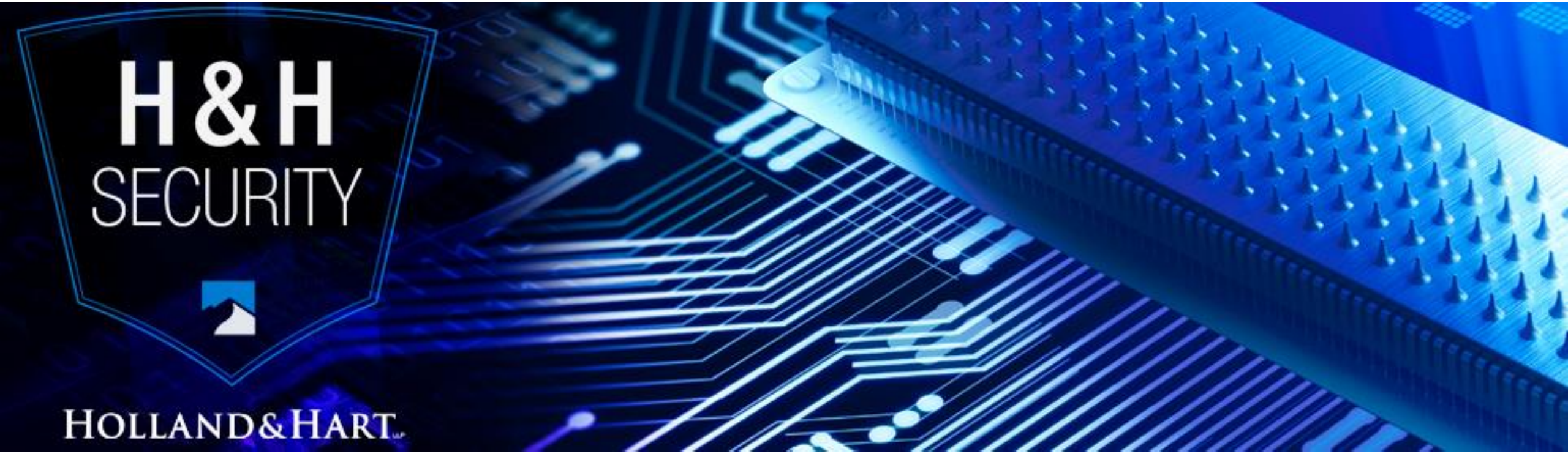
Five Questions to Evaluate any Privacy or Security Program

Wyoming Cybersecurity Symposium



October 23, 2019

HOLLAND&HART

SPEAKER BIO

- CISO at Holland & Hart
- Past President, Denver Chapter ISSA
- 18 years of Computer & Information Security Leadership in Fortune 100 and 500 companies – government & private sectors
- 3 years security consulting
- CISSP and PMP
- Based in Denver, CO

James Johnson CISSP, PMP, STS
CISO, Holland & Hart LLP
555 17th Street, Suite 3200,
Denver, CO 80202
303.295.8563
jbjohnson@hollandhart.com

THE PROBLEM

Too many standards. Too many controls and requirements.

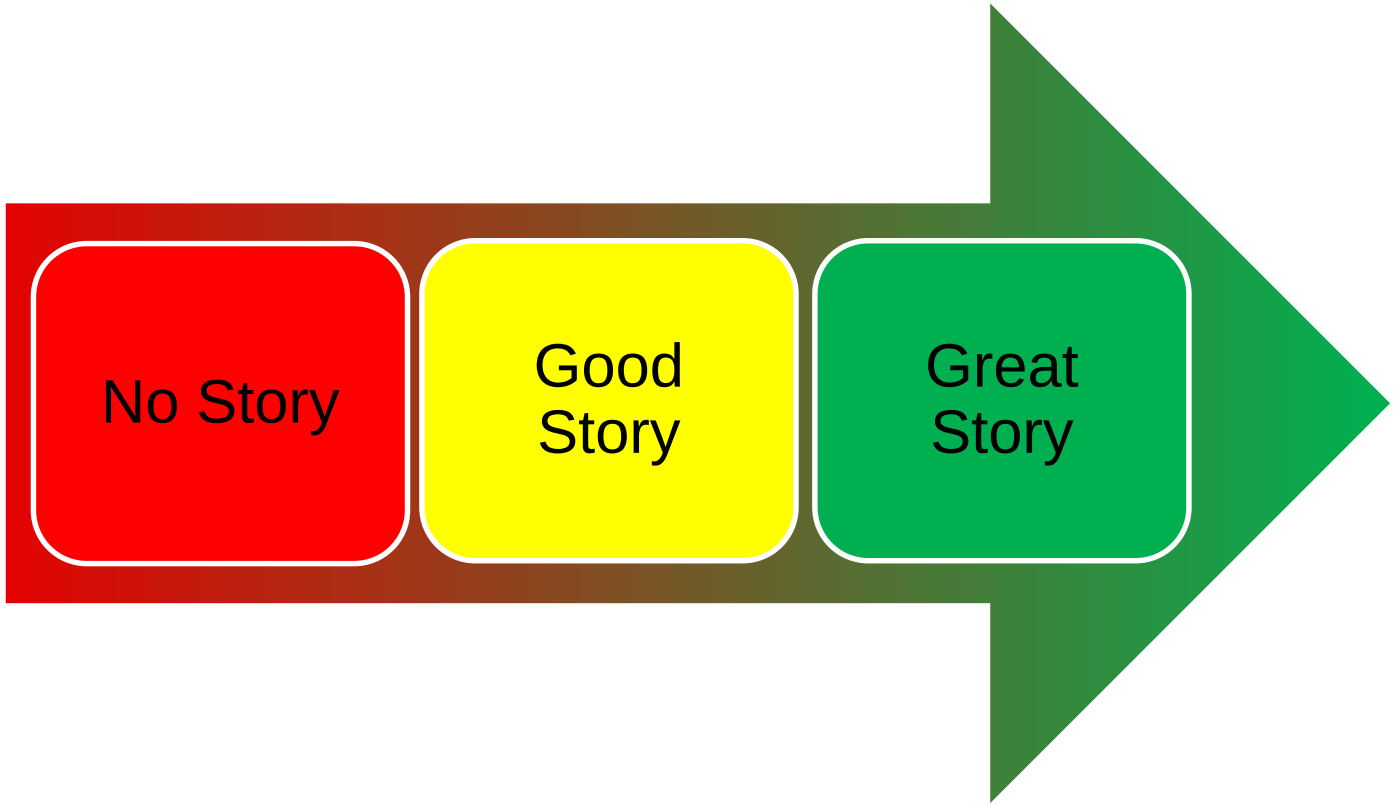
SECURITY

Standard	Controls
HIPAA	56+
CSF	98
NIST 800-171	109
ISO 27001	114
PCI-DSS	200
NIST 800-53	303

PRIVACY

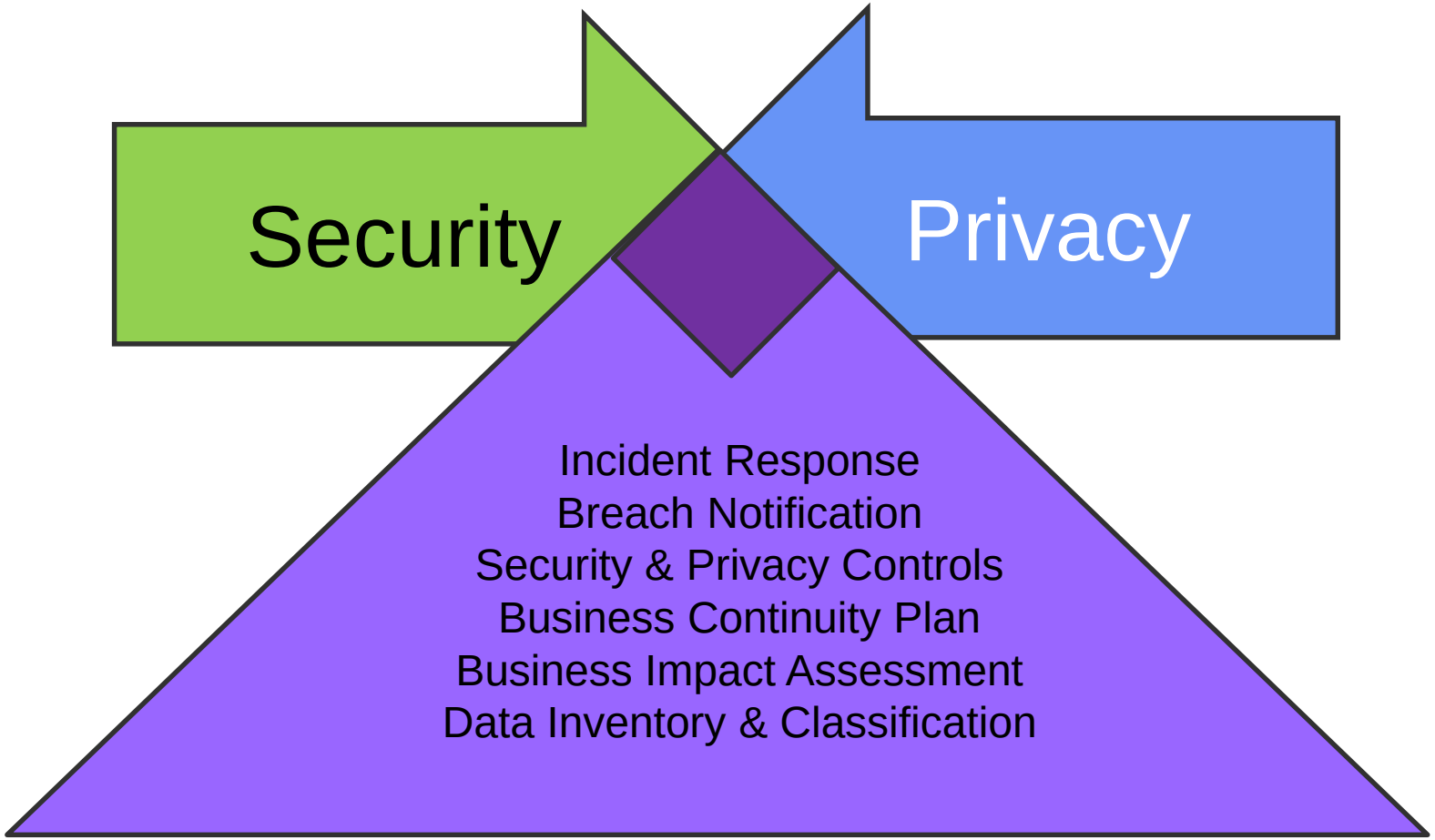
Standard	Controls
GDPR	99
HIPAA	6
ISO 27701:2019	Adds 15
NIST 800-53	26
50 States	varies

SIMPLE PRIVACY & CYBER SECURITY MEASURING SCALE

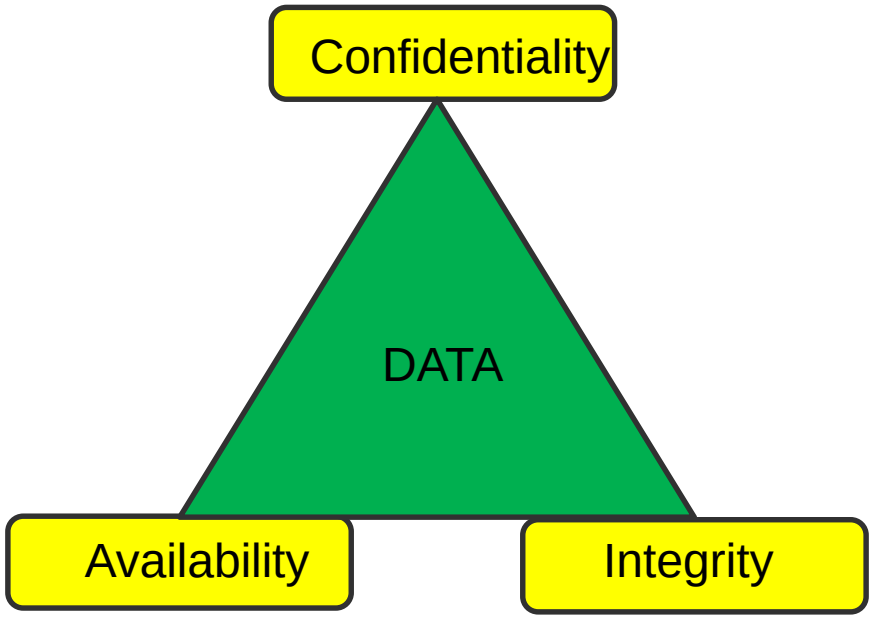


How does your Privacy & Security Book Read?

Security and Privacy are merging rapidly!



DEFINITIONS - SECURITY



"CIA Triad"

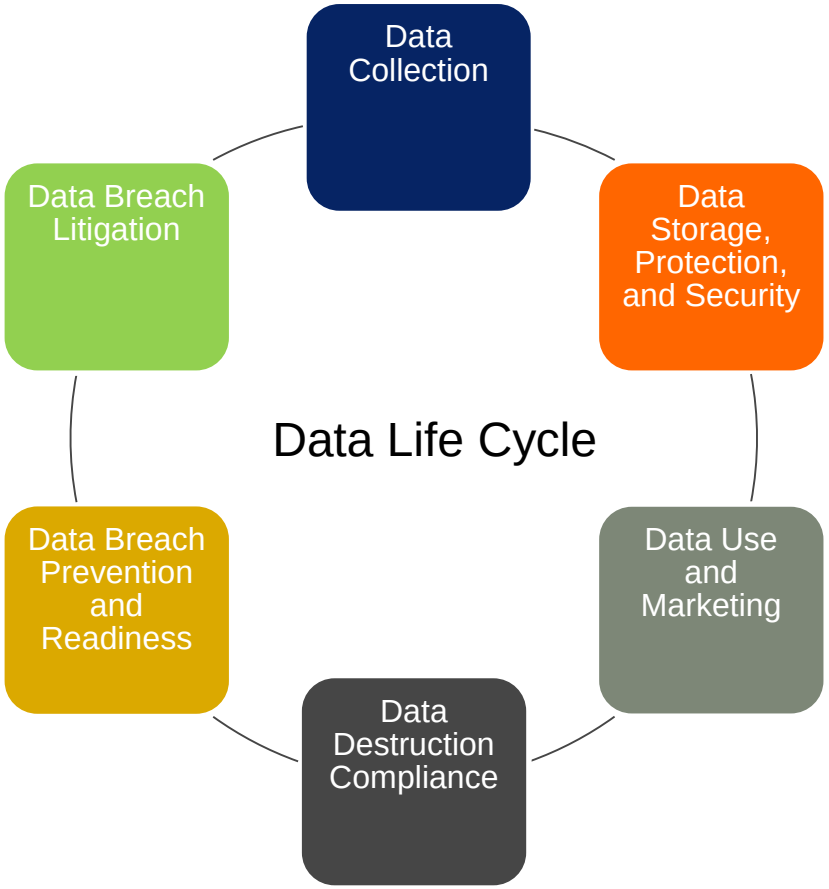
SECURITY DEFINITIONS

Confidentiality:	Data being stored is safe from unauthorized access and use
Integrity:	Data is reliable and accurate
Availability:	Data is available for use when it is needed

DEFINITIONS - PRIVACY

PRIVACY DEFINITIONS

- Collecting personal information
- Using and disclosing personal information
- Ensuring data quality
- Controlling access to personal information
- Confidentiality of sensitive data not defined as PII



THE SOLUTION

The proposed model of five questions is:

- **Meant to be a high-level evaluation.**
- **Not meant to replace detailed standards and compliance framework reviews!**

5 Security Questions

1. What security methodology or standards are followed?
2. Who is the one person assigned security responsibility and oversight?
3. Are there written and approved security policies and procedures?
4. Are the key stakeholders (CEO, CIO, BoD, etc.) briefed routinely on security risks?
5. Is the security program independently tested or audited?

5 Privacy Questions

1. What Privacy methodology or standards are followed?
2. Who is the one person assigned privacy responsibility and oversight?
3. Are there written and approved privacy policies and procedures?
4. Are the key stakeholders (CEO, CIO, BoD, etc.) briefed routinely on privacy risks?
5. Is the privacy program independently tested or audited?

What level is the person assigned Privacy – Security?

Depends upon organization size and type

Security:

5,000+ should have CISO

500+ should have position assigned security exclusively

<500 should have defined security roles but may have other responsibilities.

Privacy:

10,000+ should have CDPO

1,000+ should have position assigned privacy exclusively

<1,000 should have defined privacy roles but may have other responsibilities.

RATING A PRIVACY & CYBER SECURITY PROGRAM

Security

	Scoring		
Question	(0)	(1)	(2)
1. What security methodology or standards are followed?	None	Working on it	Certified / Compliant
2. Who is the one person assigned security responsibility and oversight?	No one	Identified but reports low in the org	Identified and reports high in the organization
3. Are there written and approved security policies and procedures?	None	Some written and maybe some approved	Written, approved and communicated
4. Are the key stakeholders (CEO, CIO, BoD, etc.) briefed routinely on security risks?	Never or only when issues	Yes – Annually or on occasion	Yes – Weekly or monthly
5. Is the security program independently tested or audited?	No	Yes – Once in the last few years	Yes – At least annually or has certification
Column Scores	0		
Overall Score			

RATING A PRIVACY & CYBER SECURITY PROGRAM

Privacy

	Scoring		
Question	(0)	(1)	(2)
1. What privacy methodology or standards are followed?	None	Working on it	Certified / Compliant
2. Who is the one person assigned privacy responsibility and oversight?	No one	Identified but reports low in the org	Identified and reports high in the organization
3. Are there written and approved privacy policies and procedures?	None	Some written and maybe some approved	Written, approved and communicated
4. Are the key stakeholders (CEO, CIO, BoD, etc.) briefed routinely on privacy risks?	Never or only when issues	Yes – Annually or on occasion	Yes – Weekly or monthly
5. Is the privacy program independently tested or audited?	No	Yes – Once in the last few years	Yes – At least annually or has certification
Column Scores	0		
Overall Score			

RATING A PRIVACY & CYBER SECURITY PROGRAM

Security or Privacy

	Scoring		
Question	(0)	(1)	(2)
1. What security or privacy methodology or standards are followed?			
2. Who is the one person assigned security or privacy responsibility and oversight?			
3. Are there written and approved security or privacy policies and procedures?			
4. Are the key stakeholders (CEO, CIO, BoD, etc.) briefed routinely on security or privacy risks?			
5. Is the security or privacy program independently tested or audited?			
Column Scores	0		
Overall Score			

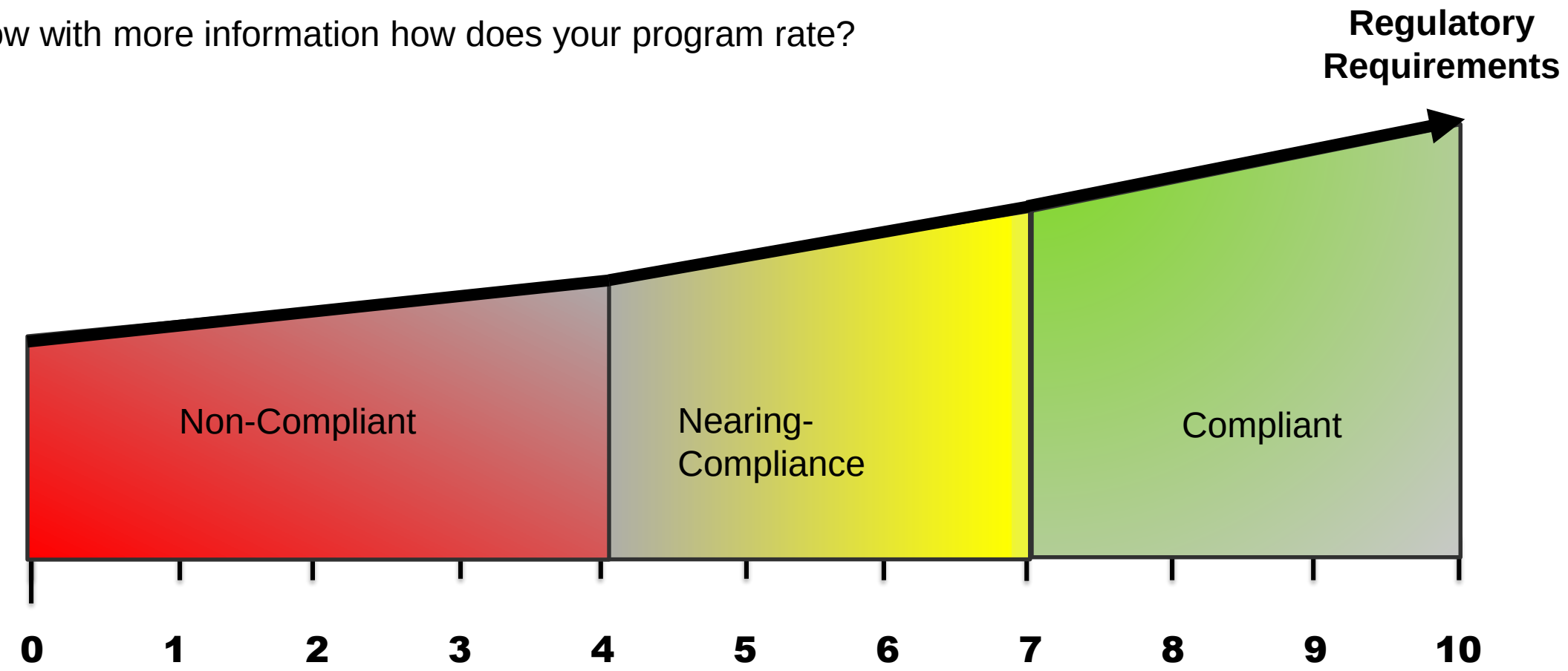
RATING A PRIVACY & CYBER SECURITY PROGRAM

Security or Privacy Example

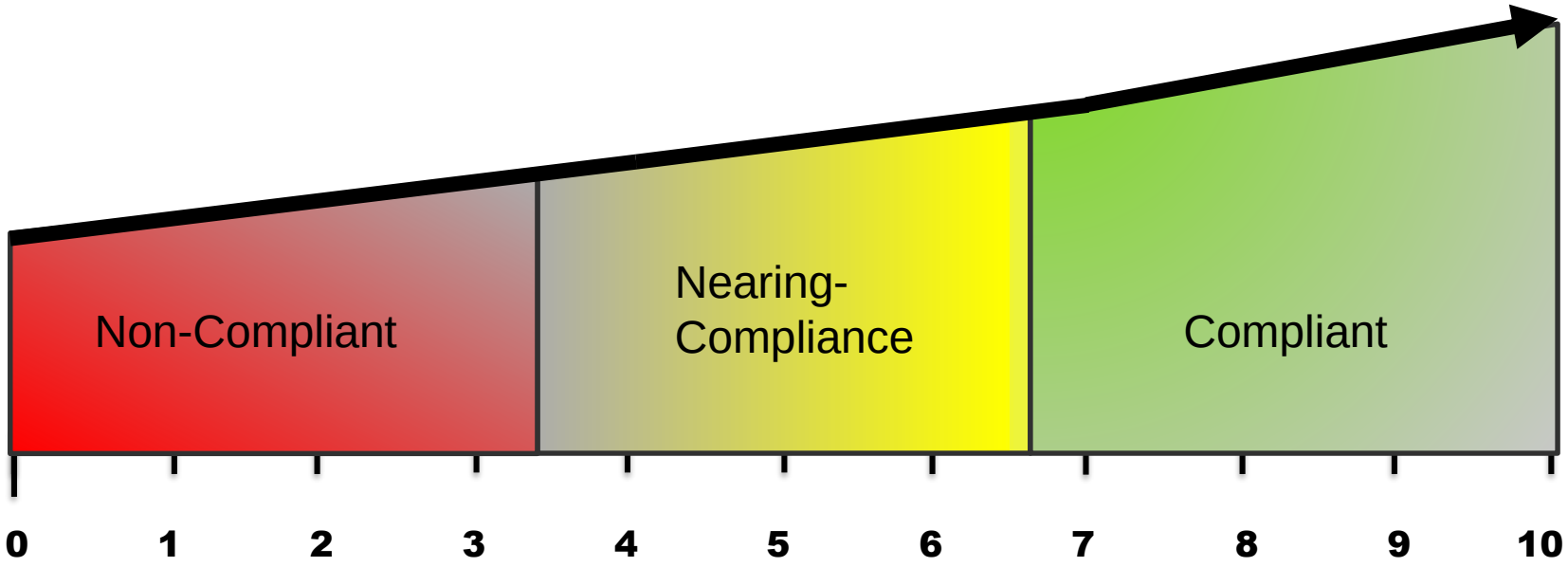
	Scoring		
Question	(0)	(1)	(2)
1. What security or privacy methodology or standards are followed?	0		
2. Who is the one person assigned security or privacy responsibility and oversight?		1	
3. Are there written and approved security or privacy policies and procedures?			2
4. Are the key stakeholders (CEO, CIO, BoD, etc.) briefed routinely on security or privacy risks?			2
5. Is the security or privacy program independently tested or audited?		1	
Column Scores	0	2	4
Overall Score		6	

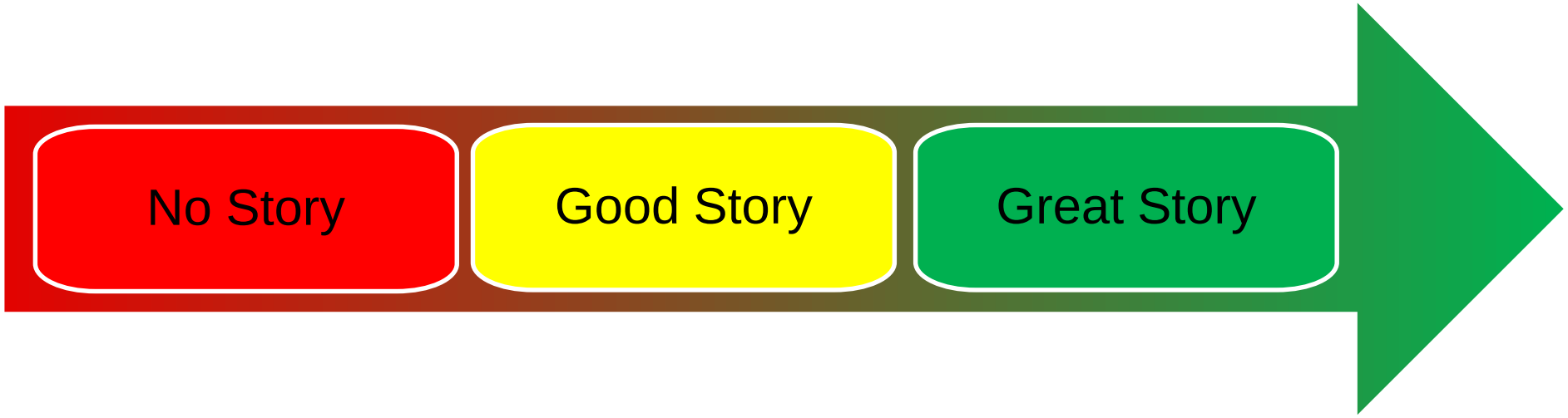
SIMPLE PRIVACY & CYBER SECURITY MEASURING SCALE

Now with more information how does your program rate?



STORY AND MEASURING CORRELATION





HELPFUL HINT WHEN EVALUATING SAAS

When evaluating a SaaS take a quick look at the T&C's no other work may be required

"-----y.com agrees during the Term to implement reasonable security measures to protect Customer Data and will, at a minimum, utilize industry standard security procedures. However, because of the nature of the Service, which combines public and private information that is conveyed over the public internet, to the maximum extent permitted by law: (i) -----y.com shall not be held liable for any damage caused as a result of your use of the Service"

PRESENTATION SUMMARY

- **5 questions can be used to evaluate security or privacy**
- **Process can be used for an organization of supplier**
- **Meant to be done quickly – may save time on a full analysis**

Questions & Discussion

James Johnson CISSP, PMP, STS
CISO
JBJohnson@hollandhart.com
303.295.8563

Holland & Hart LLP | 555 17th Street, Suite 3200 | Denver, CO 80202

HOLLAND&HART LLP