Group Business Protection

A Blueprint for Compliance Framework

Qualys CSO Forum - London

Paul Wood MBE
Group Business Protection Director
Aviva

WHY WAS A COMPLIANCE FRAMEWORK NEEDED?

- Global Organisation
- Numerous standards – which do you chose and what is appropriate?
- How many different regulatory approaches are there?
- How do you judge/measure ‘apples with apples’?
- Does it help you to identify risk?

WHY DID I NEED TO SOLVE THE PROBLEM?

- An internal review identified that the Aviva Group could not prove whether or not it was complying with its policies.

- It was decided that the Group needed a strategic group-wide compliance reporting framework.

-The aim of the framework was to strengthen the Group's overall compliance structure and provide a platform for a controls based auditable system.

- Group Business Protection were the forerunners in Aviva to producing strategic policy with an associated compliance based framework.

WHAT DID WE DO?

- Produced and issued a Business Protection overarching policy detailing all business protection requirements in one document
- Clearly identified the inherent risks.
- Produced and issued minimum security requirements (MSRs) under the overarching policy which detailed, the minimum requirements for Information Security, Physical Security, Business Continuity Management and Incident Management.
- Produced and issued a document detailing all BP-related roles and responsibilities for all staff at group and at the business units.
- Produced and issued a compliance framework process which mapped business units compliance with the policy and MSRs and transferred this compliance rating to the level of risk.

WHY USE A COMPLIANCE BASED FRAMEWORK?

- The compliance based framework allowed us to directly map the level of Business Unit compliance against the specific requirements of the minimum security requirements rather than through a generic questionnaire (e.g. ISO 17799).

- It provides completeness and accuracy of reporting.

- It allowed me to sign off the 6- monthly compliance return and quarterly risk return with confidence as an accurate assessment of the Business Unit.

- It allowed the Business Unit to pin point specific areas of concern and to produce action plans based on specific areas of remediation.

- Allowed us to start to focus on the gaps and the RISKS.

HOW DID I BUILD THE COMPLIANCE FRAMEWORK?

-The MSR documents detail the minimum standards the Business Units are required to meet.

- The Minimum Security Requirements are therefore the Controls against which overall compliance with the GBP policy are measured.

-The compliance framework directly measures the requirements of the MSRs and therefore the policy.

HOW DID I BUILD THE COMPLIANCE FRAMEWORK?

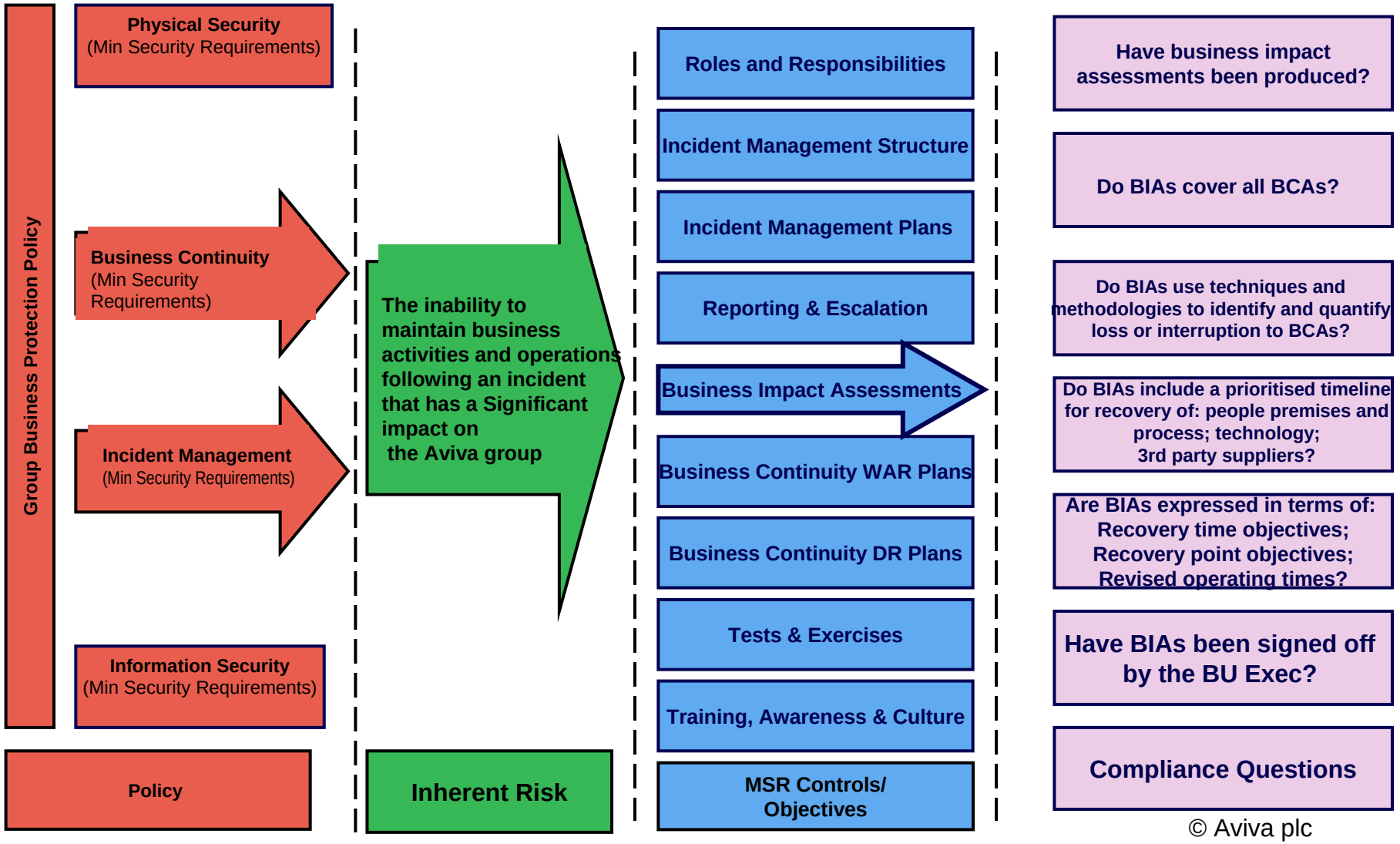
- The compliance framework is a series of binary questions.

- The questions can all be answered by the click of a mouse.

- There are approximately 200 questions in total across all of the business protection disciplines.

- The compliance questions are slit into 5 separate and distinct area: 4 of these cover the specific MSRs and a separate set of questions cover the general roles and responsibilities and governance areas.

HOW DOES THE COMPLIANCE FRAMEWORK WORK?



HOW DID I DEVELOP THEORY INTO PRACTICE?

- Once the questions were produced they needed to be incorporated into a tool which could be issued to BUs and be used as the design effectiveness for controls

- We could not find an ‘out-of-the-box’ product which could provide a solution to transfer the questions into a tool that could be used by the Business Units which would also turn the results into usable data.

- It was therefore decided that to ‘test-drive’ the framework, a cheap solution would be developed to establish whether what we thought we wanted was actually achievable and useful.

- A data management tool was produced that asked the questions and transferred the data into a basic report which was a snap shot of the replies and a detailed report which identified the risk and also showed the Business Unit where to find additional information to remediate the issue.

Back

TRAVEL

1)	Is business travel abroad approved by a senior manager?	○ YES ◉ NO
2)	Is GBP advice sought when individuals request business travel to countries rated high or medium?	○ YES ◉ NO
3)	Is advice sought from GBP for any BU high profile events which may result in undue attention?	◉ YES ○ NO
4)	Do executive protection measures meet the Physical Security MSR requirements?	◉ YES ○ NO

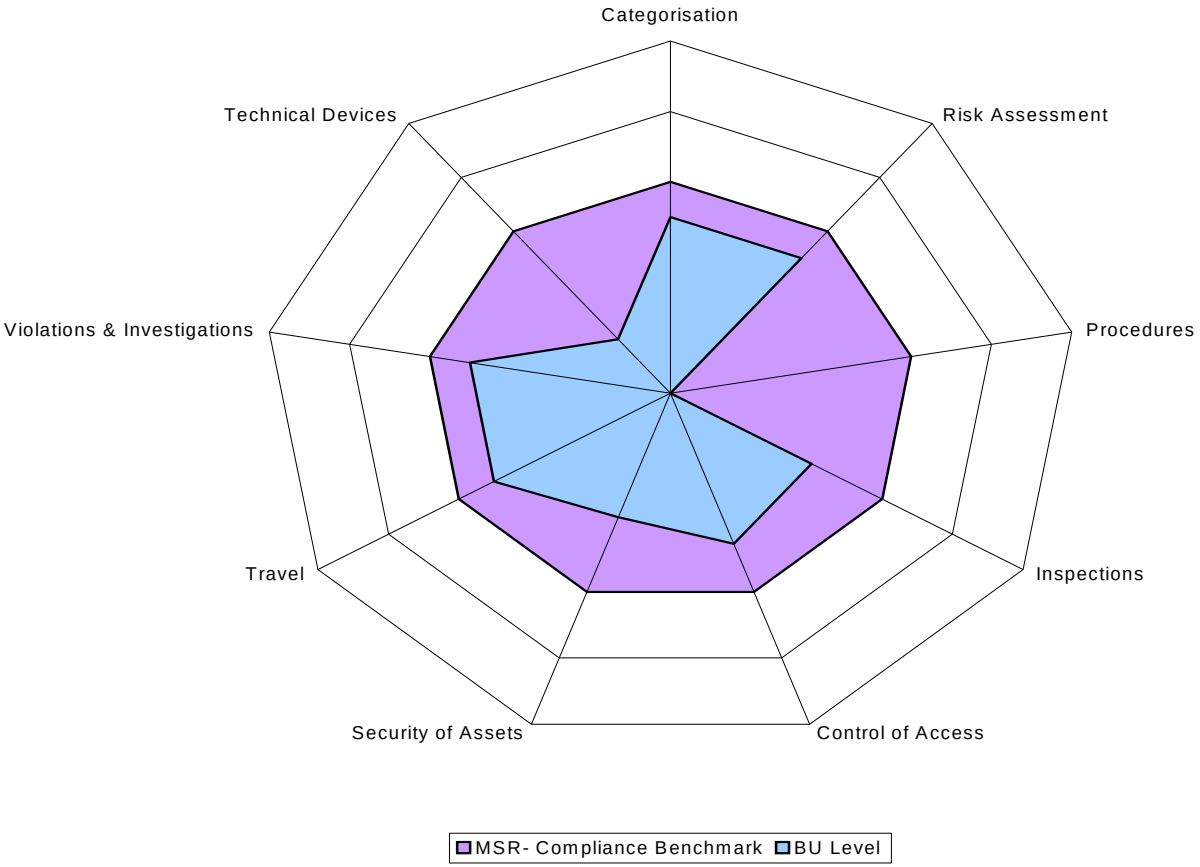
CLEAR

Continue

OVERALL RISK	RED

BP COMPLIANCE FRAMEWORK
BASIC REPORT

Basic Report		
		Section Risk
A	Categorisation	**HIGH**
B	Risk Assessment	**HIGH**
C	Procedures	**HIGH**
D	Inspections	**HIGH**
E	Control of Access	**HIGH**
F	Security of Assets	**HIGH**
G	Travel	**HIGH**
H	Violations & Investigations	**HIGH**
I	Technical Devices	**HIGH**



GBP COMPLIANCE FRAMEWORK – DETAILED REPORT (SAMPLE)

Alpha Code	Enabling Objective	Risk		Enabling Control	ANSWER	Control Risk	Overall	ACTION REQUIRED	REASON - IF ANSWERED NO
CLICK HERE TO RETURN TO SECTION A.	Categorisation	Ineffective building categorisation	1	Have all buildings been catergorised in accordance with their size criticality?	YES	LOW	HIGH	No Action Required	
			2	Have internal areas inside buildings been catergorised as detailed in the Physical Security MSR?	NO	HIGH		Please refer to Physical Security MSR, section 5.1	
CLICK HERE TO RETURN TO SECTION B.	Risk Assessment	Inadequate risk identification / assessments and reporting.	1	Has a risk assessment been produced which covers the Physical Security requirements of new buildings or major changes to exisiting facilities?	YES	LOW	HIGH	No Action Required	
			2	Are the findings of the risk assessment used to define the Physical Security requirements?	YES	LOW		No Action Required	
			3	Are all the findings recorded and subject to approval by the BU executive team or designated manager?	NO	HIGH		Please refer to Physical Security MSR, section 3.2	
			4	Are the agreed findings tracked through implementation?	NO	HIGH		Please refer to Physical Security MSR, section 7.2	

RESULTS

- The first run of the compliance framework is now complete and has identified a wide variety of policy compliance gaps across the group.

- The analysis of the results has given rise to three further actions:

  - Working with Business Units to develop action/remediation plans.

  - Building a case to take to the executive in early 2008 for funding improvements.

  - Considering how best to tackle the common themes highlighted by the compliance process.

DID IT WORK?

- Yes, 100% of Business Units submitted replies by the deadline.
- The general feeling from the Business Units was the tool was easy to use and produced useful information.
- The Action Plan process is ongoing and areas of risk within the group are being remediated.
-Some minor improvements to the tool were identified which will be amended for the next edition.
- Future editions of the tool will be Business Unit specific (questions which do not apply e.g. for local legal reasons will be omitted).
- We are working on a realistic conversion of compliance into risk.
    -- Frequency v impact.

WHAT NEXT ?

- Develop the compliance framework further to integrate it into a control based assessment tool – this will reduce the number questions and focus on key control objectives.

- Integrate our self help (‘home built’) tool into a wider Enterprise Risk Management tool being developed by the group.

- Use the data to drive cost effective pragmatic solutions to reduce risk to within appetite.