An Garda Síochána
Ag Coinneáil Daoine Sábháilte - Keeping People Safe

Oifig Saorála Fáisnéise,
An Garda Síochána, Teach áth Luimnigh,
Lárionad Gnó Udáras Forbartha Tionscail,
Baile Sheáin , An Uaimh,
Contae na Mí.
C15 ND62

www.garda.ie

Freedom of Information Office,
An Garda Síochána, Athlumney House,
IDA Business Park,
Johnstown, Navan,
Co Meath.
C15 ND62

Phone: (046) 9036350

foi@garda.ie

Re: Freedom of Information Request FOI-000548-2025
Request Part-Grant

Dear ,

I refer to your request, dated 29th September, 2025 and received on 30th September, 2025 which you have made under the Freedom of Information Act 2014 (FOI Act) for records held by An Garda Síochána.

Part 1(n) of Schedule 1 of the FOI Act states that An Garda Síochána is listed as a partially included agency *"insofar as it relates to administrative records relating to human resources, or finance or procurement matters"*. Therefore, only administrative records that relate to human resources, finance or procurement shall be considered.

Your request sought:

> *Under the FOI Act 2014, I am seeking the following:*
> - *a copy of any internal audits completed in calendar year 2025.*
>
> *I would prefer to receive this information electronically, ideally in its original electronic format.*
> *If planning to use a sharefile type service, please ensure it does not involve signing up for an account (a step that is not required for a non-personal FOI request).*

I wish to inform you that I have decided to part-grant your request on 28th October 2025. The purpose of this letter is to explain that decision.

1. **Findings, particulars and reasons for decision**

Upon receipt of your request, a search was conducted in Garda Internal Audit Section (GIAS)

and a number of records have been identified in this regard. They have advised that the following Audits have been issued by Garda Internal Audit Service.

- AGS Credit Card Review - Final Report
- Final Report An Garda Síochána ICT Governance Review
- Internal Security Fund 2014 - 2020
- Review of Divisional Continuous Professional Development Units
- Domestic Abuse Risk Evaluation Tool Review

Copies of theses audits are attached herewith except for a copy of Internal Security Fund 2014 – 2020. In accordance with Part 1(n) of Schedule 1 of the FOI Act, a number of redactions have been applied.

PART 1(N) OF SCHEDULE 1

Part 1(n) of Schedule 1 of the FOI Act states that An Garda Síochána is listed as a partially included agency *"insofar as it relates to administrative records relating to human resources, or finance or procurement matters"*. Therefore, only administrative records that relate to human resources, finance or procurement can be considered for release under the Act.

HR records refer to personal records of staff working within An Garda Síochána. They also relate to statistical information in respect of the organisation, e.g. sick leave, discipline, retirements, etc. Financial records relate to the financial expenditure of the organisation, and procurement records relate to the contracting of services and the tendering process associated with same.

Records, or part thereof, which relate to matters other than finance, procurement or human resources are outside the scope of the Act insofar as it relates to An Garda Síochána and cannot be released.

SECTION 37 – PERSONAL INFORMATION

Section 37 of the FOI Act protects the release of personal information into the public domain. Although the Act seeks to promote openness and transparency from public bodies, the Act also requires public bodies to respect the constitutional right to privacy of individuals about whom the public body holds information.

In the case of this request, a number of the records contain references to third parties. These references to third parties consist of the personal information of the third party in particular information in respect of the employment history of these third parties. This third party personal information is information which An Garda Síochána is expected to keep in a confidential manner. I am obliged by the terms of the FOI Act to refuse the release of such information under FOI.

Section 37(1) provides that a public body shall refuse to grant a request if access to the record concerned would involve the disclosure of personal information relating to an individual other than the requester. Personal information is defined by the Act as follows:

2. (1) In this Act—

"personal information" means information about an identifiable individual that, either—

(a) would, in the ordinary course of events, be known only to the individual or members of the family, or friends, of the individual, or
(b) is held by an FOI body on the understanding that it would be treated by that body as confidential,

(iii) information relating to the employment or employment history of the individual,

I am satisfied that parts of certain records relate to third parties, as well as information relating to other individuals who are named in the records. As such, I am satisfied that the records consist of the personal information of these third parties. Accordingly I find that section 37(1) of the Act applies to the records at issue.

Section 37(2) of the FOI Act sets out certain circumstances in which section 37(1) does not apply. I am satisfied that none of those circumstances arise in this case. I am also satisfied that the provisions of Section 37(5) do not apply to these records.

As per section 37 of the FOI Act I have considered the public interest issues which arise in this case and have taken account of the following factors in favour of release:

- Ensuring openness and transparency of organisational functions to the greatest possible extent,
- The public interest in members of the public exercising their rights under the FOI Act,
- That there is more than just a transitory interest by the public in this information,
- The right to privacy is outweighed by the needs of the public.

In considering the public interest factors which favour withholding the records I have taken account of the following:

- Allowing a public body to hold personal information without undue access by members of the public,
- The public interest is not best served by releasing these records,
- That the Organisation can conduct its business in a confidential manner,
- That there is a reasonable and implied expectation that sensitive personal information will remain confidential,
- That there is no overriding public interest that outweighs the individual's right to privacy.

A public interest test was carried out when considering the release of the personal information but having balanced the factors both for and against the release, I decided that the public interest in preserving the personal information and the reasonable expectation that information can be maintained in a confidential manner by An Garda Síochána outweighs the public interest which would be served were the records released to you.

I am refusing the release of the Internal Security Fund 2014 - 2020. This audit relates to the funding of operations by the Garda Security & Intelligence Section. Section 42 of the Act exempts records relating to Security & Intelligence Section from the provisions of the Act. Section 42 is an absolute exemption, and no right of access to Security & Intelligence records exists under the Act.

Restriction of Act

42. *This Act does not apply to—*

(b) a record held or created by the Garda Síochána that relates to any of the following:

(iv) the Security and Intelligence Section;

2. Right of Appeal

In the event that you are not happy with this decision you may seek an Internal Review of the matter by writing to the address below and quoting reference number **FOI-000548-2025.**

Freedom of Information Office, An Garda Síochána, Athlumney House, IDA Business Park, Johnstown, Navan, Co. Meath C15 ND62

Please note that a fee applies. This fee has been set at €30 (€10 for a Medical Card holder). Payment should be made by way of bank draft, money order, postal order or personal cheque, and made payable to Accountant, Garda Finance Directorate, Garda Headquarters, Phoenix Park, Dublin 8.

Payment can be made by electronic means, using the following details:

Account Name: An Garda Síochána Imprest Account
Account Number: 30000302
Sort Code: 951599
IBAN: IE28DABA95159930000302
BIC: DABAIE2D

You must ensure that your FOI reference number (FOI-000548-2025) is included in the payment details.

You should submit your request for an Internal Review within 4 weeks from the date of this notification. The review will involve a complete reconsideration of the matter by a more senior member of An Garda Síochána and the decision will be communicated to you within 3 weeks. The making of a late appeal may be permitted in appropriate circumstances.

Please be advised that An Garda Síochána replies under Freedom of Information may be released in to the public domain via our website at **www.garda.ie** Personal details in respect of your request have, where applicable, been removed to protect confidentiality.

Should you have any questions or concerns regarding the above, please contact the FOI Office by telephone at (046) 9036350.

Yours sincerely,

ASSISTANT PRINCIPAL
PAUL BASSETT
FREEDOM OF INFORMATION OFFICER

28th **OCTOBER, 2025.**

Requester Name:		Audits - AGS Credit Card Review Final Report		File FOI-0000548-2025		
Page No	**Date**	**Description of Document**	**Deletions**	**Relevant Section of FOI Acts**	**Reason for Redaction**	**Decision Maker's decision**
1-2	-	Contents	0			Grant
3-5	-	Executive Summary	1	Part 1(n) Schedule	Out of Scope	Part-Grant
6-8	-	Terms of Reference	1	Part 1(n) Schedule	Out of Scope	Part-Grant
9-16	-	Detailed findings & recommendations	4	Section 37	Personal Information	Part-Grant

An Garda Síochána ("AGS")

Internal Audit of Credit Card Procedures & Processes

Final Report

February 2025

forvis mazars

Contents

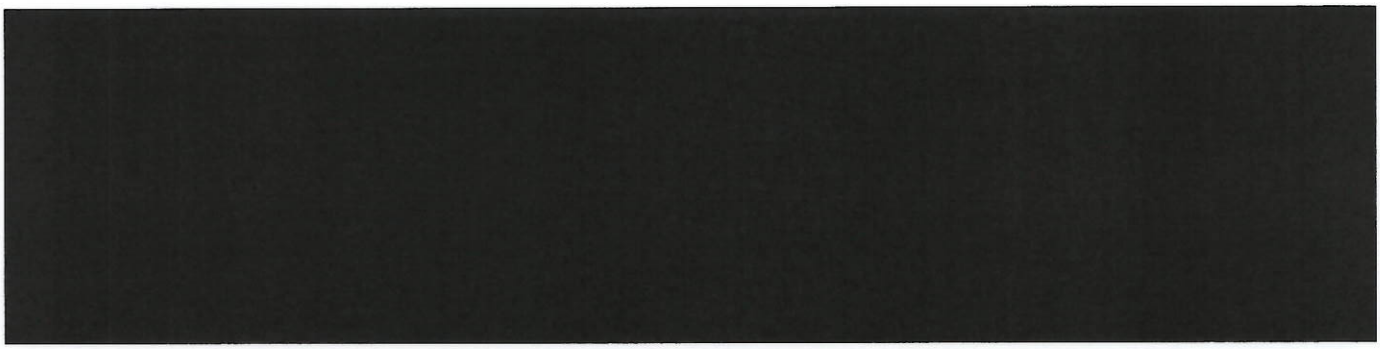
1. Executive summary 3
   1.1 Introduction 3
   1.2 Summary of results 3
   1.3 Audit opinion 4
   1.4 Acknowledgements and limitations 5
2. Terms of reference 6
   2.1 Audit objectives and scope 6
   2.2 Audit approach and methodology 6
   2.3 Reporting arrangements 7
   2.4 Classification of audit opinion 7
3. Detailed findings and recommendations 9

1. Executive summary

Forvis Mazars, in its role as contractors to the Garda Internal Audit Section ("GIAS"), was appointed to complete an Internal Audit to provide assurance to the Head of Internal Audit, GIAS, on the risk management, control and governance processes in operation in relation to Credit Card procedures and processes followed by An Garda Síochána ("AGS"). For each audit, we identify and critically evaluate the framework and controls in place and highlight in our report potential weaknesses that become apparent as a result of our work. We obtain comments and agreed action plan from appropriate management and staff for each weakness identified.

1.1 Introduction

As part of our audit scope, we sought to examine the processes and procedures in place regarding the issuing, utilisation, reconciliation and control of credit cards within AGS. As part of the initial information request issued, Forvis Mazars requested a listing of all credit cards in use during the period under review.



AGS has a policy on credit cards dated January 2018 in place. Internal Audit was informed this document was in use during the period under review. We were also informed that there is a new policy in a draft format that is in the approval process.

1.2 Summary of results

We performed an independent review of the processes and procedures in place regarding the issuing, utilisation, reconciliation and control of credit cards within AGS, ensuring compliance with both internal policies and procedures and a review against best practice.

Our audit identified **one (1) High priority** and **five (5) Medium priority** findings, which are detailed in Section 3.

Our **High priority** finding is in the area of:

3.1 Policies and Procedures, where we identified a number of deficits in the documentation expected.

Our **Medium priority** findings are in the following areas:

3.2 Credit card set up process

3.3 Credit card guidelines and thresholds

3.4 Credit card reconciliation

3.5 Business purpose of credit card expenditure

3.6 Credit card transaction testing

1.3 Audit opinion

In accordance with the classification of audit opinion stated in section 2.4 below, audit results indicate a **Limited Assurance level** i.e. *"Audit results indicate that limited assurance can be placed on the adequacy of and/or operating effectiveness of internal controls to mitigate and/or manage one or more of those key inherent risks to which the activity under review is exposed.*

There is an inadequate and/or ineffective system of governance, risk management and internal control in place and there is a significant risk that the system will fail to meet its objectives.

The disclosure of a number of high and/or medium priority observations is indicative of increased levels of control risk. Prompt management action is required to address these observations together with increased managerial supervision and on-going oversight to ensure controls are being consistently applied and risks are managed effectively"

The following table sets out the number of findings, summarised by priority ranking level:

Priority Ranking	Description	Number of Findings
High	A significant weakness which could compromise internal control and/or operational efficiency, potentially resulting in a substantial error, loss, fraud or damage to reputation. Recommendations related to this observation require management action as a matter of urgency to ensure that the organisation does not continue to be exposed to an unacceptably high level of risk.	1
Medium	A control weakness which can undermine the system of internal control and/or operational efficiency. Recommendations related to this observation should be addressed in the short term to avoid exposing the organisation to significant or increased risk.	5
Low	A weakness which does not seriously detract from the system of internal control and/or operational efficiency, but which should nevertheless be addressed by management to improve internal control in general and ensure good practice. Recommendations related to this observation should be actioned when practicable to enhance the control environment.	0
Total		6

1.4 Acknowledgements and limitations

We would like to thank all those members of management and staff at AGS who assisted us during the course of our review.

Our review was focused on specific areas (as detailed in Section 2.1). Our work, unless otherwise indicated, consisted principally of the review and analysis of information provided to us, discussions with staff and management of AGS, walkthroughs, review of relevant policies and documentation and limited substantive testing (where possible) and may not necessarily disclose all significant matters relating to the current environment within AGS. We have relied on explanations provided to us without having sought to validate these with independent sources. We have, however, satisfied ourselves that explanations received are consistent with other information furnished to us.

The contents of this report should be considered in the context of the following:

- The findings identified have been based on the information provided by AGS.
- Limited substantive testing of the controls which are in place has been conducted, where possible.
- The findings and associated risks identified are not exhaustive and no assurance is provided that additional risks do not exist.
- This review is a point in time indication of the possible gaps which may exist within AGS for the 2023 budget year.

Forvis Mazars assumes no responsibility in respect of or arising out of or in connection with the contents of this report to parties other than to AGS. If others choose to rely in any way on the contents of this report they do so entirely at their own risk.

2. Terms of reference

2.1 Audit objectives and scope

The audit objective was to examine the processes and procedures in place regarding the issuing, utilisation, reconciliation and control of credit cards within AGS. The timeframe covered for this audit was the 2023 budget year.

The review considered the following key objectives on a sample basis:

- Any relevant policies and procedures, roles and responsibilities applicable to the process;
- Procedures around the issuing, cancellation and custody of credit cards, and authorisation of same;
- Credit card expenditure guidelines and thresholds in place;
- Monitoring and reconciliation of credit card expenditure;
- Identification of the business purpose of credit card expenditure, and clarity around any restrictions of use of credit cards;
- Authorisations and supporting evidence maintained in respect of credit card expenditure;
- Process for approval and payment of credit card balances;
- Recording of reconciled credit card transactions in financial systems;
- Adherence to related purchasing and expenses controls when utilising credit cards;
- Segregation of duties between the use, recording, reconciliation and approval of credit cards and credit card transactions.

[redacted]

2.2 Audit approach and methodology

This audit was delivered in line with the GIAS and Forvis Mazars Internal Audit methodology. We performed appropriate work to test whether the appropriate policies, processes, procedures and key controls exist and, if so, have been placed in operation to ensure compliance with the policies and procedures

Planning meetings were conducted initially with the Banking and Income team within the Finance and Services Directorate to obtain a high-level understanding of the applicable processes and procedures. Following the planning phase and agreement of the terms of reference, the review was performed through:

- Meetings with AGS management and staff to gain a detailed understanding of processes and procedures as relevant;
- A review of any documented policies and procedures;
- Review of supporting evidence, information and documentation;
- Sample testing of key operational controls;
- Meetings and discussions with AGS management and staff to verify roles and responsibilities, key decisions, timelines and communications;

- Preparation of a written report documenting our observations and recommendations for improvement as appropriate.

The audit was completed remotely as far as possible, subject to requirements of the various individuals involved in the review, and specific data sharing arrangements that applied.

2.3 Reporting arrangements

Draft findings were discussed in the form of a closing meeting with the key contacts or their nominated liaisons. This meeting discussed the factual accuracy of and risks associated with audit outcomes and documented key recommendations from the review.

Subsequent to the completion of the closing meeting, a draft copy of our report was provided to AGS management within the audit areas, for their review and completion of management responses and actions.

On receipt of final comments, the report was finalised and issued to the Head of Internal Audit, GIAS.

2.4 Classification of audit opinion

The internal audit function will issue an opinion in its reports within the following assurance levels:

Assurance level	Description
Substantial assurance	Audit results indicate that substantial assurance can be placed on the adequacy and operating effectiveness of internal controls to mitigate and/or manage those inherent risks to which the activity under review is exposed. There is a sound system of governance, risk management and framework of internal control in place and the controls are being consistently applied to ensure risks are managed effectively which should ensure that objectives are fully achieved. The absence of high, medium and low priority observations means that normal on-going management supervision, together with the resolution of any enhancement observations raised in the audit report, should ensure that the control risk remains low.
Reasonable assurance	Audit results indicate that reasonable assurance can be placed on the adequacy and operating effectiveness of internal controls to mitigate and/or manage those inherent risks to which the activity under review is exposed. Overall, there is an adequate and effective system of governance, risk management and internal control. While some control risks were identified, this should not significantly impact on the achievement of objectives. The disclosure of some high, medium and/or low priority observations means that normal on-going management supervision, together with the resolution of any findings raised in this report, should ensure that the control risk remains low.
Limited assurance	Audit results indicate that limited assurance can be placed on the adequacy of and/or operating effectiveness of internal controls to mitigate and/or manage one or more of those key inherent risks to which the activity under review is exposed.

Assurance level	Description
	There is an inadequate and/or ineffective system of governance, risk management and internal control in place and there is a significant risk that the system will fail to meet its objectives. The disclosure of a number of high and/or medium priority observations is indicative of increased levels of control risk. Prompt management action is required to address these observations together with increased managerial supervision and on-going oversight to ensure controls are being consistently applied and risks are managed effectively.
No assurance	Audit results indicate that assurance cannot be placed on the adequacy of the and/or operating effectiveness of internal controls to mitigate and/or manage one or more of those key inherent risks to which the activity under review is exposed. The system of governance, risk management and/or internal control has failed or there is a real and substantial risk that the system will fail to meet its objectives. The disclosure of mostly high priority observations in combination with medium priority observations is indicative of an increased control risk. Urgent management action is required to address these observations together with increased managerial supervision and closer on-going oversight to ensure control risks are reduced.

3. Detailed findings and recommendations

Items assigned a **High priority** require **urgent** action, **Medium priority** items require action in the **short term** and items assigned a **Low priority** require action **when practicable**. See section 1.2 for a detailed description of each of the priority ratings assigned.

Findings	Risk and/or implication	Recommendation	Management comment
3.1 Policies and Procedures			Priority: High
As part of the audit scope we sought to review whether policies and procedures document key controls and processes around credit cards in use. We noted that the main document provided titled "Statement of Policy on the use of Official Credit Cards, January 2018" does not appear to be complete. The document including title page is only four pages long. We were informed that the complete document was not available. We were also advised that a new policy document is in draft format and is awaiting approval, and without such approval could not be provided to us for review. Additionally, the new draft document was not in use during the period under review. We noted that the 2018 policy document does not address or describe the following procedures: - Number of credit cards - Lost / Stolen credit cards - Suspected fraud on the card - Cancelled credit cards	In the absence of documented policies and procedures roles and responsibilities, key controls and processes may not be understood or performed. In the absence of periodic review, information in the policies and procedures may not reflect actual practices or requirements.	We recommend the following: • The policy is updated to include the relevant procedures as listed in the findings section, including number of credit cards, lost / stolen credit cards, suspected fraud on cards, cancelled credit cards); • The policy should clearly specify the allowable expenditure and the process for ensuring personal expenditure is remitted to AGS; • The policy should specifically prohibit cash withdrawals on all credit cards as they incur a daily interest charge; • The policy should stipulate that credit cards cannot be used to override purchases or procurement controls;	Management Comment: Accepted New Credit Card policy for AGS is currently under internal Finance review. Agreed Action: Revised AGS Credit Card policy to be introduced in 2025 subject to Senior Management Board approval Completion Date: Q3 2025 Responsibility: Finance Directorate

Findings	Risk and/or implication	Recommendation	Management comment
- Eligible credit card expenditure (the policy states that credit cards are for official use only, however, it does not specify what are official expenses) - Process for handling ineligible credit card expenditure We also noted that it is not clear from the policy that: a. Credit cards cannot be used for personal expenditure (the policy, however, mentions that gratuities should not exceed 10% of the value of the transaction (page 3) and that personal cheques should be made by the cardholder for any personal expenditure, tips and gratuities (page 4). b. The policy does not specify the process for ensuring that transactions are reviewed to ensure that personal expenditure (including gratuities) is returned to AGS. c. Credit cards cannot be used to make cash withdrawals - the screenshot of the online banking provided for one of the credit cards in use during 2023 shows there was a limit of 260 EUR per day for ATM withdrawals. It should be noted that cash withdrawals on credit cards incur daily interest charges therefore the use of credit cards for cash withdrawals in not recommended. d. Credit cards cannot be used to override controls for approving purchases or procurement which would have to be adhered to under the AP cycle.		• The policy should include version control and be reviewed/updated and approved every 12/24 months;	

Findings	Risk and/or implication	Recommendation	Management comment
We note the document does not include version control which details date of approval, approver name and document owner. In addition, the policy has not been updated since 2018 where the policy and procedure document should be reviewed every 12/24 months.			
3.2 Credit Card Set Up Process			**Priority: Medium**
As part of the audit we reviewed on a sample basis a process of credit card set up, to ensure compliance with documented policies. From the review we found the following: 1. The policy requires an applicant to issue a request in writing to the Executive Directorate of Finance and Services who would obtain the approval of the Chief Administrative Officer. The evidence of this step was not provided to us as part of the testing. We were advised that the only evidence for credit card set up is the Credit Card agreement signed by the cardholder (this is considered a request) and the Garda Commissioner (this is considered the Commissioner's approval). 2. No paperwork was provided for two out of three samples tested – this we were advised was due to the cardholders no longer working in AGS.	Non-compliance with documented credit card policy. Excessive number of credit cards in use. Due to lack of awareness, Cardholders do not comply with credit card policy in terms of appropriate usage.	We recommend the policy is updated to include credit card set up process description, including the reason for the credit card requirement. And that documentation is retained and an appropriate audit trail is kept for all credit cards requested and set up. We also recommend that each cardholder is required to confirm in writing that they understand the cards are for business purpose only and will comply with the credit card policy.	Management comment: Accepted Credit Card setup process to be internally reviewed in line with new AGS Credit Card policy. Agreed action: Revised AGS Credit Card policy to be introduced in 2025 subject to Senior Management Board approval Completion date: Q3 2025 Responsibility: Finance Directorate

Findings	Risk and/or implication	Recommendation	Management comment
3. The policy does not specify that cardholders are required to confirm in writing that they understand and will comply with the credit card policy in terms of appropriate usage.			
3.3 Credit Card Guidelines & Thresholds			**Priority: Medium**
As part of the audit we reviewed the credit card guidelines and thresholds. We found that the number of credit cards in use and the justification for card limit is not documented in the policy. We were advised that credit card limits exist depending on the role of the cardholder but this is not documented. However, we have not seen any approved calculation or determination that would underpin the credit card thresholds in use for difference roles.	Credit card guidelines and thresholds are not in place to provide sufficient guidance to users.	We recommend the policy is updated to include clearly defined credit card limits for each role. The policy should clearly define the basis for determination of the calculation of these thresholds.	Management comment: Accepted Agreed action: To be outlined in the new AGS Credit Card policy. Completion date: Q3 2025 Responsibility: Finance Directorate
3.4 Credit Card Reconciliation			**Priority: Medium**
We tested a sample of nine (9) monthly reconciliations across the various credit cards held to ensure compliance with the process described in the policy. We found the following: - There is no evidence the cardholders certify that the expenditure was necessarily incurred in an official capacity;	Credit card statement is not reconciled to identify ineligible expenditure.	We recommend as per the documented policy, evidence of receipts is attached by the cardholders to the Credit Card Statements, or explanation provided if receipts are not available	Management comment: Accepted Action plan Agreed action: The credit card process was reviewed in 2024 and monthly reconciliations are now

Findings	Risk and/or implication	Recommendation	Management comment
- There is no evidence all relevant receipts were attached by the cardholders to the Credit Card Statements, or explanation provided if receipts were not available; - There is no evidence of any personal cheques made payable to AGS for personal expenditure. However due to lack of supporting documentation we could not identify whether any personal expenditure existed. - We requested evidence of review to ensure the cost centres were correct and assigned accurately. We were provided with evidence of five (5) Finance District reports being sent to Financial Shared Services. We note these reports are stamped "approved for" with a signature attached. We were not provided with evidence for the four other samples. - Two of these reports were not dated, however, additional evidence attached to one of the reports (emails) confirms the date of preparation of that report. - We note one report states it's for period ended 31/10/2022, however it refers to period ended 31/10/2023. We also found the policy does not document the timing of the preparation of the reconciliation, the need to sign and date the reconciliation prepared and the need for independent review of the prepared reconciliation.	Non-compliance with credit card policy. Expenditure not assigned to the correct cost centres.	We recommend the policy includes the requirement for independent review of all credit card statements and reconciliations to ensure that the expenditure was necessarily incurred in an official capacity and are assigned correct cost centers. We also recommend that the policy documents the timing of the preparation of the reconciliation and the need to sign and date the reconciliation prepared.	being performed. Completion date: Q1 2025 Responsibility: Finance Directorate

Findings	Risk and/or implication	Recommendation	Management comment
3.5 Business Purpose of Credit Card Expenditure			**Priority: Medium**
As part of the audit we reviewed the policy and found it is not clear from the policy what expenditure is considered official use. Even though the policy states the approval is required for all expenditure, it does not specify who the approval should be obtained from and how to treat the expenditure where no approval was obtained.	Risk that expenditure is not appropriate.	We recommend the policy is updated to include allowable expenses. The policy should clearly define the reasonable / legitimate business purpose of expenditure and include an approval matrix for the expenditure.	Management comment: Partially Accepted. A listing of all allowable expenses including approval matrix per expenditure cannot be provided due to unexpected events which may arise due to AGS responsibility for carrying out all policing duties in the Irish State. Agreed Action: Revised AGS Credit Card policy to be introduced in Q3 2025 subject to Management approval Completion Date: Q3 2025 Responsibility: Finance Directorate

Findings	Risk and/or implication	Recommendation	Management comment
3.6 Credit Card Transaction Testing			**Priority: Medium**
As part of the audit we tested a sample of the credit card transactions across all credit cards that were in use during 2023. The policy states that "when expenditure is incurred by the cardholder the appropriate approval must be obtained in all cases" - however, no evidence of approval has been provided for the samples tested. The policy is vague in terms of allowable expenses - for that reason we can't confirm if the expenditures tested are in line with the policy and for reasonable / legitimate business purpose. Invoice and/or receipt has not been provided for 9 out of 42 sampled transactions. The total value of missing invoices is €902.33.	Risk that expenditure is not reasonable / legitimate business purpose.	We recommend that the policy requires cardholders to keep and / or provide all receipts to the Finance Directorate to ensure an appropriate audit trail and to allow for the review of the expenditure to ensure it is reasonable / for a legitimate business purpose.	Management comment: Accepted Agreed action: The credit card process was reviewed in 2024 and all receipts are now being collated. Completion date: Q1 2025 Responsibility: Finance Directorate

[redacted]
Partner
[redacted]@mazars.ie

[redacted]
Director
[redacted]@mazars.ie

Forvis Mazars in Ireland is a leading international audit, tax, advisory and consulting firm. Operating as a united partnership, Forvis Mazars works as one integrated team, leveraging expertise, scale and cultural understanding to deliver exceptional and tailored services in audit, assurance, tax, consulting, financial advisory, corporate finance and financial outsourcing. With 38 partners and 800+ staff based in Dublin, Galway, Limerick and Cork, the Irish firm draws on the expertise of more than 40,000 professionals in over 100 countries to assist major international groups, SMEs, private investors and public bodies at every stage in their development.

forvismazars.com/ie

Requester Name:		Audit - CPD Units Report	File FOI-0000548-2025			
Page No	**Date**	**Description of Document**	**Deletions**	**Relevant Section of FOI Acts**	**Reason for Redaction**	**Decision Maker's decision**
1-2	-	Contents	0			Grant
3	-	Executive Summary	0			Grant
4-5	-	Terms of Reference	0			Grant
6-11	-	Observations and Agreed Actions	0			Grant

Garda Internal Audit Service

Review of Divisional Continuous Professional Development Units

Final Internal Audit Report

May 2025

Contents

1.	**Executive Summary**	3
1.1	Summary of Observations	3
1.2	Audit Assurance Level	3
1.3	Acknowledgements and Limitations	3
2.	**Terms of Reference**	4
2.1	Audit Objective	4
2.2	Audit Scope and Methodology	4
2.3	Reporting Arrangements	4
2.4	Ranking of Observations	4
2.5	Classification of Audit Assurance Levels	5
3.	**Observations and Agreed Actions**	6
3.1	Strategic Planning	6
3.2	Annual Planning	7
3.3	Quantity of Courses Delivered	8
3.4	Resource Numbers	9
3.5	Resource Records	10
3.6	Training Records	11

1. Executive Summary

Continuous Professional Development (CPD) is the process by which professionals undertake learning activities to develop and enhance their abilities.

The Commission on the Future of Policing in Ireland found, in 2018, that An Garda Síochána had no professional development strategy and recommended that such a strategy be developed.

A stated strategic outcome for An Garda Síochána in the latest Strategy Statement was that Garda personnel would have the appropriate training, information and supports they need to succeed in their role.

The current Programme for Government commits to training new recruits to An Garda Síochána annually.

Divisional Continuous Professional Development Units (CPD Units) are Garda units based in each Division that undertake training and professional development for Divisional Garda personnel.

While the Chief Superintendent, Director of Training & CPD is agreed as the Responsible Person for the specific agreed actions, it is understood that any systemic restructuring of Divisional CPD Units is not within the remit of the Chief Superintendent.

1.1 Summary of Observations

We made four high priority observations, relating to

- strategic planning for the Divisional CPD Units
- annual planning for the Divisional CPD Units
- the quantity of courses delivered by the Divisional CPD Units; and
- Garda resources at Divisional CPD Units.

1.2 Audit Assurance Level

In accordance with the classification of audit opinion in Section 2.5 below, our results indicated an **unsatisfactory assurance level**, i.e. *"The system of governance, risk management or control has substantial weaknesses that need to be addressed urgently."*

The assurance level was deemed limited due to the lack of coordinated planning and inconsistency of resourcing and number of courses delivered across the Divisional CPD Units.

1.3 Acknowledgements and Limitations

We would like to thank all Garda personnel who assisted us during the course of this review, in particular the Leadership, Management and Professional Development team in Garda College, and members attached to Divisional CPD Units around the country.

Our review focused on specific areas, as detailed in Section 2. Our procedures consisted primarily of the review and analysis of information provided to us, discussion with Garda personnel and management, walkthroughs of relevant processes, review of relevant policies and documentation, and limited substantive testing where required.

Our work may not necessarily disclose all significant matters relating to the implementation of key actions to mitigate against risks identified. We have relied on explanations provided to us and satisfied ourselves that these explanations are consistent with other information provided to us.

2. Terms of Reference

2.1 Audit Objective

The objective of this engagement was to review the effectiveness of Divisional Continuous Professional Development Units' planning and training delivery structures.

2.2 Audit Scope and Methodology

The scope of our work was informed by a risk assessment and involved a review of the following areas:

- Strategic planning,
- Annual planning for 2023,
- Resources attached to Divisional CPD Units' and
- Records associated with Divisional CPD Units.

We reviewed information provided to us, held meetings with Garda personnel and management, performed walkthroughs of relevant processes, reviewed relevant policies and documentation and undertook substantive testing where required.

We have relied primarily on the information disclosed in the Internal Control Questionnaires (ICQs) by the Divisional CPD Units. The ICQs were tailored for this review to capture key qualitative and quantitative information, and we had 90% a response rate.

Our testing was designed to provide reasonable assurance that expected processes are in place and functioning as expected.

2.3 Reporting Arrangements

This report will be issued to:

- Commissioner
- Deputy Commissioner, Security, Strategy, and Governance
- Deputy Commissioner, Policing Operations
- Chief Corporate Officer
- The Audit Committee

2.4 Ranking of Observations

Priority Ranking	Description	Number of Observations
High	Major issues that we consider need to be brought to the attention of senior management.	4
Medium	Important issues which should be addressed by management in their areas of responsibility.	2
Low	Detailed issues of a minor nature that can be resolved with limited time and effort.	0

2.5 Classification of Audit Assurance Levels

Audit Assurance Level	Description
Adequate	Overall there is an adequate system of governance, risk management or control.
Limited	There are weaknesses within the governance, risk management or control framework which need to be addressed.
Unsatisfactory	The system of governance, risk management or control has substantial weaknesses that need to be addressed urgently.

3. Observations and Agreed Actions

4. Observation	Risk / Potential Implication	Agreed Actions
3.1 Strategic Planning		High
There is no strategic planning process undertaken to prioritise Divisional CPD Unit's efforts, to effectively allocate resources, or to align the goals of the Divisional CPD Units with those of An Garda Síochána.	Without an agreed intended direction for the Divisional CPD Units there may be unclear prioritisation of efforts, ineffective resource allocation, and a lack of alignment with organisational strategic goals, resulting in Garda personnel not getting the required learning, training and professional development.	The risk associated with the lack of a joined up strategic plan for the Divisional CPD Unit's will be formally communicated to Executive Director, Human Resources and People Development. This communication will include the proposal that the management of Divisional CPD Units, and the development of a coordinated strategic plan for the Divisional CPD Units, should come under the remit of the Director of Training & CPD within 2025. **Responsible Person:** Chief Superintendent Director of Training & CPD **Implementation Date:** Q3 2025

Observation	Risk / Potential Implication	Agreed Actions
3.2 Annual Planning		High
There was no formal annual planning process undertaken by the Divisional CPD Units for the period reviewed, including no planning for, or calculation of, abstraction rates.	A key strategic enabler for An Garda Síochána for the period under review was to enhance the organisational capacity to provide appropriate HR, training, learning and development supports. Without a plan to set out how these objectives were to be achieved, the method of achieving them is not clear, and it is not possible to determine if the objectives have been successful.	In line with the Action at 3.1, the Director of Training & CPD will formally communicate to Executive Director, Human Resources and People Development the risks associated with a lack of annual planning within the Divisional CPD Units, along with a proposal that, as soon as possible, the Director of Training & CPD should be exclusively responsible for a coordinated planning process across all the Divisional CPD Units. **Responsible Person:** Chief Superintendent Director of Training & CPD **Implementation Date:** Q3 2025

Observation	Risk / Potential Implication	Agreed Actions
3.3 Quantity of Courses Delivered		**High**
The number of courses delivered for the period reviewed varied widely across the Divisional CPD Units. There was also a wide variance between the proportion of all courses delivered by Divisional CPD Units that related to probationer / trainee training.	Without a consistent approach to the quantity of courses expected to be delivered by Divisional CPD Units, these Units may be operating inefficiently and ineffectively.	In line with the Action at 3.2, the Director of Training & CPD should, as soon as possible, determine the annual course delivery objectives for Divisional CPD Units. **Responsible Person:** Chief Superintendent Director of Training & CPD **Implementation Date:** Q3 2025

Observation	Risk / Potential Implication	Agreed Actions
3.4 Resource Numbers		High
There is no internal guidance as to the optimum level of staffing for the Divisional CPD Units. Member numbers allocated to CPD Units vary widely across Divisions. Differences also exist in the ratio of CPD Unit members to both Garda members and trainees / probationers across the Divisions.	Without a methodology for determining the optimum staffing level for Divisional CPD Units there is a possibility that the quality and quantity of HR, training, learning and development is inconsistent across the organisation.	In line with the Actions at 3.1 and 3.2, the Director of Training & CPD will formally communicate to Executive Director, Human Resources and People Development the risks associated with the lack of a Divisional CPD Unit resourcing methodology that give appropriate consideration to the strategic and operational objectives of Divisional CPD Units. **Responsible Person:** Chief Superintendent Director of Training & CPD **Implementation Date:** Q3 2025

Observation	Risk / Potential Implication	Agreed Actions
3.5 Resource Records		Medium
Discrepancies exist between the actual number of members attached to Divisional CPD Units and the number as recorded on the Garda Employee Management System (GEMS).	Without an accurate central record of the number of Garda members attached to Divisional CPD Units there is a possibility that incorrect information is used by decision makers when making important decisions.	The Principal Officer with responsibility for the Garda HR Directorate will be formally communicated with and informed of the risk associated with poor HR data quality for the management of Divisional CPD Units. A request should be made to the Principal Officer for assurance over the standard of HR data quality, to include details of regular reconciliations undertaken by the HR Directorate. **Responsible Person:** Chief Superintendent Director of Training & CPD **Implementation Date:** Q3 2025

Observation	Risk / Potential Implication	Agreed Actions
3.6 Training Records		**Medium**
There is an inconsistent understanding in Divisional CPD Units as to the requirements for recording training on the central Garda Educational Training System (GETS).	Without an accurate and consistent recording process for Garda personnel training there is a possibility that centrally recorded "single source of the truth" information is incorrect.	Updated guidelines for the recording of information on GETS, to include the creation of appropriate key controls, will be created and communicated appropriately across the organisation. **Responsible Person:** Chief Superintendent Director of Training & CPD **Implementation Date:** Q3 2025

Requester Name:		Audit - Domestic Abuse Risk Evaluation Tool Review		File FOI-0000548-2025		
Page No	**Date**	**Description of Document**	**Deletions**	**Relevant Section of FOI Acts**	**Reason for Redaction**	**Decision Maker's decision**
1-2	-	Contents	1	Part 1(n) Schedule 1	Out of Scope	Part-Grant
3-4	-	Executive Summary/Terms of Reference	2	Part 1(n) Schedule 1	Out of Scope	Part-Grant
5-8	-	Observations & Agreed Actions	3	Part 1(n) Schedule 1	Out of Scope	Part-Grant

Garda Internal Audit Service

Domestic Abuse Risk Evaluation Tool Review

Final Internal Audit Report

November 2024

Contents

1. Executive Summary 3

1.1 Summary of High Priority Observations 3

1.2 Audit Assurance Level 3

1.3 Acknowledgements and Limitations 3

2. Terms of Reference 3

2.1 Audit Objective 3

2.2 Audit Scope and Methodology 3

2.3 Reporting Arrangements 4

2.4 Ranking of Observations 4

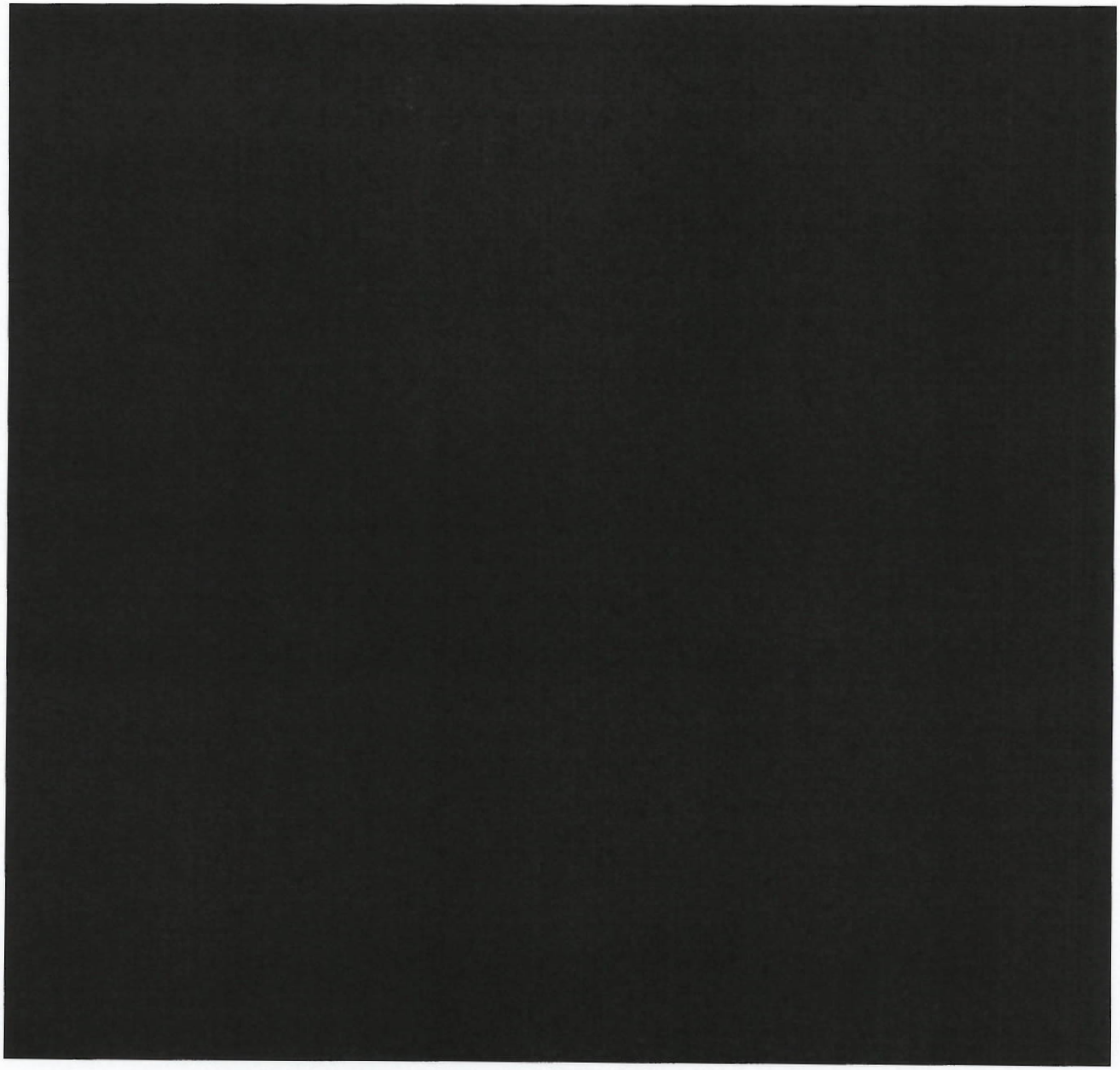
2.5 Classification of Audit Assurance Levels 4

3. Observations and Agreed Actions 5

3.1 Domestic Abuse RET Training & Guidance 5

[redacted]

1. Executive Summary



2. Terms of Reference

2.3 Reporting Arrangements

This report will be issued to:

- Commissioner
- Deputy Commissioner, Security, Strategy, and Governance
- Deputy Commissioner, Operations
- Chief Corporate Officer
- The Audit and Risk Committee

2.4 Ranking of Observations

Priority Ranking	Description	Number of Observations
High	Major issues that we consider need to be brought to the attention of senior management.	0
Medium	Important issues which should be addressed by management in their areas of responsibility.	3
Low	Detailed issues of a minor nature that can be resolved with limited time and effort.	1

2.5 Classification of Audit Assurance Levels

Audit Assurance Level	Description
Adequate	Overall there is an adequate system of governance, risk management or control.
Limited	There are weaknesses within the governance, risk management or control framework which need to be addressed.
Unsatisfactory	The system of governance, risk management or control has substantial weaknesses that need to be addressed urgently.

3. Observations and Agreed Actions

Observation	Risk / Potential Implication	Agreed Actions
3.1 Domestic Abuse RET Training & Guidance		**Medium**
An online training course (Domestic Abuse – Risk Evaluation) exists on the Garda Learning Management System (LMS). To date, not all Garda members who are required to undertake the course have completed the training. A review of the guidance available for the completion of the Domestic Abuse RET identified some inconsistencies.	If a member has not completed the mandatory training, it could lead to incorrect use of the Domestic Abuse RET.	GNPSB will liaise with the Garda College and the Strategic Transformation Office to request that quarterly information focused on improving training rates is provided to each Regional Office. GNPSB will undertake a one off review of RET Online Training and RET Procedure Guide, identify any discrepancies, and determine which version is correct. On the next occasion that incorrect version is being updated the incorrect element is corrected. **Responsible Person:** Detective Chief Superintendent, Garda National Protective Services Bureau **Implementation Date:** Q1 2025

Observation	Risk / Potential Implication	Agreed Actions
[redacted]		

Observation	Risk / Potential Implication	Agreed Actions
[redacted]		

Observation	Risk / Potential Implication	Agreed Actions
[redacted]		

Requester Name:		Audit - Final Report AGS ICT Governance Review		File FOI-0000548-2025		
Page No	**Date**	**Description of Document**	**Deletions**	**Relevant Section of FOI Acts**	**Reason for Redaction**	**Decision Maker's decision**
1-2	-	Contents	1	Part 1(n) Schedule 1	Out of Scope	Part-Grant
3-9	-	Overview	19	Part 1(n) Schedule 1	Out of Scope	Part-Grant
10-11	-	Scope of Review & Outcome	4	Part 1(n) Schedule 1	Out of Scope	Part-Grant
12-18	-	Detailed Findings & Recommendations	7	Part 1(n) Schedule 1	Out of Scope	Part-Grant
19	-	Appendix 1 - Statement of Responsibility	5	Part 1(n) Schedule 1, Section 37	Out of Scope, Personal Information	Part-Grant
20	-	Appendix 2 - Risk Grading	0	Part 1(n) Schedule 1	Out of Scope	Part-Grant
21	-	Appendix 3 - Audit Assurance Level	0	Part 1(n) Schedule 1	Out of Scope	Part-Grant
22-23	-	Appendix 4 - ICT Structure	1	Part 1(n) Schedule 1	Out of Scope	Part-Grant

Deloitte.

An Garda Síochána

Final Report Review of Information & Communication Technology (ICT) Governance

February 2025

Deloitte.

Contents

1.	Overview	3
2.	Scope of review and Outcome	10
3.	Detailed findings and recommendations	12
Appendix 1: Statement of Responsibility		19
Appendix 2: Risk Grading		20
Appendix 3: Audit Assurance Level		21

[redacted]

Deloitte.

1. Overview

1.1. Introduction

This report presents the results of a review of Information and Communication Technology (ICT) Governance for An Garda Síochána (AGS). [redacted]

The objectives for this review are set out in **Section 2.**

1.2. Overview

[redacted]

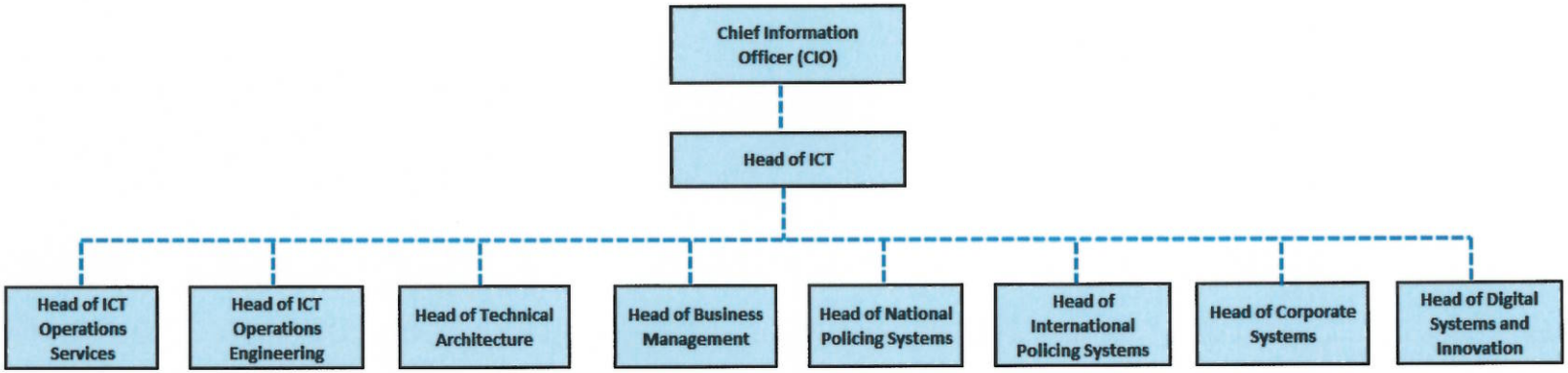
Roles & Responsibilities of the ICT team within AGS

[redacted]

ICT is under the remit of the Chief Information Officer (CIO), who in addition to ICT is responsible for Data Architecture, the Garda Information Services Centre (GISC), the An Garda Síochána Analysis Service (GSAS), the National Data Protection Office (DPO), and the National Vetting Bureau (NVB). The CIO reports to the AGS Chief Corporate Officer (CCO) on ICT matters.

ICT is overseen by the ICT Director, with nine distinct functions reporting to the Director per the ICT organisational structure which was updated in August 2024. The diagram below reflects the current structure at the time of this review with eight Heads of Functions in place. [redacted]

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.



ICT Strategy for An Garda Síochána (AGS)

[redacted]

In support of this principal, the Data and Technology Vision for information-led Policing was developed as a high-level ICT strategy within AGS. This vision is also noted as a key enabler in the AGS Strategy Statement 2022 - 2024.

There are six strategic themes outlined in the vision statement, data culture, quality service delivery, empowered workforce, agility and innovation, standards-based approach, and trusted partnerships.

[redacted]

3. ***Empowered workforce*** to focus on investing in the ICT workforce to develop the data and technology skills required to provide an information-led policing service.

[redacted]

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

[redacted]

Four enablers are also outlined to support implementation of the vision, leadership capabilities, skills development, workforce enablement and collaboration.

1. ***Leadership capability*** to focus on building technology and data leaderships skills internally to drive decision-making, ensuring the knowledge remains in house and achieving the optimal balance of permanent and contracted ICT personal.
2. ***Skills development*** to focus on developing a continuous professional development framework for Data and Technology personnel.
3. ***Workforce enablement*** to focus on digitising corporate services to support Garda personnel & implement an effective recruitment process to find the right data and technology talent.

[redacted]

[redacted]

ICT Prioritisation Roadmap

The ICT Prioritisation Roadmap captures all ICT projects currently ongoing or in the pipeline for commencement of work. All ICT projects in the roadmap are categorised into strategic themes which include:

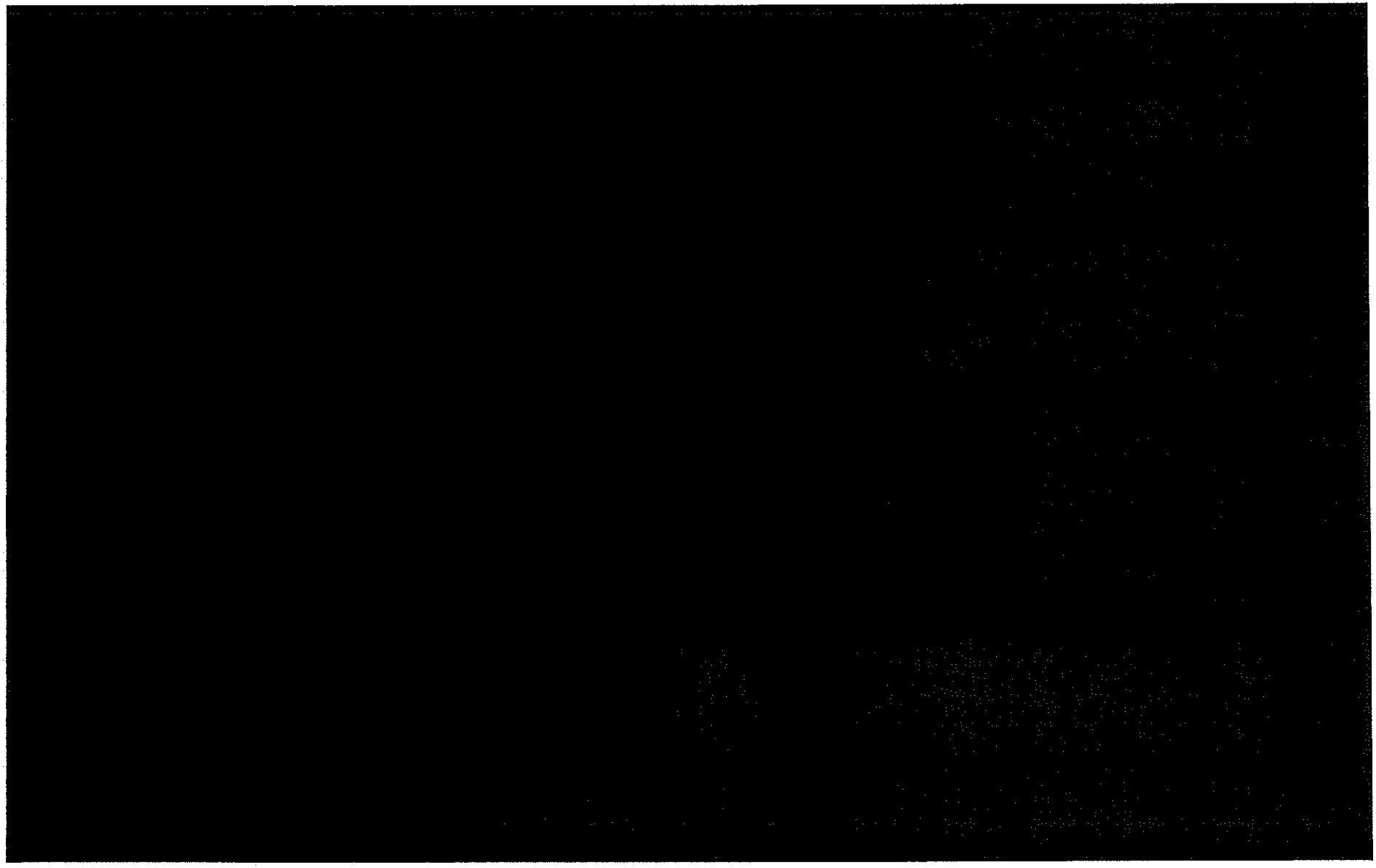
[redacted]

Human Resource (HR) Transformation - ICT projects which support the delivery of Human Resource (HR) ICT solutions to support HR transformation agenda.

[redacted]

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.



This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

[redacted]

ICT Budget

The ICT budget is set annually, after which this is allocated to ICT projects and Business as Usual (BAU) activities. ICT spending is tracked monthly against budget, based on data extracted from the finance system. AGS ICT are required to adhere to the Department of Public Expenditure and Reform Circular 14/2021 - Arrangements for Oversight of Digital and ICT-related Initiatives in the Civil and Public Service. This requires for start and end of year submissions to the Department of Public Expenditure and Reform, submitting requests for specific sanction for new projects to the Digital Government Oversight Unit, and engaging with the peer review process for major ICT projects.

AGS ICT utilise both full time ICT employees and vetted external contractors to deliver on ICT projects and BAU activities; this headcount for ICT resources is tracked on an ongoing basis, including the ICT team breakdown across full time employees and external contractors as well as the breakdown across ICT functions.

[redacted]

Acknowledgement

We extend our thanks to the staff and management of AGS ICT with whom we worked with during the course of this review.

We appreciate the level of co-operation, courtesy and time made available to us throughout the review.

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

1.3. Approach

To complete this engagement, we used a combination of the following:

- An initial planning meeting to agree the scope, objectives, timing and conduct of the audit.
- Review of relevant AGS documentation.
- Discussions with key contacts to obtain an up to date understanding of the ICT Governance processes in place, including the CCO, CIO, Director of ICT, Head of Business Management, Assistant Principal of Business Management, and the Head of the Garda Risk Management Unit.
- Close out meetings with the key audit contacts to discuss any matters arising and to verify the accuracy of our understanding and findings.

Our sole source for information has been management information and representations. We do not accept responsibility for such information and have not performed any substantiation or external confirmation procedures to establish its accuracy.

Our work was performed in accordance with the Deloitte Internal Audit Methodology which is consistent with the standards of the Chartered Institute of Internal Auditors. Our work was carried out during September and October 2024.

1.4. Report Rating

We have set out our overall report rating below. This rating provides an overall view on the in-scope areas reviewed as part of this engagement. Rating definitions are outlined in **Appendix 3.**

Rating Level	Description
Limited	There are weaknesses within the governance, risk management or control framework which need to be addressed.

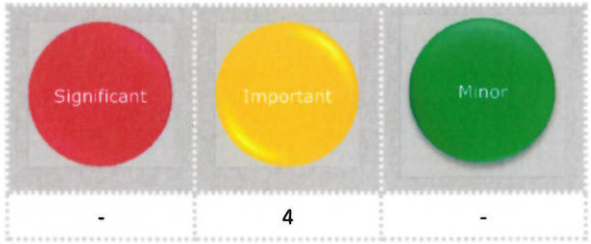
This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

1.5. Summary of findings

In **Section 3** we have set out our detailed findings and recommendations arising from our review. Our findings have been graded using the scale outlined in **Appendix 2.**

The number of findings by risk grade can be summarised as follows:



There were no **significant** findings identified during our review.

There were 4 **important** findings identified during our review. These can be summarised as follows:

[redacted]

2. Absence of detailed tracking for resource and staff time allocation on individual projects (see **Section 3.2**).

[redacted]

4. Lack of a detailed technical ICT training plan and ICT skills matrix (see **Section 3.4**).

Full details of the issues may be found in **Section 3** of this report.

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

2. Scope of review and Outcome

The scope of this internal audit was to examine the sufficiency of ICT governance structures in place within AGS. This internal audit took a holistic top-down approach to examining ICT governance processes, considering the organisations overarching ICT structure and practices.

Assessment of the below objectives was performed against industry standards including ISO/IEC 38500 *Information Technology – Governance of IT for the Organisation* and COBIT 5 *Framework for the Governance and Management of Enterprise IT*.

We set out hereunder a summary of the review objectives, outcomes, and any references to observations.

Review Objectives	Outcome	Observation Ref.
[redacted]		
2. Roles, responsibilities, and accountabilities are established and enforced for information requirements, data, and system ownership.	A new ICT organisational structure was developed in August 2024 which splits ICT in nine functions, with each function lead reporting directly to the Director of ICT. The remit of each function has been documented. However, it was noted that there is no formally documented ICT skills matrix or technical ICT learning plan in place for the current and future needs of the AGS ICT. Skills development is noted as a key enabler of the Data and Technology Vision for information-led policing. [redacted]	**Section 3.3 and 3.4**

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

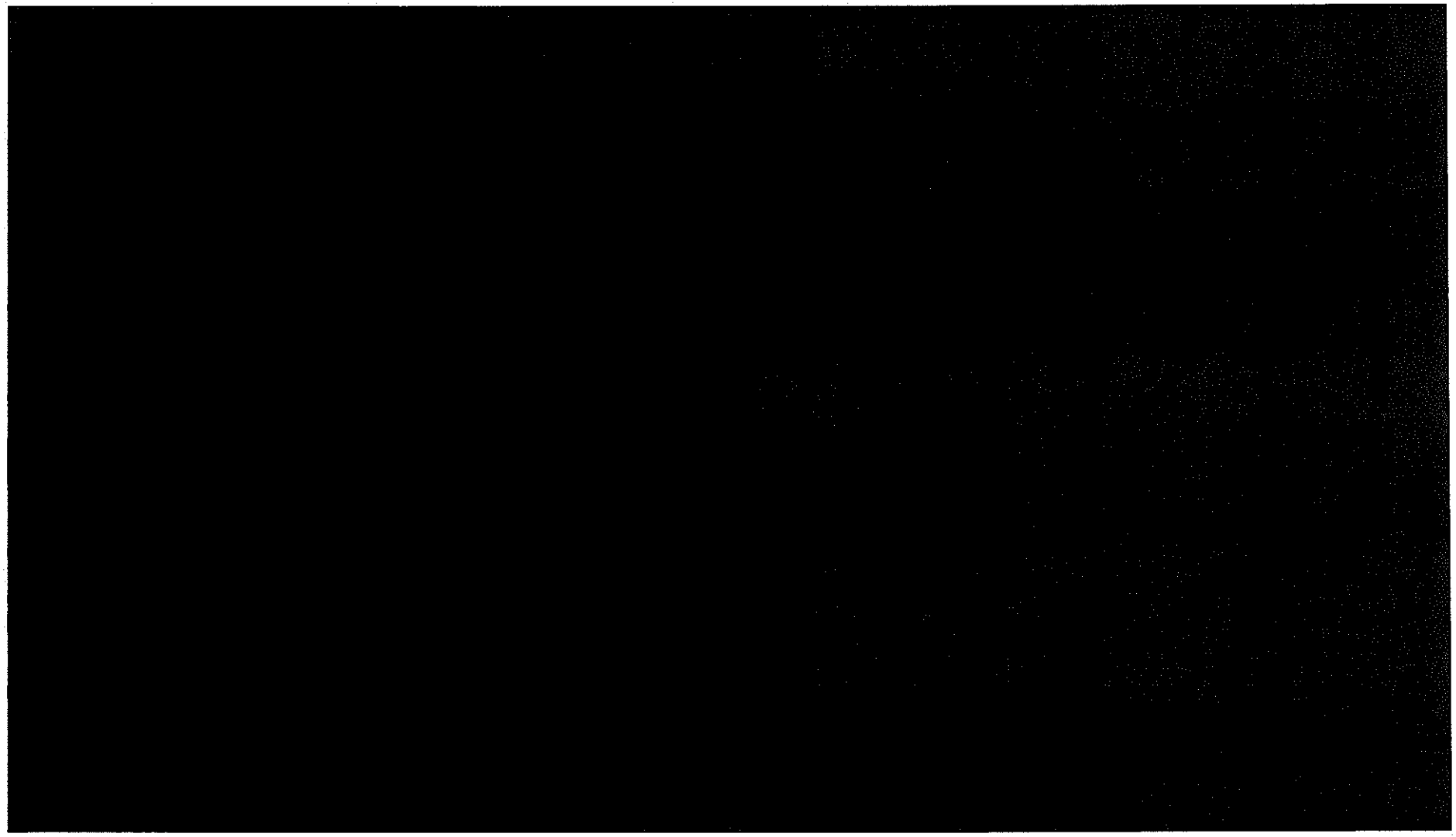
Deloitte.

Review Objective	Outcome	Observation Ref.
[redacted]		
4. Senior leadership have a clear understanding of ICT costs and how they contribute to the achievement of the organisation's strategic objectives	The ICT budget is set annually, after which this is allocated to ICT projects and Business as Usual (BAU) activities. ICT spending is tracked monthly against budget, based on data extracted from the finance system. It was noted that while ICT resource numbers and overall utilisation is recorded, there is no tracking of individual ICT resources at a project level.	**Section 3.1**
[redacted]		

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

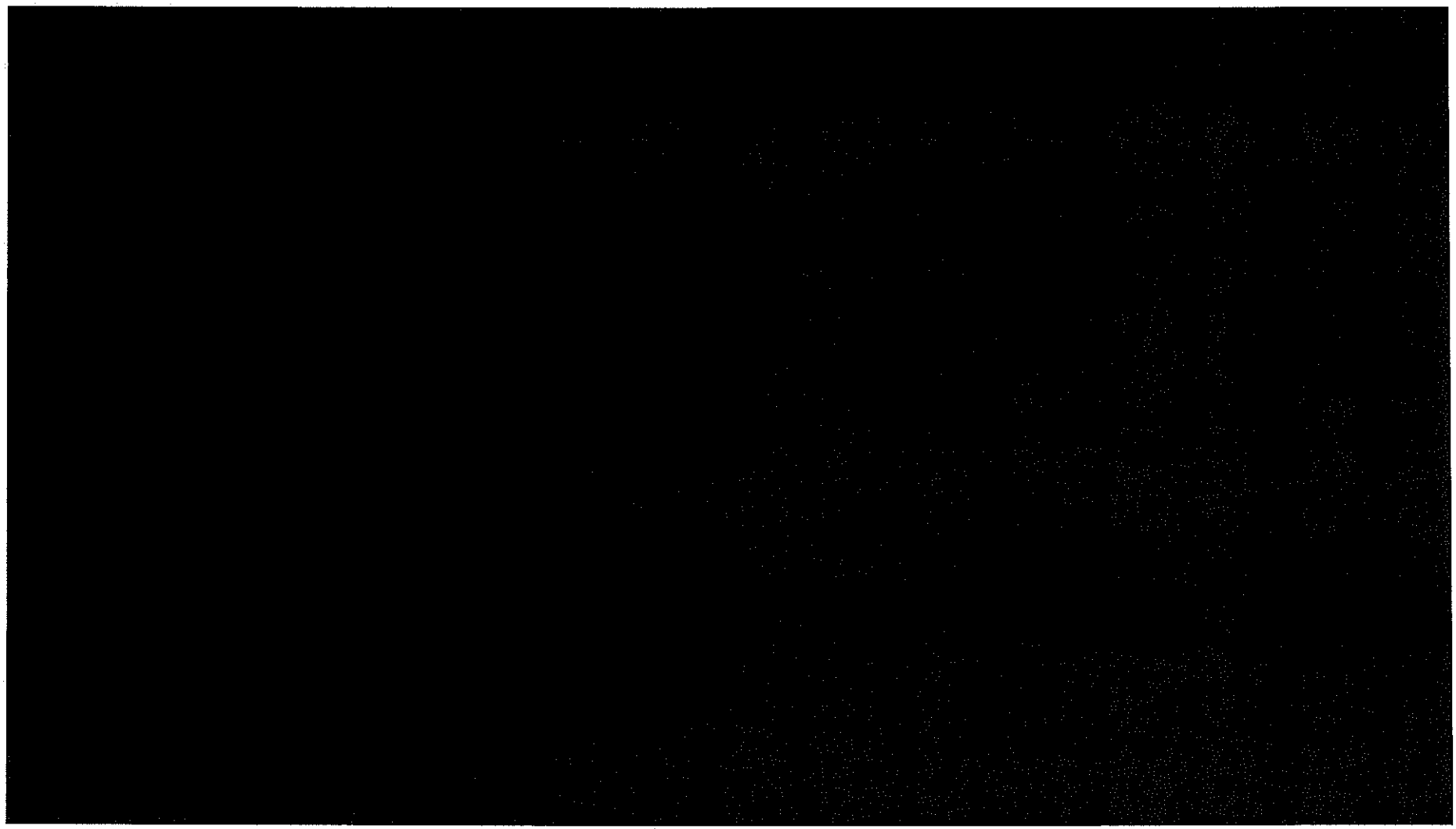
Deloitte.

3. Detailed findings and recommendations



This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.



This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

3.2 Absence of Detailed Tracking for Resource Time Allocation on Individual Projects

Finding	Recommendation	Priority
1. Currently, the tracking of ICT resource time spent on individual projects is not performed. This lack of detailed tracking results in limited visibility into the specific contributions of resources to each project, making it challenging to accurately assess resource allocation and individual resource spend and contribution. This applies to tracking time on ICT projects for both full time and contractors. While budgets take into consideration the total number of days required for projects or Business As Usual (BAU) activities, it is not possible to analyse the breakdown of the time and cost at an individual level. **Potential Impact** • Without time tracking, it is challenging to understand the actual capacity of the team, making it difficult to plan and allocate resources effectively. • Lack of individual project time tracking data can hinder the ability to make informed, data-driven decisions regarding project management and resource allocation.	1. At the time of the review AGS ICT were in the process of implementing a tool that will support the tracking of ICT resources and staff time spent on individual ICT projects. To ensure success of this tool, ICT should: • Develop Time Tracking Policies and Procedures: Establish clear policies and procedures for time tracking. Define what activities need to be tracked, how time should be recorded, and the frequency of time entry (e.g., daily, weekly). • Train Employees: Provide training to all employees on the importance of time tracking and how to use the selected tool. Ensure that employees understand the policies and procedures and the benefits of accurate time tracking. • Monitor and Enforce Compliance: Regularly monitor time tracking compliance and address any issues promptly. Implement checks and balances to ensure that time entries are accurate and complete. • Utilise Time Tracking Data: Use the data collected from time tracking to improve project management. Analyse the data to identify trends, allocate resources more effectively, and make informed decisions regarding project timelines and budgets. • Review and Improve: Periodically review the time tracking system and processes to ensure they remain effective.	

Management response		
Action Plan	**Owner/ Title**	**Target Date of Implementation**
1. The EPPM application referred to in Section 3.1 includes a resource utilisation module. This module will be implemented and adopted for all projects across ICT. The implementation of this module will address the recommendation above.	Head of ICT Business Management	Q2 2025

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

3.3 Linking Open Positions to Specific Risks and Project Fulfilment Challenges

Finding	Recommendation	Priority
At the time of this review, several key staffing positions within ICT were vacant. These positions include, but are not limited to, a [redacted] Quality Assurance Manager, and Innovation & Future Systems Manager. Roles and responsibilities of the vacant positions were being performed, where possible, by other members of the ICT team, in addition to their own day-to-day job responsibilities. However, several key ICT management positions were unfilled at the time of this review. It was noted that while some of the vacant positions were actively being recruited for, other positions were pending sanctioning before an active recruitment process could be initiated to fill the positions. **Potential Impact** Vacant IT positions may result in operational inefficiencies and risks which may include: • Increased workload on existing IT staff, leading to burn out or decreased productivity. • Delays in IT project implementation and system maintenance; and • Heightened risk of security breaches due to inadequate monitoring and response capabilities.	1. Staffing issues will inevitably arise; however, it is imperative that certain roles, such as those in [redacted] are filled swiftly. [redacted] To support in providing clear rational to senior leadership tasked with approving such roles ICT should establish a clear rationale for their resourcing needs, explicitly linking these requirements to specific project resource demands or skillset gaps or ICT risk. 2. In addition, AGS ICT should regularly conduct workforce planning to anticipate future staffing needs and support with identifying potential gaps proactively. This should involve analysing current workforce capabilities and forecasting future requirements.	Important

Management response		
Action Plan	**Owner/ Title**	**Target Date of Implementation**
1. A strategic workforce plan for ICT was developed in 2021, incorporating three phases of workforce growth to address capability and capacity gaps. Phase 1 has been approved, and Phase 2A to address immediate gaps in [redacted] has been submitted for approval. This WFP will be presented to the CCO in parallel with addressing immediate priorities for [redacted]	Director of ICT	Q1 2025

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

2.	The business case for the remainder of Phase 2 of the WFP will be completed and submitted for review by all stakeholders.	Head of ICT Business Management	Q3 2025
3.	Review external contract personnel across all teams in conjunction with available budget and priority of BAU and project activities. If required, submit business case for additional funding	Head of ICT Business Management	Q1 2025

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

3.4 Development of a technical ICT training plan and ICT skills matrix

Finding	Recommendation	Priority
At present, AGS ICT does not have a dedicated training budget to ensure the technical and specialist skills of resources are maintained in line with team progression and industry developments. Limited training is delivered to AGS ICT by the Garda Training College, but this training focuses more on soft skills and limited technical skills. Specific technical trainings can be provided separate to trainings provided by the Garda Training College on an ad-hoc basis however there is no formal training plan in place for the ICT department. Further, AGS ICT does not maintain an ICT skills matrix, outlining the technical capabilities and expectations for team members. As AGS ICT employs a large contractor base, there is a risk of higher rates of staff turnover leading to the loss of systems knowledge. **Potential Impact** • Without a structured training plan, employees may lack the necessary skills to perform their roles effectively, leading to decreased productivity and efficiency. • A lack of ongoing training can stifle innovation, as employees may not be exposed to new technologies, methodologies, or industry best practices. • Without a skills matrix, it may become challenging to identify gaps in the team's skill set, leading to inefficiencies and potential project delays.	1. It is recommended that AGS ICT develop a comprehensive annual technical training plan to ensure that all personnel possess the necessary skills and knowledge to perform their roles effectively. This includes conducting regular skills assessments, identifying training needs, and providing ongoing professional development opportunities to keep up with technological advancements and industry best practices. The training plan should be developed in addition to training provided currently by the Garda Training College and should focus on specific technical skills required across the nine functions within AGS ICT. 2. It is further recommended that AGS ICT should assess the current ICT skillset within the ICT department to create a matrix of the current skills and competencies maintained within the team. The skills operated by Contractors should also be assessed as part of this exercise. Contractors often possess specialised knowledge and skills that are not always transferred to permanent staff. When they leave, this expertise goes with them, creating a knowledge gap.	

Management response		
Action Plan	**Owner/ Title**	**Target Date of Implementation**
1. Carry out a skills requirement analysis for all AGS ICT functions to identify the learning requirements for all AGS teams	Head of ICT Business Management	Q2 2025

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

2.	Perform a skills gap analysis of all personnel within each function, and identify & prioritise learning needs	Each Head of ICT Function	Q3 2025
3.	Liaise with Garda College and ICT management to identify and implement suitable mechanisms for learning plans.	Head of ICT Business Management	Q3 2025

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

Appendix 1: Statement of Responsibility

[redacted]

[redacted]

For and on behalf of
Deloitte Ireland LLP
Chartered Accountants
Deloitte & Touche House
29 Earlsfort Terrace
Dublin 2

Date: 11 February 2025

Partner: [redacted]
Director: [redacted]
Manager: [redacted]
T: 01 417 2200

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

Appendix 2: Risk Grading

Risk Grade	Definition	Required Escalation
	**Internal control** Major control weakness or issue that has potential for: • Significant damage to An Garda Síochána's reputation; • Significant financial loss or loss of value for money; • Significant operational disruption; • Non-compliances with legislative and regulatory requirements; and • Significant inefficiency costing senior management time. Approval of Board to accept Risk Exposure. Findings of this nature will need Board approval if no management action is to be taken to ensure that the Board has explicitly accepted the risk exposure.	Highest level of risk assessed. Management action required and communication to the Audit Committee and Board.
	**Internal control** Important control weakness or issue that has potential for: • Adverse impact to reputation; • Financial loss or loss of value for money; • Operational disruption; and • Inefficiency costing senior management time. Approval of appropriate senior management to accept Risk Exposure if no management action is to be taken.	Moderate level of risk requiring management action and reporting to Executive Director responsible for business areas and the Audit Committee.
	**Internal control** Control improvements required or strengthening of the areas risk management/ control culture. Minor control deficiency or non-compliance identified.	Low level of risk requiring senior management of the business area to consider cost/ benefit of implementing control to cover risk.

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

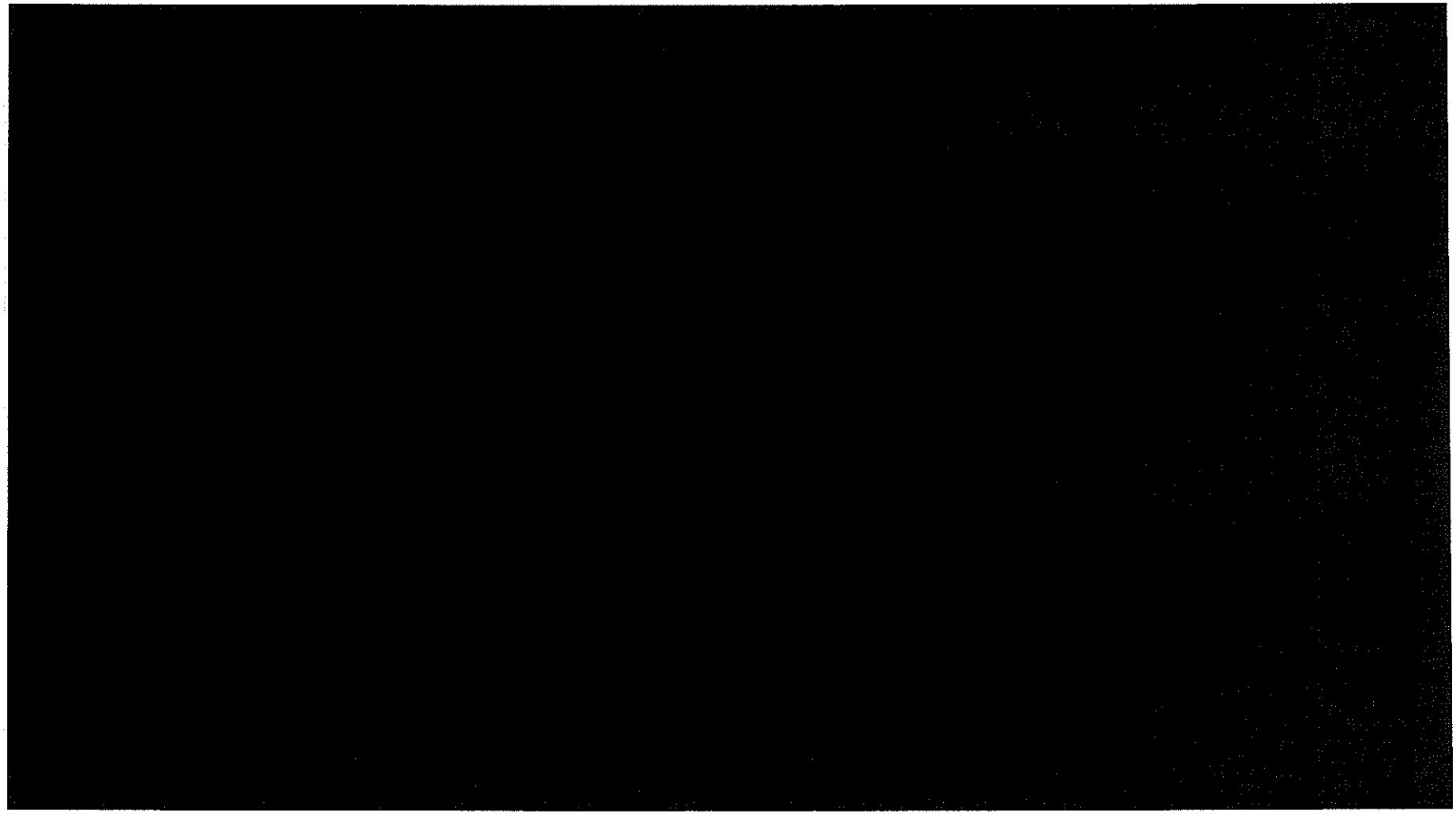
Deloitte.

Appendix 3: Audit Assurance Level

Audit Assurance Level	Description
Adequate	Overall, there is an adequate system of governance, risk management or control.
Limited	There are weaknesses within the governance, risk management or control framework which need to be addressed.
Unsatisfactory	The system of governance, risk management or control has substantial weaknesses that need to be addressed urgently.

This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.



This report is intended solely for the information and internal use of An Garda Síochána and should not be used or relied upon by any other person or entity.

Deloitte.

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with over 415,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has over 3,000 people providing audit, tax, consulting, corporate finance financial advisory, and risk advisory services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience, and insight to collaborate with clients taking them wherever they want to go.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte Ireland LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte Ireland LLP is a limited liability partnership registered in Northern Ireland with registered number NC001499 and its registered office at The Ewart, 3 Bedford Square, Belfast, BT2 7EP, Northern Ireland.

Deloitte Ireland LLP is the Ireland affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

The Deloitte Ireland LLP privacy notice is available at www.deloitte.ie/privacy

© 2025 Deloitte Ireland LLP. All rights reserved.