TransGrid

Critical Infrastructure Security Costs

Operating Expenditure Requirements

Operational Technology Environment & Physical Security

Document Control					
Revision no:	0	**TRIM No:**	D2021/01486	**Approval/ Reviewed date:**	July 2021
Business process:	Maintain			**Document type:**	Report
Author:	Adam Hoare | Digital Infrastructure Asset Manager | Network Planning & Operations				
Reviewers:	Andrew McAlpine | Asset Systems & Compliance | Network Planning & Operations Braam Broodryk | A/Corporate Security Officer | Corporate Services				
Approver:	Lance Wee | Head of Asset Manager | Network Planning & Operations				

Contents

1. Executive Summary 4

1.1 Introduction 4

1.2 Operational Technology Environment - Options Evaluated 4

1.3 Physical Security - Options Evaluated 5

2. Operational Technology Cyber Security Requirements 6

2.1 Relevant Critical Infrastructure Bill Requirements 6

2.2 Key Initiatives 6

2.3 Options 8

3. Physical Security Requirements 10

3.1 Critical Infrastructure Bill Requirements 10

3.2 Key Initiatives 10

3.3 Options 11

Appendix A – Method of Salary Band Usage 12

Appendix B – Resource Calculations 13

List of Tables

Table 1: OT key initiatives 6

Table 2: AESCSF linkage to key initiatives 7

Table 3: Initiative OPEX requirements (5 years) 8

Table 4: Physical security key initiatives 10

Table 5: Salary bands 12

Table 6: Junior and senior resource costs 12

Table 7: OT resource costs per initiative (per annum) 13

Table 8: Physical security resource costs per initiative (per annum) 14

Table 9: Resource basis per initiative 14

Table 10: Physical security resource costs per initiative (per annum) 15

Table 11: Resource basis per initiative 15

List of Figures

No table of figures entries found.

1. Executive Summary

1.1 Introduction

The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Bill) was introduced to parliament on 10 December 2020. This bill proposes to extend the scope of the Security of Critical Infrastructure Act 2018 (CI Act) to cover critical infrastructure in a wider range of sectors including: communications, financial services and markets, data storage or processing, defence industry, higher education and research, energy, food and grocery, health care and medical, space technology, transport, and water and sewerage.

The Commonwealth Department of Home Affairs (Department) recently concluded a public consultation on a proposal to introduce an enhanced regulatory framework that increases the security and resilience requirements of Australia's critical infrastructure. As part of this framework, we expect the Department will impose new regulatory obligations (via a rule change) requiring us as a transmission network service provider to uplift our cyber security capability and infrastructure security. These obligations will result in a step increase in people, processes and solutions required to monitor, identify and respond to cyber and physical security attacks on our infrastructure.

This report details the operational expenditure uplift requirements associated with our Operational Technology (OT) environment and high voltage network infrastructure security. These are separate packets of work considered under the Bill requirements, and the various options described within the report are not treated as being linked across both spaces.

This analysis has been prepared utilising methods externally validated by KPMG[1] for the same work being performed within TransGrid's Information Technology (IT) environment.

1.2 Operational Technology Environment - Options Evaluated

Option OT1 - Maintaining Current Maturity

Cyber security maturity will be retained at current levels with the threat landscape under this option. Marginal improvements and initiatives will be required in order to maintain current capabilities in the face of an expected growing threat landscape. This option will not meet the Bill requirements as they are currently understood.

There is no incremental opex over the 2023-28 regulatory period uplift required for this option.

Option OT2 - Complying with Current Bill Requirements

This option will implement cyber security program initiatives to comply with the new security obligations from the proposed Bill. This option will enable TransGrid to comply with the new security obligations under the Bill as they are currently understood. Of note is that sector specific rules have not yet been confirmed, and is highly likely that subsequent revisions will mandate TNSP's comply with the Australian Energy Sector Cyber Security Framework[2] (AESCSF) security profile of SP3.

The AESCSF is a cyber security framework that has been developed and tailored to the Australian energy sector. It has been established to address increasing cyber security threats faced by the sector and developed in collaboration with organisations such as AEMO, ACSC, DHA and CIC. The framework outlines measures of cyber security capability and maturity, those being a Maturity Indicator Level (MIL) and Security

[1] KPGM Report: TransGrid – Critical Infrastructure Security Cost Analysis (June 2021)

[2] https://aemo.com.au/-/media/files/initiatives/cyber-security/2021/aescsf-framework-overview-2020-21.pdf?la=en

Profile (SP). These levels both varying from a grading of 1 through to 3, reflective of an increasing state of maturity requirement. A level of SP3 represents the highest cyber security maturity state under the framework.

This option will not meet the mandatory AESCSF maturity level of SP3.

Total incremental opex uplift over the 2023-28 regulatory period for this option is $1.29M.

Option OT3 - Maturing to AESCSF SP3

This option will implement security uplifts to comply with the new security obligations from the Critical Infrastructure Bill and mature sufficiently to qualify as SP3 within the AESCSF. This option will meet the mandatory AESCSF maturity level of SP3.

Total incremental opex over the 2023-28 regulatory period for this option is $3.13M.

1.3 Physical Security - Options Evaluated

Option PS1 - Maintaining Current Maturity

This option continues the status-quo of physical security assurance, hazard and control assessment, and reporting functions. This option will not meeting the physical security requirements under the Critical Infrastructure Bill Positive Security Obligations.

There is no incremental opex over the 2023-28 regulatory period for this option.

Option PS2 - Compliance driven assurance (critical sites only)

This option uplifts the organisations Physical Security Assurance activities to meet Positive Security Obligation requirements under the Bill. This requirement mandates self-assessed critical sites undergo both internal and external governance/assurance activities that are aligned under TransGrid's corporate risk management framework.

This option includes all initiatives for increased activities in the following spaces:

- Assurance activities
- Compliance reporting
- Site treatment assessments
- Engagements with regulator and wider industry
- External assurance based activities

Total incremental opex over the 2023-28 regulatory period for this option is $1.66m.

Option PS3 - Complete network assurance case (all sites)

This option expands on Option PS2 through increasing the scope of required assurance practices to cover not only self-assessed critical sites, but to the entire High Voltage network. This option includes all initiatives outlined in Option PS2 but in more depth. This will to be to a level assessed as exceeding the minimum Bill requirements as they are currently understood, however provides additional assurance that key physical security risk controls are being implemented effectively across TransGrid's entire network.

Total incremental opex over the 2023-28 regulatory period for this option is $2.38m.

2. Operational Technology Cyber Security Requirements

2.1 Relevant Critical Infrastructure Bill Requirements

Based on sector specific rules work by the Department of Home Affairs, AEMO and industry to date, we anticipate the following cyber security obligations applicable to our OT environment:

> Within 12 months of rule commencement comply with requirements to meet SP1 of AESCSF.
> Within 24 months of rule commencement comply with requirements to meet SP2 of AESCSF
> Within 60 months of rule commencement comply with requirements to meet SP3 of AESCSF
> Demonstration of regard to the requirements of IEC-62443 and accounted for in the organisations risk management program

Note the requirement of these sector specific rules have not yet been formalised under the draft Bill, and an AESCSF maturity of SP3 is more mature than that currently required. It is widely expected based departmental and industry working groups to date that the additional maturity of SP3 will become a requirement for TNSPs as the Bill is finalised.

2.2 Key Initiatives

This section details initiative works packages required to close the current OT cyber security maturity gap in order to meet AESCSF SP3 requirements. For each initiative a brief scope description has been given, along with their mapping to the AESCSF security domains, and the estimated opex costs associated with implementing.

Options under consideration in Section 2.3 have been formed utilising either a subset of, or the complete set of initiatives. Each option articulates which initiatives are being considered within scope.

2.2.1 Summary of Initiatives

Table 1 describes the initiatives proposed for inception within RP3 and Table 2 references linkages of these initiatives against the AESCSF.

Table 1: OT key initiatives

#	Name	Description
1	Zero Trust Authority (ZTA) / Secure Access Service Edge (SASE)	Facilitates a transition to an access-on-demand / zero trust model from the existing flat access style network. This will drive an access-as-required capability within the environment.
2	Enhanced MSSP / IR	Enhanced OT interface with the organisation level managed security service provider (MSSP) solution that will allow continuous monitoring of logs within the managed Security Information and Event Management (SIEM).
3	Enhanced Identity Governance and Assurance (IGA)	Enhancement to automate governance processes around user access requests, granting of access and access level review.
4	Enhanced Patch	Enhanced patch management capabilities to more effectively address

	Management	detected network vulnerabilities through better testing facilities and rollout out consistency.
5	Enhanced Attack Surface Management & Deception Technology	Increase TransGrid's OT capability to identify compromises within the environment. This is achieved by increasing the ability to determine changes to the OT attack surface area and deployment of deception technologies.
6	Enhanced Network and Firewall Assurance	Enhance security capabilities through continuous firewall monitoring, assurance and network device analysis.
7	Control Assurance - Projects	Expansion of control assurance activities on projects augmenting or modifying the OT environment
8	Technical Control Assurance - Projects	Expansion of technical control assurance activities on projects augmenting or modifying the OT environment. This is aimed to increase the assurance of control effectiveness.
9	Risk Management - Assessment / Follow Up	Increased level of risk management activities including conduct of assessment and follow-up activities.

Table 2: AESCSF linkage to key initiatives

AESCSF Domain Link	#1	#2	#3	#4	#5	#6	#7	#8	#9
Situational Awareness (SA)		X							
Event and Incident Response, Continuity of Operations (IR)		X							
Information Sharing and Communications (ISC)									
Identity and Access Management (IAM)	X		X						
Threat and Vulnerability Management (TVM)				X	X	X			
Supply Chain and External Dependencies Management (EDM)				X	X				
Asset, Change and Configuration Management (ACM)				X	X	X	X	X	X
Cyber Security Program Management (CPM)				X	X	X			
Workforce Management (WM)									
Risk Management (RM)							X	X	X
Australian Privacy Management (APM)							X	X	X

2.2.2 Opex Requirements

The below section outlines opex requirements associated with each initiative and is to be read in conjunction with costing methods described in Appendix A and Appendix B. Opex requirements comprise:

> Ongoing licencing and support costs
> Resource requirements

Note licencing and support costs are calculated based on an *OT proportional factor* applied against validated costing conducted for deployment within the IT environment. These factors have been subjectively assessed jointly by the relevant SME's within Asset Management and Corporate Security.

Table 3: Initiative OPEX requirements (5 years)

#	Name	OT Factor	Licencing & Support ($)	Resource Uplift ($)
1	Zero Trust Authority (ZTA) / Secure Access Service Edge (SASE)	0.2	$176k	$116k
2	Enhanced MSSP / IR	0.2	-	$232k
3	Enhanced Identity Governance and Assurance (IGA)	0.3	$231k	$206k
4	Enhanced Patch Management	0.5	$200k	$259k
5	Enhanced Attack Surface Management & Deception Technology	0.6	$240k	$317k
6	Enhanced Network and Firewall Assurance	0.4	$320k	$232k
7	Control Assurance - Projects	-	-	$163k
8	Technical Control Assurance - Projects	-	-	$163k
9	Risk Management - Assessment / Follow Up	-	-	$274k

2.3 Options

This section summarises options that are under consideration for RP3 including the associated opex uplift where appropriate.

Option OT1 - Maintaining Current Maturity

Cyber security maturity will be retained at current levels with the threat landscape under this option. Marginal improvements and initiatives will be required in order to maintain current capabilities in the face of an expected growing threat landscape.

This option will not meet the Bill requirements as they are currently understood.

There is no incremental opex over the 2023-28 regulatory period uplift required for this option.

Option OT2 - Complying with Proposed Requirements

This option will implement cyber security program initiatives to comply with the new security obligations from the proposed Bill. This option will enable TransGrid to comply with the new security obligations as they are currently understood. Further updates to this Bill are unlikely to be covered by this option at this point in time (for example a requirement of SP3 maturity).

This option contains the following initiatives required for complying with the Bill as it currently stands:

> Enhanced MSSP / IR
> Enhanced Patch Management
> Control Assurance – Projects
> Technical Control Assurance – Projects
> Risk Management - Assessment / Follow Up

This option will not meet the mandatory AESCSF maturity level of SP3.

Total incremental opex uplift over the 2023-28 regulatory period for this option is $1.29M (Licencing/Support - $200k, Resourcing - $1.09M).

Option OT3 - Maturing to AESCSF SP3

This option will implement security uplifts to comply with the new security obligations from the Critical Infrastructure Bill and mature sufficiently to qualify as SP3 within the AESCSF.

This option contains the following initiatives required for complying with the Bill once sector specific rules, as anticipated, are formally mandated:

- Zero Trust Authority (ZTA) / Secure Access Service Edge (SASE)
- Enhanced MSSP / IR
- Enhanced Identity Governance and Assurance (IGA)
- Enhanced Patch Management
- Enhanced Attack Surface Management & Deception Technology
- Enhanced Network and Firewall Assurance
- Control Assurance – Projects
- Technical Control Assurance – Projects
- Risk Management - Assessment / Follow Up

This option will meet the mandatory AESCSF maturity level of SP3.

Total incremental opex over the 2023-28 regulatory period for this option is $3.13M (Licencing/Support - $1.17M, Resourcing - $1.96M).

Preferred Option

The preferred option is Option OT3 - Maturing to AESCSF SP3.

This option ensures our compliance obligation as a utility of national significance are fully met under all expected requirements of the Bill (including both positive security obligations and sector specific rules), and our cyber security risks are appropriately managed via the strengthened security posture of SP3.

3. Physical Security Requirements

3.1 Critical Infrastructure Bill Requirements

Based on work by the Department of Home Affairs, AEMO and industry to date, we anticipate the following infrastructure security obligations will be applicable:

> Within 12 months of rule commencement, ensure that our risk management program sets out how we:
  a) detect and deter unauthorised persons accessing secure areas, and respond to incidents where unauthorised access occurs;
  b) restrict, control and monitor access by unauthorised persons; and
  c) control authorised access, including restricting access to only those persons with the appropriate approval who have an operational need to access.

> Within 12 months of rule commencement, demonstrate in our risk management program how we conduct tests, as appropriate, to ensure active security measures are effective and appropriate to detect, deter, respond to and recover from breaches of security at self-assessed critical sites.
  a) These tests may be conducted in conjunction with other safety, security or emergency management exercises or procedures.

> Within 12 months of rule commencement, ensure that our risk management program sets out how we have regard to ENA Doc 015 2006 “National guidelines for prevention of unauthorised access to electricity infrastructure”.

3.2 Key Initiatives

Physical security related uplifts from the Asset Management organisational level are captured in Table 4 below as initiatives. Note, Corporate Security specific initiatives are outside the scope of this document and are captured within Corporate Services governance documentation.

3.2.1 Summary of Initiatives

Table 4: Physical security key initiatives

#	Name	Description
1	Increased assurance based activities	Increased requirement for assurance based tasks on *critical* classified sites within the HV network. This requires additional formal control assurance be completed, additional supporting administrative processes and general risk management activities.
2	Compliance reporting internally/externally	Increased level of compliance and performance reporting both within the organisation for Level 2 and Level 3 assurance activities, and externally to a technical regulator governing the CI Bill.
3	Site treatment assessments	Increased levels of site treatment assessments including frequency of site criticality, and appropriateness of existing treatments.
4	Engagements with regulator and wider industry	Regular engagements including working groups are expected with regulatory bodies, federal security departments, AEMO, ENA etc.
5	External assurance based activities	Enhance independent physical security control validation and assurance. Requires engagement of third-party organisations for the purpose of fulfilling validation requirement.

3.2.2 Opex Requirements

See Physical Security section of Appendix B which details initiative resource estimates for all options under consideration.

3.3 Options

This section summarises options that are under consideration for RP3 including the associated opex uplift where appropriate.

Option PS1 - Maintaining Current Maturity

This option continues the status-quo of physical security assurance, hazard and control assessment, and reporting functions.

This option will not meeting the physical security requirements under the Critical Infrastructure Bill Positive Security Obligations.

There is no incremental opex over the 2023-28 regulatory period for this option.

Option PS2 - Compliance driven assurance (critical sites only)

This option uplifts the organisations Physical Security Assurance activities to meet Positive Security Obligation requirements under the Bill. This requirement mandates self-assessed critical sites undergo both internal and external governance/ assurance activities that are aligned under TransGrid's corporate risk management framework.

This option includes all initiatives outlined in Section 3.2.1 completed to a level assessed as meeting the minimum Bill requirements as they are currently understood.

Total incremental opex over the 2023-28 regulatory period for this option is $1.66m. This option includes a $75k external engagement fee per year for the purpose of assurance/validation on critical classified sites.

Option PS3 - Complete network assurance case (all sites)

This option expands on Option 2 through increasing the scope of required assurance practices to cover not only self-assessed critical sites, but to the entire High Voltage network.

This option includes all initiatives outlined in Section 3.2.1 completed to a level assessed as exceeding the minimum Bill requirements as they are currently understood, however provides additional assurance that key physical security risk controls are being implemented effectively across TransGrid's entire network.

Total incremental opex over the 2023-28 regulatory period for this option is $2.38m. This option includes a single $150k external engagement fee per year for the purpose of assurance/validation on critical classified sites (all in this case).

Preferred Option

The preferred option is Option PS2 - Compliance driven assurance (critical sites only).

This option ensures our compliance obligation as a utility of national significance are fully met under the Bill. Under this Option we will achieve compliance at the lowest incremental opex whilst still assuring our physical security risks are appropriately managed as mandated under the Bill requirements.

Appendix A – Method of Salary Band Usage

Four salary positions have been assessed for calculating resource requirements associated with initiatives described within this report. These are detailed in Table 5 below and cover a spread of both junior and senior roles envisaged to be engaged.

Notes:

> On-cost value of 40% used (less CO role which was calculated from contract officer salary rates)
> Average salary per position calculated using the bottom and top of salary band ranges

Table 5: Salary bands

Salary Point Band	Title	Salary Package Low (bottom of band)	Salary Package High (top of band)	Salary Package + Oncosts Low (bottom of band)	Salary Package + Oncosts High (top of band)	Average
SP 14-18	Junior Analyst, Technician	$89,688.58	$104,445.79	$125,564.01	$146,224.11	$135,894.06
SP 24-28	Asset Analyst / Engineer, Senior Technician	$127,028.34	$144,849.73	$177,839.68	$202,789.62	$190,314.65
SP 30-34	Strategist / Compliance Specialist	$154,671.88	$176,552.85	$216,540.63	$247,173.99	$231,857.31
Contract Officer (CO01 - CO08)	Senior Role or Manager	$177,145.80	$465,052.80	$177,145.80	$465,052.80	$321,099.30

In order to simplify resource calculations generic junior and senior roles are calculated using averages. See Table 6 below.

Table 6: Junior and senior resource costs

Title	Salary
Junior Analyst, Technician	$135,894.06
Asset Analyst / Engineer, Senior Technician	$190,314.65
Junior Resource Average	**$163,104.35**
Strategist / Compliance Specialist	$231,857.31
Senior Role or Manager	$321,099.30
Senior Resource Average	**$276,478.31**

Appendix B – Resource Calculations

Resource requirements have been examined from the perspective of junior and senior role utilisation per initiative. The FTE requirement for both junior and senior resources is calculated as:

$$FTE\ Req = \#resources \times Allocation \times Role\ \%\ Allocation \times 1.25$$

$$Total\ Req = Junior\ FTE\ Req + Senior\ FTE\ Req$$

- #resources = Number of resources allocated to the initiative
- Allocation = Allocation for each initiatives resources
- Role % Allocation = Resourcing split between junior/senior for each initiative
- 1.25 = Utilisation factor of 80% considered as resource being fully booked

Resource costs for each initiative are estimates only and subject to change as details of each initiative become more granular.

Operational Technology Cyber Security Resource Requirements

Table 7: OT resource costs per initiative (per annum)

Initiative	#	Allocat-ion	Hours / wk	%Allocat-ion	Junior FTE Req	Junior ($)	%Allocat-ion	Senior FTE Req	Senior ($)	Total FTE Req
				Junior Resourcing			Senior Resourcing			
ZTA / SASE	1	10%	4	80%	0.10	**$16,310**	20%	0.03	**$6,912**	**0.13**
Enhanced MSSP / IR	1	20%	8	80%	0.20	**$32,621**	20%	0.05	**$13,824**	**0.25**
Enhanced IGA (Identity Governance & Assurance)	1	15%	6	50%	0.09	**$15,291**	50%	0.09	**$25,920**	**0.19**
Enhanced Patch Management (Vulnerability Prioritisation etc.)	1	15%	6	0%	0.00	-	100%	0.19	**$51,840**	**0.19**
Enhance Attack Surface Management & Deception Technology	1	20%	8	20%	0.05	**$8,155**	80%	0.20	**$55,296**	**0.25**
Enhancing Network & Firewall assurance	1	20%	8	80%	0.20	**$32,621**	20%	0.05	**$13,824**	**0.25**
Control	1	15%	6	90%	0.17	**$27,524**	10%	0.02	**$5,184**	**0.19**

Assurance - Projects										
Technical Control Assurance - Projects	1	15%	6	90%	0.17	**$27,524**	10%	0.02	**$5,184**	**0.19**
Risk Management - Assessment / Follow Up	1	20%	8	50%	0.13	**$20,388**	50%	0.13	**$34,560**	**0.25**
				Totals	**1.11**	**$180,434**		**0.77**	**$212,543**	**1.88**

Physical Security Resource Requirements

Option PS2 - Compliance driven assurance (critical sites only)

Table 8: Physical security resource costs per initiative (per annum)

Initiative	#	Allocat-ion	Hours / wk	%Allocat-ion	Junior FTE Req	Junior ($)	%Allocat-ion	Senior FTE Req	Senior ($)	Total FTE Req
				Junior Resourcing			Senior Resourcing			
Increased assurance based activities	2	22%	17.6	60%	0.33	**$53,824**	40%	0.22	**$60,825**	**0.55**
Compliance reporting internally/externally	1	9%	3.6	50%	0.06	**$9,175**	50%	0.06	**$15,552**	**0.11**
Site treatment assessments	2	22%	17.6	80%	0.44	**$71,766**	20%	0.11	**$30,413**	**0.55**
Engagements with regulator and wider industry	1	5%	2	30%	0.02	**$3,058**	70%	0.04	**$12,096**	**0.06**
				Totals	**0.85**	**$137,823**		**0.43**	**$118,886**	**1.28**

Table 9: Resource basis per initiative

Initiative	Initiative Tasks	Days / year	Hours / week
Increased assurance based activities	> 17x Tier 1 subs (1.5 days/year each) > 100x Tier 2 subs (0.4 days/year each) > 90x RRS (0.25 days/year each)	88	**17.6**
Compliance reporting internally/externally	Operational reports, assurance WG reports, internal compliance/LGR reports. > 1.5 days / month	18	**3.6**
Site treatment assessments	> 17x Tier 1 subs (1.5 days/year each) > 100x Tier 2 subs (0.4 days/year each)	88	**17.6**

	> 90x RRS (0.25 days/year each)		
Engagements with regulator and wider industry	> 1 day per quarter > 0.5 day per month	10	**2**

Option PS3 - Complete network assurance case (all sites)

Table 10: Physical security resource costs per initiative (per annum)

Initiative	#	Allocat-ion	Hours / wk	%Allocat-ion	Junior FTE Req	Junior ($)	%Allocat-ion	Senior FTE Req	Senior ($)	Total FTE Req
				Junior Resourcing			Senior Resourcing			
Increased assurance based activities	2	29%	23.3	60%	0.44	**$71,256**	40%	0.29	**$80,524**	**0.73**
Compliance reporting internally/externally	1	9%	3.6	50%	0.06	**$9,175**	50%	0.06	**$15,552**	**0.11**
Site treatment assessments	2	29%	23.3	80%	0.58	**$95,008**	20%	0.15	**$40,262**	**0.73**
Engagements with regulator and wider industry	1	5%	2	30%	0.02	**$3,058**	70%	0.04	**$12,096**	**0.06**
				Totals	**1.09**	**$178,497**		**0.54**	**$148,434**	**1.63**

Table 11: Resource basis per initiative

Initiative	Initiative Tasks	Days / year	Hours / week
Increased assurance based activities (same as Option 1 but more exhaustive / in-depth activities)	> 17x Tier 1 subs (2 days/year each) > 100x Tier 2 subs (0.6 days/year each) > 90x RRS (0.25 days/year each)	116.5	**23.3**
Compliance reporting internally/externally	Operational reports, assurance WG reports, internal compliance/LGR reports. > 1.5 days / month	18	**3.6**
Site treatment assessments (same as Option 1 but more exhaustive / in-depth activities)	> 17x Tier 1 subs (2 days/year each) > 100x Tier 2 subs (0.6 days/year each) > 90x RRS (0.25 days/year each)	116.5	**23.3**
Engagements with regulator and wider industry	> 1 day per quarter > 0.5 day per month	10	**2**