



Red

Amber

Green

1.1	A member of the executive board is responsible for overseeing and providing strategic management and support for all security management work within the organisation.	Green	
1.2	The organisation employs or contracts in a qualified person to undertake the full range of security management work.	Green	
1.3	The organisation allocates resources and investment to security management in line with its identified risks.	Green	
1.4	The organisation reports annually to its board on how it has met the standards set by NHS Protect in relation to security management, and its local priorities as identified in its work plan.	Green	
1.5	The organisation has a security management strategy aligned to NHS Protect's strategy. The strategy has been approved by the executive body or senior management team and is reviewed, evaluated and updated as required.	Green	

STRATEGIC GOVERNANCE LEVEL

GREEN

OVERALL LEVEL

GREEN

0 0 1

0 0 1

0 0 1

0 0 1

0 0 1

High **Medium** **Low**
0 0 5

: **GREEN**

Note: If Q1.2 is "Red" then this will be "Red" regardless of the rating here

<u>Calculation of OVERALL</u>		<u>Red</u>	<u>Amber</u>	<u>Green</u>
Strategic Governance	GREEN	0	0	1
Inform & Involve	GREEN	0	0	1
Prevent & Deter	GREEN	0	0	1
Hold to Account	GREEN	0	0	1
		0	0	4
Max value		4		
HIGH		0	0	
MEDIUM		0	0	
LOW		1	1	
		1		

GREEN



Red Amber Green

0 0 1

0 0 1

0 0 1

2.4	The organisation demonstrates effective communication between risk management, capital projects management, estates, security management and external agencies to discuss security weaknesses and to agree a response.	Green	
2.5	All new staff, permanent and temporary, receive information about security measures and security management. Staff induction programmes include a security management component and learning outcomes can be evidenced.	Green	
2.6	All staff know how to report a violent incident, theft, criminal damage or security breach. Their knowledge and understanding in this area is regularly checked and improvements in staff training are made where necessary.	Green	
2.7	All staff who have been a victim of a violent incident have access to support services should they require it.	Green	
INFORM & INVOLVE LEVEL			
GREEN			

Standards Self Review Tool



Please complete this sheet in as much detail as possible.
To 'Select from list', click on the relevant field, then click on the arrow button, which will reveal a drop down menu.

PREVENT & DETER

	Standard	Select Level	Comment
3.1	The organisation provides prevention of violence training or conflict resolution training (CRT) to all its front line staff in accordance with NHS Protect's guidance. The training is monitored, reviewed and evaluated.	Green	
3.2	The organisation has arrangements in place for 'post incident' learning in relation to a) security breaches/incidents b) acts of violence c) thefts d) criminal damage and a mechanism for feeding this back into the development of policies.	Green	
3.30000	The organisation issues national and regional NHS Protect alerts to relevant staff and action is taken to raise awareness of security risks and incidents. The process is controlled, monitored reviewed and evaluated.	Green	
3.40000	The organisation ensures that the provision of a secure environment is a key criterion for any new build projects, or the modification and alteration (e.g. refurbishment or refitting) of existing premises.	Green	
3.5	The organisation has arrangements in place to manage access and control the movement of people within its premises, buildings and any associated grounds.	Green	
3.6	The organisation has systems in place to protect its assets from the point of procurement to the point of decommissioning or disposal.	Green	
3.7	The organisation has clear policies and procedures in place for the security of medicines and controlled drugs (CDs).	Green	
3.80000	The organisation operates a corporate asset register for assets worth £5,000 or more.	Green	
3.9	The organisation has in place departmental asset registers and records for assets worth less than £5,000.	Green	
3.10	Staff and patients have access to safe and secure facilities for the storage of their personal property.	Green	
3.11	The organisation maintains a detailed record of security incidents affecting its property and assets that involve theft and/or criminal damage and this is used to help inform security management priorities.	Green	

3.12	The organisation takes a risk-based approach to identifying and protecting its critical assets and infrastructure. This is embedded in policy and can be evidenced.	Green	
3.13	In the event of an increased security threat level, the organisation is able to increase its security resources and responses.	Green	
3.14	The organisation has in place suitable lockdown arrangements for each of its sites, or for other specific buildings/areas of priority.	Green	
3.15	Where applicable, the organisation has clear policies and procedures in place in relation to preventing a potential child or infant abduction, and these are regularly tested, monitored and reviewed.	Green	

PREVENT & DETER LEVEL

GREEN



0 0 1

0 0 1

0 0 1

0 0 1

High	Medium	Low
0	0	15

Calculation of risk

Max value:	15	
HIGH	0	0
MEDIUM	0	0
LOW	1	1
Risk	1	

GREEN

Note: If Q1.2 is "Red" then this will be "Red" regardless of the rating here

Standards Self Review Tool



*Please complete this sheet in as much detail as possible.
To 'Select from list', click on the relevant field, then click on the arrow button, which will reveal a drop down menu.*

HOLD TO ACCOUNT

	Standard	Select Level	Comment
4.1	The organisation is committed to applying all appropriate sanctions against those responsible for acts of violence, security breaches, theft and criminal damage.	Green	
4.2	The organisation has arrangements in place to ensure that allegations of violence, theft and criminal damage are investigated in a timely and proportionate manner and these arrangements are monitored, reviewed and evaluated.	Green	
4.3	Where appropriate, the organisation publicises successful prosecutions of cases relating to a) denying unnecessary access to premises b) the consequences of assaulting NHS staff c) breaching the security of NHS premises and property d) acts of theft and criminal damage.	Green	
4.4	The organisation has a clear policy on the recovery of financial losses incurred due to theft of, or criminal damage to, its assets and can demonstrate its effectiveness.	Green	

HOLD TO ACCOUNT LEVEL

GREEN



High Medium Low

0 0 1

0 0 1

0 0 1

0 0 1

High Medium Low

0 0 4

Calculation of risk

Max value:	4	
HIGH	0	0
MEDIUM	0	0
LOW	1	1
Risk	1	

GREEN

Note: If Q1.2 is "Red" then this will be "Red" regardless of the

Note: If Q1.2 is "Red" then this

Security Management Work Plan for							<DATE>				
							tes	Completed Date	Days/Time Allocated	Actual Days	
SRT LEVEL	STRATEGIC GOVERNANCE										0
	1.1	A member of the executive board is responsible for overseeing and providing strategic management and support for all security management work within the organisation.									Green
	1.2	The organisation employs or contracts in a qualified person to undertake the full range of security management work.									Amber
	1.3	The organisation allocates resources and investment to security management in line with its identified risks.									Red
	1.4	The organisation reports annually to its board on how it has met the standards set by NHS Protect in relation to security management, and its local priorities as identified in its work plan.									Not Applicable
	1.5	The organisation has a security management strategy aligned to NHS Protect's strategy. The strategy has been approved by the executive body or senior management team and is reviewed, evaluated and updated as required.									
INFORM & INVOLVE											
	2.1	The organisation undertakes risk assessments in relation to: a) protecting NHS staff and patients b) security of premises c) protecting property and assets d) security preparedness and resilience. The organisation uses its identified risks to develop inclusive policies in respect of the above (a-d) and can demonstrate implementation of these policies. The policies are monitored, reviewed and communicated across the organisation.									Green

Green	2.2	Local memorandums of understanding, concordats and agreements are in place with the police and the Crown Prosecution Service (CPS) to help protect and secure NHS staff, premises, property and assets. This can be evidenced.								
Green	2.3	The organisation participates in all national and local publicity initiatives, as required by NHS Protect, to raise security awareness.								
Green	2.4	The organisation demonstrates effective communication between risk management, capital projects management, estates, security management and external agencies to discuss security weaknesses and to agree a response.								
Green	2.5	All new staff, permanent and temporary, receive information about security measures and security management. Staff induction programmes include a security management component and learning outcomes can be evidenced.								
Green	2.6	All staff know how to report a violent incident, theft, criminal damage or security breach. Their knowledge and understanding in this area is regularly checked and improvements in staff training are made where necessary.								
Green	2.7	All staff who have been a victim of a violent incident have access to support services should they require it.								
PREVENT & DETER										
	3.1	The organisation provides prevention of violence training or conflict resolution training (CRT) to all its front line staff in accordance with NHS Protect's guidance. The training is monitored, reviewed and evaluated.								

	3.2	The organisation has arrangements in place for 'post incident' learning in relation to a) security breaches/incidents b) acts of violence c) thefts d) criminal damage and a mechanism for feeding this back into the development of policies.								
	3.3	000000 The organisation issues national and regional NHS Protect alerts to relevant staff and action is taken to raise awareness of security risks and incidents. The process is controlled, monitored reviewed and evaluated.								
	3.4	000000 The organisation ensures that the provision of a secure environment is a key criterion for any new build projects, or the modification and alteration (e.g. refurbishment or refitting) of existing premises.								
	3.5	The organisation has arrangements in place to manage access and control the movement of people within its premises, buildings and any associated grounds.								
	3.6	The organisation has systems in place to protect its assets from the point of procurement to the point of decommissioning or disposal.								
	3.7	The organisation has clear policies and procedures in place for the security of medicines and controlled drugs (CDs).								
	3.8	000000 The organisation operates a corporate asset register for assets worth £5,000 or more.								
	3.9	The organisation has in place departmental asset registers and records for assets worth less than £5,000.								
	3.10	Staff and patients have access to safe and secure facilities for the storage of their personal property.								
	3.11	The organisation maintains a detailed record of security incidents affecting its property and assets that involve theft and/or criminal damage and this is used to help inform security management priorities.								

3.12	The organisation takes a risk-based approach to identifying and protecting its critical assets and infrastructure. This is embedded in policy and can be evidenced.								
3.13	In the event of an increased security threat level, the organisation is able to increase its security resources and responses.								
3.14	The organisation has in place suitable lockdown arrangements for each of its sites, or for other specific buildings/areas of priority.								
3.15	Where applicable, the organisation has clear policies and procedures in place in relation to preventing a potential child or infant abduction, and these are regularly tested, monitored and reviewed.								

HOLD TO ACCOUNT

4.1	The organisation is committed to applying all appropriate sanctions against those responsible for acts of violence, security breaches, theft and criminal damage.								
4.2	The organisation has arrangements in place to ensure that allegations of violence, theft and criminal damage are investigated in a timely and proportionate manner and these arrangements are monitored, reviewed and evaluated.								
4.3	Where appropriate, the organisation publicises successful prosecutions of cases relating to a) denying unnecessary access to premises b) the consequences of assaulting NHS staff c) breaching the security of NHS premises and property d) acts of theft and criminal damage.								
4.4	The organisation has a clear policy on the recovery of financial losses incurred due to theft of, or criminal damage to, its assets and can demonstrate its effectiveness.								

Signature of the local security management specialist:	Date:
Print name:	

	Signature of the director with responsibility for security management:		Date:					
								

<u>Risk (3 selections)</u>	<u>Risk (2 selections)</u>	<u>Risk (2 selections)</u>
Green	Green	Green
Amber	Amber	Red
Red	Red	
Not Applicable		
<u>Region</u>	<u>Org type</u>	
North East	Special Health Authority	
North West	Community Care Trust	
South East	Acute	
South West	Ambulance	
Eastern	Care Trust	
West Midlands	Mental Health	
East Midlands		
London		