual Risk Statement are owned by me.

Name	Appointment	Signature[1]	Contact Details (Email / Phone)
[Insert Name]	*[Insert Appointment]*	*[Please Sign]*	*[Insert Email & Phone No']*

[1] Note: A signed and scanned copy of the Self-Assessment Questionnaire is required for the document to be accepted.

National curriculum tests

Key stage 2

Science sampling test framework

National curriculum tests from 2016

For test developers

Standards & Testing Agency

2016 key stage 2 science sampling test framework:
national curriculum tests from 2016
Electronic version product code: STA/15/7344/e ISBN: 978-1-78315-828-7

This document is available for download on the GOV.UK website at www.gov.uk/sta.

Contents

1. Overview

This test framework is based on the national curriculum programme of study (2014) for science, introduced for teaching in schools from September 2014 and first assessed in the summer term 2016. The framework specifies the purpose, format, content and cognitive domains of the key stage 2 science sampling tests; it is not designed to be used to guide teaching and learning or to inform statutory teacher assessment.

These tests are used to monitor national standards using pupil-level matrix sampling. This approach uses a largely common set of questions which are securely administered to compare standards over a number of test cycles.

This document has been produced to aid the test development process.

1.1 Purposes of statutory assessment

The main purpose of sample statutory assessment is to estimate national performance in relation to areas of the national curriculum (2014) in science, based on the performance of a sample of pupils.

The main use of the data is to inform schools and other stakeholders about trends in pupils' performance in science.

No information is kept or reported on any school's or pupil's performance on the science sampling assessment.

1.2 Pupil-level matrix sampling

Pupil-level matrix sampling will use a number of different test instruments to assess the science national curriculum (2014). The sampling tests will be securely administered by external assessors to a representative sample of pupils. The exact size of each sample will be determined by the data and reporting requirements.

Matrix sampling, requiring the use of several test instruments, will ensure that there is greater national curriculum coverage in each assessment cycle than if there were a single instrument of assessment. In 2016, pupil-level matrix sampling will assess the 2014 curriculum using paper-based tests.

The pupil-level matrix sampling approach also has scope for monitoring national performance against international benchmarks such as Trends in International Maths and Science Survey (TIMSS). The International Association for the Evaluation of Educational Achievement (IEA) has agreed that a sample of the questions used in the TIMSS survey can be used, which will allow international assessment results to be linked with UK national sample testing.

2. What is a test framework?

The purpose of the test framework is to provide the documentation to guide the development of the tests. The framework is written primarily for those who write test materials and to guide subsequent development and test construction. It is being made available to a wider audience for reasons of openness and transparency.

Some elements of the statutory national curriculum are not possible to assess using the current form of testing; they will need to be assessed by teachers as part of their statutory assessment of the complete national curriculum.

The test framework includes those parts of the programme of study as outlined in the national curriculum (2014) that will be covered in the test (the content domain). The cognitive processes associated with measurement of science are also detailed in the cognitive domain.

The test framework also includes a test specification from which valid, reliable and comparable tests will be constructed each year. This includes specifics about test format, question types, response types, marking and a clear test-level reporting strategy.

By providing all of this information in a single document, the test framework answers questions about what the test will cover, and how, in a clear and concise manner. The framework does not provide information on how teachers should teach the national curriculum.

The test development process used by the Standards and Testing Agency (STA) embeds within it the generation of validity and reliability evidence through expert review and trialling. Given the nature of evidence collected, it is not anticipated that any additional studies will be required to demonstrate that the tests are fit for purpose. The test framework does not provide detail of the validity and reliability of individual tests; this will be provided in the test handbook, which will be published on the DfE's website following the administration of the test.

The test framework should be used in conjunction with the national curriculum (2014) and the annual 'Assessment and reporting arrangements' (ARA) document.

3. Nature of the test

The key stage 2 science sampling test forms part of the statutory assessment arrangements for pupils at the end of key stage 2.

The test is based on the relevant sections of the national curriculum statutory programme of study (2014) for science at key stage 2.

The test will cover the aspects of the curriculum that lend themselves to paper-based, externally marked testing.

The tests will be securely administered in the selected schools by external administrators. Schools will not have access to the test papers after the administration. A set of questions will be made public after each assessment cycle, which schools can use for teaching purposes.

3.1 Population to be assessed

All pupils who are registered at maintained schools, special schools, or academies (including free schools) in England and are at the end of key stage 2 will be eligible to be selected to take part in the key stage 2 science sampling test.

Some pupils are exempt from the tests. Further details will be made available to participating schools.

3.2 Test format

The key stage 2 science sampling test comprises three components, which will be presented to pupils as three separate papers. The test is administered on paper and the total testing time is 75 minutes. There are five different versions for each component and each pupil will be assigned one version of each component. The order of the components will vary for each pupil.

Table 1: Format of the test for each pupil

Component	Description	Number of papers	Number of marks	Approximate timing of component
Test paper b	questions in a biology context	1 (from 5 versions)	22	25 minutes
Test paper c	questions in a chemistry context	1 (from 5 versions)	22	25 minutes
Test paper p	questions in a physics context	1 (from 5 versions)	22	25 minutes
	Total	**3**	**66**	**75 minutes**

4. Content domain

The content domain sets out the relevant elements from the national curriculum programme of study (2014) for science at key stage 2 that are assessed in the science sampling tests. It is intended that all assessable elements of the content domain will be assessed in each administration.

The content domain for biology, chemistry and physics identifies strands of the programme of study that can only be partially assessed in the sampling tests due to the practical nature of those strands. These are marked with an asterisk (*) in Tables 2, 3, 4 and 5 and summarised and explained in Table 6.

To facilitate test development, each strand of the new programme of study has been assigned to one of the three core areas of science: biology, chemistry and physics. The suite of assessments for any one year in which matrix sampling occurs will cover these three core areas in approximately equal measure, even though there are slightly fewer strands for chemistry than there are for biology or physics. In the tables that follow, all the strands from the new programme of study for biology, chemistry and physics are given, as it is possible to assess all areas to some extent with paper-based tests. The 'Working scientifically' content has been described separately but will be assessed within the context of one of the three core areas of biology, chemistry or physics and will therefore always be classified under both areas.

4.1 Content domain for biology

Table 2: Content domain for biology

Topic	Strand from programme of study		Year group
Plants (B)	**B3a**	identify and describe the functions of different parts of flowering plants: roots, stem / trunk, leaves and flowers	**3**
	B3b	explore the requirements of plants for life and growth (air, light, water, nutrients from soil and room to grow) and how they vary from plant to plant*	**3**
	B3c	investigate the way in which water is transported within plants*	**3**
	B3d	explore the part that flowers play in the life cycle of flowering plants, including pollination, seed formation and seed dispersal*	**3**
Living things and their habitats (B)	**B4a**	recognise that living things can be grouped in a variety of ways	**4**
	B4b	explore and use classification keys to help group, identify and name a variety of living things in their local and wider environment*	**4**
	B4c	recognise that environments can change and that this can sometimes pose dangers to living things	**4**
	B5a	describe the differences in the life cycle of a mammal, an amphibian, an insect and a bird	**5**
	B5b	describe the life process of reproduction in some plants and animals	**5**
	B6a	describe how living things are classified into broad groups according to common observable characteristics and based on similarities and differences, including micro-organisms, plants and animals	**6**
	B6b	give reasons for classifying plants and animals based on specific characteristics	**6**
Animals including humans (B)	**B3e**	identify that animals, including humans, need the right types and amount of nutrition, and that they cannot make their own food; they get nutrition from what they eat	**3**

Topic	Strand from programme of study		Year group
Animals including humans (B) (continued)	**B3f**	identify that humans and some other animals have skeletons and muscles for support, protection and movement	3
	B4d	describe the simple functions of the basic parts of the digestive system in humans	4
	B4e	identify the different types of teeth in humans and their simple functions	4
	B4f	construct and interpret a variety of food chains, identifying producers, predators and prey	4
	B5c	describe the changes as humans develop to old age	5
	B6c	identify the main parts of the human circulatory system, and describe the functions of the heart, blood vessels and blood	6
	B6d	recognise the impact of diet, exercise, drugs and lifestyle on the way their bodies function	6
	B6e	describe the ways in which nutrients and water are transported within animals, including humans	6
Evolution and inheritance (B)	**B6f**	recognise that living things have changed over time and that fossils provide information about living things that inhabited the Earth millions of years ago	6
	B6g	recognise that living things produce offspring of the same kind, but normally offspring vary and are not identical to their parents	6
	B6h	identify how animals and plants are adapted to suit their environment in different ways and that adaptation may lead to evolution	6

4.2 Content domain for chemistry

Table 3: Content domain for chemistry

Topic	Strand from programme of study		Year group
Rocks (C)	**C3a**	compare and group together different kinds of rocks on the basis of their appearance and simple physical properties*	**3**
	C3b	describe in simple terms how fossils are formed when things that have lived are trapped within rock	**3**
	C3c	recognise that soils are made from rocks and organic matter	**3**
States of matter (C)	**C4a**	compare and group together materials according to whether they are solids, liquids or gases	**4**
	C4b	observe that some materials change state when they are heated or cooled, and measure or research the temperature at which this happens in degrees Celsius (°C)*	**4**
	C4c	identify the part played by evaporation and condensation in the water cycle and associate the rate of evaporation with temperature	**4**
Properties and changes of materials (C)	**C5a**	compare and group together everyday materials on the basis of their properties, including hardness, solubility, transparency, conductivity (electrical and thermal), and response to magnets*	**5**
	C5b	know that some materials will dissolve in liquid to form a solution, and describe how to recover a substance from a solution	**5**
	C5c	use knowledge of solids, liquids and gases to decide how mixtures might be separated, including through filtering, sieving and evaporating	**5**
	C5d	give reasons, based on evidence from comparative and fair tests, for the particular uses of everyday materials including metals, wood and plastic	**5**
	C5e	demonstrate that dissolving, mixing and change of state are reversible changes*	**5**
	C5f	explain that some changes result in the formation of new materials, and that this kind of change is not usually reversible, including changes associated with burning and the action of acid on bicarbonate of soda	**5**

4.3 Content domain for physics

Table 4: Content domain for physics

Topic	Strand from programme of study		Year group
Light (P)	**P3a**	recognise that they need light in order to see things and that dark is the absence of light	**3**
	P3b	notice that light is reflected from surfaces	**3**
	P3c	recognise that light from the sun can be dangerous and that there are ways to protect their eyes	**3**
	P3d	recognise that shadows are formed when the light from a light source is blocked by an opaque object	**3**
	P3e	find patterns in the way that the size of shadows change	**3**
	P6a	recognise that light appears to travel in straight lines	**6**
	P6b	use the idea that light travels in straight lines to explain that objects are seen because they give out or reflect light into the eye	**6**
	P6c	explain that we see things because light travels from light sources to our eyes or from light sources to objects and then to our eyes	**6**
	P6d	use the idea that light travels in straight lines to explain why shadows have the same shape as the objects that cast them	**6**
Forces and magnets (P)	**P3f**	compare how things move on different surfaces	**3**
	P3g	notice that some forces need contact between two objects, but magnetic forces can act at a distance	**3**
	P3h	observe how magnets attract or repel each other and attract some materials and not others*	**3**
	P3i	compare and group together a variety of everyday materials on the basis of whether they are attracted to a magnet, and identify some magnetic materials*	**3**
	P3j	describe magnets as having two poles	**3**
	P3k	predict whether two magnets will attract or repel each other, depending on which poles are facing	**3**

Topic	Strand from programme of study		Year group
Sound (P)	**P4a**	identify how sounds are made, associating some of them with something vibrating	4
	P4b	recognise that vibrations from sounds travel through a medium to the ear	4
	P4c	find patterns between the pitch of a sound and features of the object that produced it*	4
	P4d	find patterns between the volume of a sound and the strength of the vibrations that produced it*	4
	P4e	recognise that sounds get fainter as the distance from the sound source increases	4
Electricity (P)	**P4f**	identify common appliances that run on electricity	4
	P4g	construct a simple series electrical circuit*, identifying and naming its basic parts, including cells, wires, bulbs, switches and buzzers	4
	P4h	identify whether or not a lamp will light in a simple series circuit, based on whether or not the lamp is part of a complete loop with a battery	4
	P4i	recognise that a switch opens and closes a circuit and associate this with whether or not a lamp lights in a simple series circuit	4
	P4j	recognise some common conductors and insulators, and associate metals with being good conductors	4
	P6e	associate the brightness of a lamp or the volume of a buzzer with the number and voltage of cells used in the circuit	6
	P6f	compare and give reasons for variations in how components function, including brightness of bulbs, loudness of buzzers and on / off position of switches	6
	P6g	use recognised symbols when representing a simple circuit in a diagram	6
Forces (P)	**P5e**	explain that unsupported objects fall towards the Earth because of the force of gravity acting between the Earth and the falling object	5
	P5f	identify the effects of air resistance, water resistance and friction that act between moving surfaces	5

Topic	Strand from programme of study		Year group
Forces (P) (continued)	**P5g**	recognise that some mechanisms, including levers, pulleys and gears, allow a smaller force to have a greater effect	**5**
Earth and space (P)	**P5a**	describe the movement of the Earth, and other planets, relative to the Sun in the solar system	**5**
	P5b	describe the movement of the Moon relative to the Earth	**5**
	P5c	describe the Sun, Earth and Moon as approximately spherical bodies	**5**
	P5d	use the idea of the Earth's rotation to explain day and night and the apparent movement of the sun across the sky	**5**

4.4 Content domain for 'Working scientifically'

'Working scientifically' replaces the area of 'scientific enquiry' in the national curriculum (1999) document. Between 2003 and 2012, 'scientific enquiry' had a major emphasis in the science national curriculum tests and in the science sampling tests, with 40 per cent of all questions in the tests being attributed to strands from this area of the programme of study. In the national curriculum (2014), 'Working scientifically' is considered an integral part of the other three core areas of science and will no longer be assessed as a separate domain. Questions will be integrated within the contexts of biology, chemistry and physics.

The content domain for 'Working scientifically' also includes strands of the programme of study that cannot be assessed or can only be partially assessed in the key stage tests due to their direct association with practical skills or experiences linked to school location. These are marked with an asterisk (*) in Table 5 and summarised and explained in Table 6.

Table 5: Content domain for 'Working scientifically'

Topic	Strand from programme of study		Key stage (lower / upper)
Planning	**WSLa**	asking relevant questions and using different types of scientific enquiries to answer them*	**lower**
	WSUa	planning different types of scientific enquiries to answer questions, including recognising and controlling variables where necessary	**upper**
Carrying out	**WSLb**	setting up simple practical enquiries, and comparative and fair tests*	**lower**

Topic	Strand from programme of study		Key stage (lower / upper)
Measuring	**WSLc**	making systematic and careful observations and, where appropriate, taking accurate measurements using standard units, using a range of equipment, including thermometers and data loggers*	**lower**
	WSUb	taking measurements, using a range of scientific equipment, with increasing accuracy and precision, taking repeat readings when appropriate*	**upper**
Recording	**WSLd**	gathering, recording, classifying and presenting data in a variety of ways to help in answering questions*	**lower**
	WSLe	recording findings using simple scientific language, drawings, labelled diagrams, keys, bar charts, and tables	**lower**
	WSUc	recording data and results of increasing complexity using scientific diagrams and labels, classification keys, tables, scatter graphs, bar and line graphs	**upper**
Concluding	**WSLg**	using results to draw simple conclusions, make predictions for new values, suggest improvements and raise further questions	**lower**
	WSLh	identifying differences, similarities or changes related to simple scientific ideas and processes	**lower**
	WSLi	using straightforward scientific evidence to answer questions, or to support their findings	**lower**
	WSUf	identifying scientific evidence that has been used to support or refute ideas or arguments	**upper**
Reporting	**WSLf**	reporting on findings from enquiries, including oral and written explanations, displays or presentations of results and conclusions*	**lower**
	WSUe	reporting and presenting findings from enquiries, including conclusions, causal relationships and explanations of and degree of trust in results, in oral and written forms such as displays and other presentations*	**upper**
Further work	**WSUd**	using test results to make predictions to set up further comparative and fair tests*	**upper**

4.5 Elements of the curriculum that cannot be assessed fully

The table below provides more detailed information about the strands marked with an asterisk in Tables 2 to 5, which cannot be assessed or can only partially be assessed in a paper-based test due to the more practical nature of the strand. Table 6 describes the aspects of each strand that will be assessed on paper and identifies if there are any aspects that are not assessed at all.

Table 6: Elements of the curriculum that cannot be assessed fully

Content domain reference		Explanation of what is and what is not assessed in the paper-based tests
Years 3-4	Years 5-6	
Living things and their habitats - explore and use classification keys to help group, identify and name a variety of living things in their local and wider environment (B4b)		This requires access to, and interaction with the local environment. Questions about the pupil's wider environment, such as using classification keys to group, name or identify living things could be asked in a paper-based test.
Plants - explore the requirements of plants for life and growth (air, light, water, nutrients from soil, and room to grow) and how they vary from plant to plant (B3b)		Whilst 'exploration' of plants' requirements cannot be done in a paper test pupils' knowledge of the requirements and how they may vary can be tested.
Plants - investigate the way in which water is transported within plants (B3c)		Whilst 'investigation' of water transport in plants cannot be done in a paper test pupils' knowledge of the phenomenon can be tested.
Plants - explore the part that flowers play in the life cycle of flowering plants, including pollination, seed formation and seed dispersal (B3d)		Whilst 'exploration of the roles of flowers cannot be done in a paper test pupils' knowledge of the phenomenon can be tested.

Content domain reference		Explanation of what is and what is not assessed in the paper-based tests
Years 3-4	Years 5-6	
Rocks - compare and group together different kinds of rocks on the basis of their appearance and simple physical properties (C3a)		Because classification is based on observed features of actual rock specimens, pupils should ideally physically handle rock specimens to ascertain the rocks' features. However, classification of rocks can be assessed using secondary data in a paper-based test.
States of matter - observe that some materials change state when they are heated or cooled, and measure or research the temperature at which this happens in degrees Celsius (°C) (C4b)		Parts of this strand would be better assessed during practical investigations. For example, measuring or researching the temperature at which materials change state requires practical work and access to other information sources (such as textbooks and the internet). These skills cannot be fully assessed in a paper-based test. However, questions may be asked that draw upon a pupil's understanding, gained through experience, of heating and cooling materials.
Electricity - construct a simple series electrical circuit, identifying and naming its basic parts, including cells, wires, bulbs, switches and buzzers (P4g)		This requires practical equipment to assess validly. However, the identification, naming and drawing of electrical components and circuits can be assessed in a paper-based test.

Content domain reference		Explanation of what is and what is not assessed in the paper-based tests
Years 3-4	Years 5-6	
Forces and magnets - observe how magnets attract or repel each other and attract some materials and not others (P3h)		Whilst 'observation' of magnets interacting with each other cannot be actually done in a paper test, pupils' knowledge and understanding of the phenomena can be tested. It would be *better* tested in a performance assessment. It is more difficult to test the second part of the strand. We *can* test knowledge of what everyday objects should be attracted if we use commonplace objects, but we need to think very carefully about which objects are referred to in an item. This part of the strand would definitely be better tested in a performance assessment.
Forces and magnets - compare and group together a variety of everyday materials on the basis of whether they are attracted to a magnet, and identify some magnetic materials (P3i)		Because classification is based on observed features of actual everyday materials, pupils should ideally physically handle everyday materials to ascertain the everyday materials' features. However, classification of everyday materials can be assessed using secondary data in a paper-based test.
Sound - find patterns between the pitch of a sound and features of the object that produced it (P4c)		This would be better tested as a performance assessment. However, knowledge of the phenomenon can be assessed in a paper test.
Sound - find patterns between the volume of a sound and the strength of vibrations that produced it (P4d)		This would be better tested as a performance assessment. However, knowledge of the phenomenon can be assessed in a paper test.
Planning - asking relevant questions and using different types of scientific enquiries to answer them (WSLa)		This requires a discursive approach between the pupil and their teacher. Pupils are assessed on their understanding of different types of scientific enquiry, including fair tests, through WSUa in the paper-based test.

Content domain reference		Explanation of what is and what is not assessed in the paper-based tests
Years 3-4	Years 5-6	
Carrying out - setting up simple practical enquiries, and comparative and fair tests (WSLb)		This requires the pupil to use practical equipment, including making measurements and being able to either follow instructions or make decisions about a procedure. This is not possible in a paper-based test.
Using test results to make predictions to set up further comparative and fair tests (WSUd)		The strand would be better assessed in a performance assessment although aspects of it could be assessed in a paper-based tests.
Measuring - making systematic and careful observations and, where appropriate, taking accurate measurements using standard units, using a range of equipment, including thermometers and data loggers (WSLc)		This requires pupils to use actual equipment over a period of time. It also requires pupils to determine when readings should be taken (i.e. to manage their time during a practical activity). Pupils can be assessed on reading measurements from diagrams or photographs of equipment and also using correct units in a paper-based test.
	Measuring - taking measurements, using a range of scientific equipment, with increasing accuracy and precision, taking repeat readings when appropriate (WSUb)	This requires the pupil to use equipment and to determine how and when to take readings. Pupils can be assessed on their understanding of when and why repeat readings need to be taken in a paper-based test.
Recording - gathering, recording, classifying and presenting data in a variety of ways to help in answering questions (WSLd)		This requires the pupil to gather, process and present their own data based on a specific investigative question, which is not possible in a paper-based test. Pupils can be assessed on their ability to use a variety of formats to record specific data provided to them in a test question and use data to answer questions relating to a given investigation in a paper-based test.

Content domain reference		Explanation of what is and what is not assessed in the paper-based tests
Years 3-4	Years 5-6	
Reporting - reporting on findings from enquiries, including oral and written explanations, displays or presentations of results and conclusions (WSLf)		This requires the pupil to have carried out their own investigative work and to present information in ways that are not possible in a paper-based test.
	Reporting - reporting and presenting findings from enquiries, including conclusions, causal relationships and explanations of and degree of trust in results, in oral and written forms such as displays and other presentations (WSUe)	This strand would take too long and some activities (for example, giving a presentation) would not be possible in a test situation. Pupils can be asked to write conclusions, describe and / or explain causal relationships and to provide scientific explanations for a given set of data in a paper-based test.
	Properties and changes of materials - demonstrate that dissolving, mixing and changes of state are reversible changes (C5e)	Whilst 'demonstration' cannot be actually done in a paper test, pupils' knowledge and understanding of the phenomena can be tested. It would be *better* tested in a performance assessment.
	Properties and changes of materials - compare and group together everyday materials on the basis of their properties, including their hardness, solubility, transparency, conductivity (electricity and thermal), and response to magnets (C5a)	Because classification is based on observed or tested properties, pupils need to physically handle materials to do this. Pupils can classify materials based on their properties using secondary data and can be assessed on their understanding of properties of materials in a paper-based test.

5. Cognitive domain

The cognitive domain seeks to make the thinking skills and intellectual processes required for the key stage 2 science sampling test explicit. Each question will be rated against the two strands of the cognitive domain listed in Tables 7 and 8.

The cognitive domain will be used during test development to ensure comparability of demand, as well as difficulty for tests over successive years.

The cognitive domain provides a framework to which the facts, processes and interpretations that need to be tested in science can be matched. It allows broad testing of different aspects of pupils' scientific knowledge, including basic recall (for example, of terminology); interpretation of data; and formulation of original responses to novel scenarios that draw on a broad scientific knowledge and skills base. Items have been grouped as follows:

- items that assess factual knowledge (Knowledge and comprehension)
- items that require pupils to deduce an answer from presented data, or produce an answer based on use of scientific knowledge in a familiar or straightforward context (Application and analysis)
- items that require pupils to select which knowledge is appropriate, and possibly produce an answer that is original and tailored to a specific scenario (Synthesis and evaluation)

The strands used to determine cognitive domain are:

- cognitive complexity
- response strategy

Items will be written for each strand of the programme of study as outlined in the content domain and rated according to the two strands above. As far as possible all strands of the programme of study will be assessed at each rating for both strands. A detailed explanation of each of the two strands follows in sections 5.1 and 5.2.

5.1 Complexity rating

The complexity scale is described in Table 7. Recall of knowledge is considered to place the lowest level of cognitive demand on a pupil in order to answer a question. Evaluation has the highest demand, requiring pupils to demonstrate complex thought processes in order to put forward and argue their reasoning, supported by their knowledge and understanding. There are three ratings within this strand (low to high).

Within the science sampling matrix as a whole, items will cover each rating for cognitive demand. Some strands of the content domain will lend themselves to being assessed at particular ratings for cognitive demand.

Table 7: Cognitive complexity rating scale

Item dimension - complexity	Knowledge and comprehension (low)	Application and analysis	Synthesis and evaluation (high)
The complexity of each component operation or idea and the links between them	Remembers previously learned information and demonstrates an understanding of the facts	Applies knowledge to actual situations, breaks down information into simpler parts and finds evidence to support generalisations	Compiles component ideas into a new whole or proposes alternative solutions. Makes and defends judgements based on evidence
	Recalls or describes simple factual information as required Makes straightforward observations of features or objects Reads or extracts information from simple data sources or text or diagrams	Applies knowledge to given contexts Provides an explanation based on knowledge or simple evidence Identifies patterns in data and makes comparisons Makes predictions based on data given Analyses data sources	Makes links between different sources of evidence or information to provide an explanation Makes inferences and deductions from information given and own knowledge Draws conclusions from evidence and relates to scientific understanding

5.2 Response strategy rating

The response strategy is considered within a scale that ranges from closed or selected response formats to extended response formats. The response strategies are grouped into three ratings for science as shown in Table 8.

Table 8: Response strategy rating scale

	1. Selected response (low)	2. Short constructed response	3. Extended constructed response (high)
The extent to which a candidate is required to devise a strategy for tackling and answering an item	The response format is given in the question information and the strategy for responding is clearly provided	The response format may not be given in the question information but the strategy for how the pupil determines the answer is clearly provided	Pupils are required to construct their own extended response
	Multiple choice, matching item, true / false style, circle, sequencing, ticking cells in a table, selecting correct data from a table, identifying from a key	Short open response items, for example, naming processes, parts, objects and variables Describing, giving one difference, way or reason, completing bar or line graphs	Longer open response items, that are likely to be two lines of writing, for example, describing relationships or providing explanations
		Drawing or completing diagrams by drawing arrows or circuit diagrams	

6. Test specification

This section provides details of each test component and the sampling matrix design as a whole. The test will be administered on paper by external administrators and externally marked.

6.1 Summary of test and matrix design

Overall, a question pool totalling 330 marks will be selected. These questions will be divided into five papers for each content area (biology, chemistry and physics), giving a total of 15 test papers worth 22 marks each.

Each pupil will sit one paper from each content area, giving a total of three papers worth 66 marks.

Pupils will be given 25 minutes to complete each paper. The total testing time will be 75 minutes.

Table 9: Overall format of the item pool

Content area	Number of marks	Number of versions
Biology	110	5
Chemistry	110	5
Physics	110	5
Total	**330**	**15**

Table 10: Format of the test for each pupil

Component	Description	Number of papers	Number of marks	Approximate timing of component
Test paper b	questions in a biology context	1 (from 5 versions)	22	25 minutes
Test paper c	questions in a chemistry context	1 (from 5 versions)	22	25 minutes
Test paper p	questions in a physics context	1 (from 5 versions)	22	25 minutes
	Total	**3**	**66**	**75 minutes**

Each pupil takes three papers: one biology, one chemistry and one physics. Table 11 shows an example of how the different papers will be combined within each of the 15 possible test combinations a pupil could be given: the numbers in the cells represent the version number and the letter in brackets represents the component (biology, chemistry or physics).

Table 11: Matrix design

Combination	Order of administration		
	1st	2nd	3rd
1	1 (b)	6 (c)	11 (p)
2	2 (b)	7 (c)	12 (p)
3	3 (b)	8 (c)	13 (p)
4	4 (b)	9 (c)	14 (p)
5	5 (b)	10 (c)	15 (p)
6	6 (c)	13 (p)	2 (b)
7	7 (c)	14 (p)	3 (b)
8	8 (c)	15 (p)	4 (b)
9	9 (c)	11 (p)	5 (b)
10	10 (c)	12 (p)	1 (b)
11	11 (p)	3 (b)	10 (c)
12	12 (p)	4 (b)	6 (c)
13	13 (p)	5 (b)	7 (c)
14	14 (p)	1 (b)	8 (c)
15	15 (p)	2 (b)	9 (c)

This design may be adapted in each assessment year in order to include other papers of questions for specific purposes, such as TIMSS material and trial material. These materials will form additional papers which will be added to the design.

6.2 Breadth and emphasis

The content and cognitive domains for the science tests are specified in sections 4 and 5. Although each element may not be included within each set of booklets administered to a pupil, the full range of content detailed in this document will be assessed over the full range of booklets. Consolidation of the key stage 1 material is assumed within the

key stage 2 programme of study and therefore, material from key stage 1 may appear within the key stage 2 test. The questions in each test will be placed in approximate order of difficulty. Items within questions are not necessarily in order of difficulty as they need to fit within the context and show a follow through for a storyline (for example, an investigation from planning to conclusion). Where possible, however, easier items are positioned at the start of a question to familiarise pupils with each context.

The following sections show the proportion of marks attributed to each of the areas of the content and cognitive domains, both in the item pool as a whole and in the test administered to each pupil.

6.2.1 Profile of content domain

Questions are designed to be related to one of the three content areas of biology, chemistry and physics. Table 12 shows the proportion of marks in the item pool expected to be related to each of the three core content areas. Each content area will contribute one third of the marks in the item pool.

Table 12: Profile of marks by content area

Content area	Number of marks in item pool	Number of papers in item pool	Number of marks per paper
Biology	110 (33%)	5	22
Chemistry	110 (33%)	5	22
Physics	110 (33%)	5	22
Total in test	330	15	66

In 2016, only elements that are common to the old and new curriculum documents will be assessed from the Year 3-4 content areas.

Within each content area, some items only assess the related strand (in the national curriculum), while other items assess the related strand plus 'Working scientifically'.

Table 13 shows the profile of the 'Working scientifically' strand.

Table 13: Profile of marks assessing 'Working scientifically'

Number of marks in item pool	Minimum number of marks per paper
83–115 (25%–35%)	5

6.2.2 Profile of cognitive domain

Items will be rated in terms of demand against both strands of the cognitive domain (see section 5).

Table 14 shows the expected proportion of marks classified at each level of cognitive complexity within the item pool as a whole. No specific restrictions are placed on the distribution of marks within each individual paper but it is intended that each paper covers a range of items at different levels of complexity.

Table 14: Profile of marks by cognitive complexity

Cognitive complexity	Number of marks in item pool	Percentage of marks in item pool
Knowledge and comprehension	99-165	30-50%
Application and analysis	99-165	30-50%
Synthesis and evaluation	33-99	10-30%

Table 15 shows the expected proportion of marks classified at each level of response strategy within the item pool as a whole. No specific restrictions are placed on the distribution of marks within each individual paper but it is intended that each paper covers a range of different types of item.

Table 15: Profile of marks by response strategy

Response strategy	Number of marks in item pool	Percentage of marks in item pool
Selected response	116-165	35-50%
Short answer	99-149	30-45%
Extended response	50-99	15-30%

6.3 Format of items and responses

All three types of paper (biology, chemistry, physics) contain the same range of item types.

There are two broad formats for item type: selected response and constructed response.

Selected response items, where pupils are required to select a response from a limited range of options, including:

- multiple choice items
- matching items
- true / false items

Constructed response items are where pupils are required to write a short answer on their own. Short answer items and extended response items are both examples of constructed response items.

Short-answer items, where pupils are required to produce a short response and no options have been given. Examples of short answer items include:

- naming an object or process
- completing a sentence with a missing word
- completing a table or chart
- labelling a diagram or key

Extended response items, where pupils are required to construct their own longer response. Examples of extended response items include:

- explanations
- justifications for previous answers
- various elements of planning an investigation
- graphing or describing a data set

6.4 Marking and mark schemes

The test will be externally marked on screen by trained markers.

The tests will be administered securely and kept confidential. Mark schemes will be developed alongside the test materials so that the tests can be marked reliably, however they will not be published.

In each year the science sampling tests are administered in schools, a sample of questions will be published with an accompanying mark scheme.

The mark scheme will give general principles for marking the papers to ensure consistency of marking together with specific guidance for each item.

The mark scheme will provide the total number of marks available for each question and the criteria by which markers should award the marks. Where multiple correct answers are possible, examples of different types of correct answer will be given. Additional guidance will indicate minimally acceptable responses and unacceptable responses, where applicable.

For all questions, the mark schemes will be developed during the test development process and will combine the expectations of experts with examples of pupils' responses obtained during trialling.

For multi-mark questions, the mark scheme will provide details of how partial credit can be awarded.

The mark schemes will contain the following information:

- a content domain reference
- marks – the maximum number of marks for each item in a question
- requirements – for open response items this will include a generic statement describing the type or types of responses that will enable a pupil to gain credit, followed by a number of exemplar responses to indicate the types of answer a pupil may write. For selected response items this will indicate the response required for the pupil to gain credit
- allowable responses – this section will provide exemplars of allowable responses. Allowable responses are minimally acceptable and are usually not as good from a scientific perspective
- additional guidance – this section will give information on response types that are not creditworthy because they are either insufficient or incorrect

6.5 Reporting

Analysis will be undertaken using the combined data from all pupils in the sample in order to produce a scaled score representing the performance of the sample as a whole. The purposes of translating raw scores onto scaled scores for science sampling are twofold:

- Performance can be reported as a whole, having taken into account the varying difficulties of the specific test combinations taken by different pupils.
- Scaled scores retain the same meaning from one year to the next so a particular scaled score reflects the same level of attainment in one year of administration as in the previous, allowing national performance to be compared across years.

Additionally, an estimate of the proportion of pupils who have achieved the required standard on the test will be produced. A standard-setting exercise will be conducted on the first live test in 2016 in order to determine the scaled score needed for a pupil to be considered to have met the standard. This process will be facilitated by the performance descriptor in section 6.7, which defines the performance level required to meet the standard. In subsequent years, the standard will be maintained using appropriate statistical methods to translate performance across a new item pool into scaled scores. The scaled score required to achieve the expected standard will always remain the same.

6.6 Desired psychometric properties

The focus of the outcome of the science sampling model is to provide an estimate of the proportion of pupils nationally who would have achieved the required standards. While it is important to minimise the standard errors of measurement throughout the scale, it is particularly important to do so around the threshold of the expected standard.

6.7 Performance descriptor

This performance descriptor describes the typical characteristics of pupils whose performance is at the threshold for the expected standard at the end of key stage 2. Pupils who achieve the expected standard in the tests have demonstrated sufficient knowledge to be well placed to succeed in the next phase of their education having studied the full key stage 2 programme of study in science. This performance descriptor will be used by teachers to set the standards on the new tests following their first administration in 2016. It is not intended to be used to support teacher assessment since it reflects only the elements of the programme of study that can be assessed in a paper-based test (see the content domain in section 4).

The complete suite of key stage 2 science sampling tests taken in each live sample year includes questions assessing the entire key stage 2 programme of study in the national curriculum (2014) including the 'Working scientifically' strand. Each pupil will only take three tests. It is therefore the aggregated results from the complete test suite that will provide an indication of how pupils are performing in science across England. It is assumed that pupils working at the threshold will be generally secure in the scientific knowledge and skills they acquired at key stage 1.

6.7.1 Overview

Pupils working at the expected standard will be able to engage with all questions within the test. However, they will not always achieve full marks on each question, particularly if they are working at the threshold of the expected standard, or if the question has a high cognitive demand.

Questions will range from those requiring recall of facts to those requiring synthesis and evaluation. There will be a variety of question formats including selected response, short answer and constructed response where no strategy is provided within the question.

Question difficulty will be affected by the scientific content (including the 'Working scientifically' strand) and by the different strands of the cognitive domain, such as question complexity and the extent to which support is given in the question to help pupils identify or construct their response. This should be borne in mind when considering the remainder of this performance descriptor.

The following sections describe examples of the threshold standard, most of which a typical pupil in Year 6 should be able to demonstrate. It is recognised that different pupils will exhibit different strengths, so this is intended as a general guide rather than a prescriptive list. It is also recognised that the topics in the science national curriculum (2014) are described by year group, therefore a topic covered in a discrete year may not be covered again towards the end of key stage 2.

The content in the national curriculum (2014) has been divided up into 'Working scientifically' and the three scientific disciplines. The performance descriptors that follow reflect this.

6.7.2 Working scientifically

Pupils should be able to recall, use and apply their knowledge, understanding and skills in 'Working scientifically' to familiar and unfamiliar contexts. Pupils should be able to (with no order of priority or hierarchy intended):

- recall and use appropriately terminology such as accurate, conclusion, evidence, fair test, method, observe, pattern, prediction, reliable, results, supports (evidence) and variable
- identify the most appropriate approach for answering scientific questions and select the most appropriate equipment and sources of evidence needed for a task
- know when to use different types of scientific enquiry, make careful observations, take accurate measurements or readings using the appropriate units as required and identify when to repeat measurements, if necessary, to ensure given results are reliable
- record, present and interpret data from different sources, using a range of methods, including tables, graphs (bar charts and line graphs), diagrams and keys
- apply their understanding of scientific concepts to draw valid conclusions from data
- use data to make predictions for missing values
- identify or use evidence to support or refute ideas or arguments
- recognise the validity and reliability of evidence and the difference between fact and opinion

6.7.3 Biology

Pupils should be able to recall, use and apply their knowledge and understanding to familiar and unfamiliar contexts. They should draw conclusions, make simple evaluations and synthesise information.

Pupils should be able to (with no order of priority or hierarchy intended) respond to the majority of statements below, but may be less secure in areas that have not been covered since Years 3 or 4:

- recall and use appropriately terminology such as adaptation, circulatory system, classification, consumer, evolution, function, germination, invertebrates, nutrients, pollination, predator, prey, producer, reproduction, seed dispersal and vertebrates
- describe the processes involved in different stages of the flowering plant's life cycle and the function of different parts of flowering plants
- describe how water and nutrients are transported in plants
- compare the requirements of plants and animals to live and grow well
- compare the similarities and differences between the life cycles of different animals (including humans and other mammals, birds, amphibians, and insects)
- describe the functions of parts of the digestive system in animals
- describe the functions of the main parts of the circulatory system (including the transport of nutrients and water) in animals

- describe the functions of the skeleton and muscles in animals
- describe the effects of diet, exercise, drugs and lifestyle on how our bodies function in the long and short term
- construct and interpret food chains; use keys to group, classify or identify living things, and construct simple dichotomous keys
- describe the main characteristics used to group plants, animals and micro-organisms according to the main groups (vertebrates, invertebrates, birds, mammals, reptiles, fish and amphibians) in the classification system
- explain how a change in an environment may have an impact on living things
- identify that there is variation between offspring and between offspring and their parents because of differences in inherited characteristics
- describe how plants and animals have adapted to their environment and how this may have led to their evolution
- describe how living things have changed over time and that fossils provide information about living things in the past

6.7.4 Chemistry

Pupils should be able to recall, use and apply their knowledge and understanding to familiar and unfamiliar contexts. They should draw conclusions, make simple evaluations and synthesise information.

Pupils should be able to (with no order of priority or hierarchy intended) respond to the majority of statements below, but may be less secure in areas that have not been covered since Years 3 or 4:

- recall and use appropriately terminology such as condensation, °C (degrees Celsius), evaporation, filtering, freezing, insoluble, melting, mixture, non-reversible, properties, reversible, solidifying, soluble and solution
- compare the characteristics of different states of matter (solids, liquids and gases)
- describe how materials can change state with reference to temperature, and explain everyday phenomena (including the water cycle) where changes of state occur
- classify and group materials according to properties, such as appearance (for rocks), hardness, solubility, transparency, conductivity and magnetism
- describe the advantages and disadvantages for the uses of everyday materials based on an understanding of their properties using appropriate terminology
- identify and recognise everyday phenomena where dissolving occurs
- describe how to appropriately separate different mixtures of materials, including solutions
- identify and compare reversible and non-reversible changes
- describe in simple terms how fossils are formed
- describe the composition of soil

6.7.5 Physics

Pupils should be able to recall, use and apply their knowledge and understanding to familiar and unfamiliar contexts. They should draw conclusions, make simple evaluations and synthesise information.

Pupils should be able to (with no order of priority or hierarchy intended) respond to the majority of statements below, but may be less secure in areas that have not been covered since Years 3 or 4:

- recall and use appropriately terminology such as air resistance, attraction, conductor, friction, gravity, insulator, newtons (N), opaque, orbit, pitch, repulsion, sphere, translucent, transparent, vibration, voltage, volume and water resistance
- explain how we see other objects (from a single reflection) and represent this in simple diagrammatic form
- explain shadow formation and how the size of shadows may change
- explain how sounds are made and describe how they require a medium to travel through from the source to the ear
- describe how volume can be changed with reference to vibration
- describe how the features of an object determine the pitch of a sound
- describe the shape of bodies (spheres) in the solar system and the movement of bodies in the solar system relative to each other
- explain how day and night, including the apparent movement of the Sun across the sky, are related to the Earth's rotation
- draw or complete a simple series circuit diagram using recognised symbols including straight lines for wires
- explain how changes made to a circuit can affect how it works
- identify and describe the effects of contact and non-contact forces on moving and stationary objects
- describe the effects of magnets on magnets and other materials
- describe how simple pulleys, levers, springs and gears increase the effects of a force

7. Diversity and inclusion

The Equality Act 2010 sets out the principles by which the national curriculum assessment and its associated development activities are conducted. During the development of the tests, STA's test development division will make provision to overcome barriers to fair assessment for individuals and groups wherever possible.

National curriculum tests will also meet Ofqual's core regulatory criteria. One of the criteria refers to the need for assessment procedures to minimise bias: 'The assessment should minimise bias, differentiating only on the basis of each learner's ability to meet national curriculum requirements' (Regulatory framework for national assessment, published by Ofqual 2011).

The end of key stage 2 science sampling test should:

- use appropriate means to allow all pupils to demonstrate their knowledge and skills in biology, chemistry and physics
- provide a suitable challenge for all pupils and give every pupil the opportunity to achieve as high a standard as possible
- provide opportunities for all pupils to achieve, irrespective of gender, disability or special educational need, social, linguistic or cultural backgrounds
- use materials that are familiar to pupils and for which they are adequately prepared
- not be detrimental to pupils' self-esteem or confidence
- be free from stereotyping and discrimination in any form

The test development process uses the principles of universal design, as described in the 'Guidance on the principles of language accessibility in national curriculum assessments' (New language accessibility guidance, published by Ofqual 2012).

In order to improve general accessibility for all pupils, where possible, questions will be placed in order of difficulty. As with all national curriculum tests, attempts have been made to make the question rubric as accessible as possible for all pupils, including those who experience reading and processing difficulties, and those for whom English is an additional language, while maintaining an appropriate level of demand to adequately assess the content. This includes applying the principles of plain English and universal design wherever possible, conducting interviews with pupils, and taking into account feedback from expert reviewers.

For each test in development, expert opinions on specific questions are gathered, for example at inclusion panel meetings which are attended by experts and practitioners from across the fields of disabilities and special educational needs. This provides an opportunity for some questions to be amended or removed in response to concerns raised.

Issues likely to be encountered by pupils with specific learning difficulties have been considered in detail. Where possible, features of questions that lead to construct irrelevant variance (for example, question formats and presentational features) have been considered and questions have been presented in line with best practice for dyslexia and other specific learning difficulties.

7.1 Access arrangements

The full range of access arrangements applicable to key stage 2 assessments as set out in the ARA will be available to eligible pupils as required.

Appendix: Glossary of terminology used in the test framework

cognitive domain	Cognitive processes refer to the thinking skills and intellectual processes that occur in response to a stimulus. The cognitive domain makes explicit the thinking skills associated with an assessment. The cognitive domain, as shown in this framework, also identifies other factors that may influence the difficulty of the questions.
component	A section of a test, presented to pupils as a test paper or test booklet. Some tests may have two or more components that each pupil needs to sit in order to complete the test. The key stage 2 science sampling test comprises three components.
construct irrelevant variance	Construct irrelevant variance is the variation in pupils' test scores that does not come from their knowledge of the content domain. It can result in pupils gaining fewer marks than their knowledge would suggest or lead to the award of more marks than their knowledge alone would deserve. The former can occur, for example, when questions in a mathematics test also unintentionally measure reading ability. The latter often occurs when unintended clues within questions allow pupils to answer correctly without having the required subject knowledge.
content domain	The body of subject knowledge to be assessed by the test.
distribution	The range of possible scaled scores.
domain	The codified definition of a body of skills and knowledge.
item	The smallest unit that can be awarded a mark within a science question.
mark scheme	The document explaining the creditworthy responses or the criteria that must be applied to award the mark for a question in the test.
matrix sampling	A sampling assessment whereby different groups of pupils take different test instruments, which are all linked together in a matrix.
national curriculum	The statutory description of subject knowledge, skills and understanding for a key stage. The key stage 1 and 2 programmes of study are published online at https://www.gov.uk/government/publications/national-curriculum-in-england-primary-curriculum
performance descriptor	Description of the typical characteristics of pupils working at a particular standard. For these tests, the performance descriptor will characterise the minimum performance required to be working at the appropriate standard for the end of the key stage.

question	A group of related items assessing a common context.
raw score	The unmodified score achieved on a test, following marking. In the case of these tests it is the total marks achieved. For example, if a pupil scores 27 out of 60 possible marks, the raw score is 27. Raw scores are often then converted to other measures such as percentile ranks, standardised scores, or grades.
sample	The group of pupils selected to take the test in a given year.
scaled score	A score which has been translated from a raw score onto a score on a fixed, defined scale. This allows performance to be reported on a consistent scale for all pupils, which retains the same meaning from one year to the next. Therefore, a particular scaled score reflects the same level of attainment in one year as in the previous year, having adjusted for any differences in difficulty of the specific tests.
standard	The required level of attainment in order to be classified into a particular performance category.
standard error of measurement	A reliability estimate that allows the user to determine a confidence interval around a test score. It is a measure of the distribution of scores that would be attained by a pupil had that pupil taken the test repeatedly under the same conditions.
standard setting	The process of applying the standard onto a particular test in order to determine the score required for a pupil to be classified within a particular performance category.
test framework	A document that sets out the principles, rationale and key information about the test and contains a test specification.
test specification	A detailed specification of what is to be included in a test in any single cycle of development.
truncate	To shorten by removing ends.

References

Independent review of key stage 2 testing, assessment and accountability (2011), Lord Bew.
www.gov.uk/government/collections/key-stage-2-ks2-testing-review

Standards & Testing Agency

About this publication

Who is it for?

This document is primarily aimed at those responsible for developing the key stage 2 national curriculum test in science sampling. It may also be of interest to schools with pupils in key stage 2 and other education professionals.

What does it cover?

Detailed information to ensure an appropriate test is developed, including the:

- content domain
- cognitive domain
- test specification
- test performance descriptor

Related information

Visit the GOV.UK website at www.gov.uk/sta for all related information.

For more copies

Printed copies of this document are not available. It can be downloaded from the GOV.UK website at www.gov.uk/sta.