CIS-SIR$^{\text{Q\&As}}$

Certified Implementation Specialist - Security Incident Response

Pass ServiceNow CIS-SIR Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cis-sir.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ServiceNow Official Exam Center

QUESTION 1

Which improvement opportunity can be found baseline which can contribute towards process maturity and strengthen costumer\\'s overall security posture?

A. Post-Incident Review

B. Fast Eradication

C. Incident Containment

D. Incident Analysis

Correct Answer: D

QUESTION 2

Why is it important that the Platform (System) Administrator and the Security Incident administrator role be separated? (Choose three.)

A. Access to security incident data may need to be restricted

B. Allow SIR Teams to control assignment of security roles

C. Clear separation of duty

D. Reduce the number of incidents assigned to the Platform Admin

E. Preserve the security image in the company

Correct Answer: BCD

QUESTION 3

Security tag used when a piece of information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

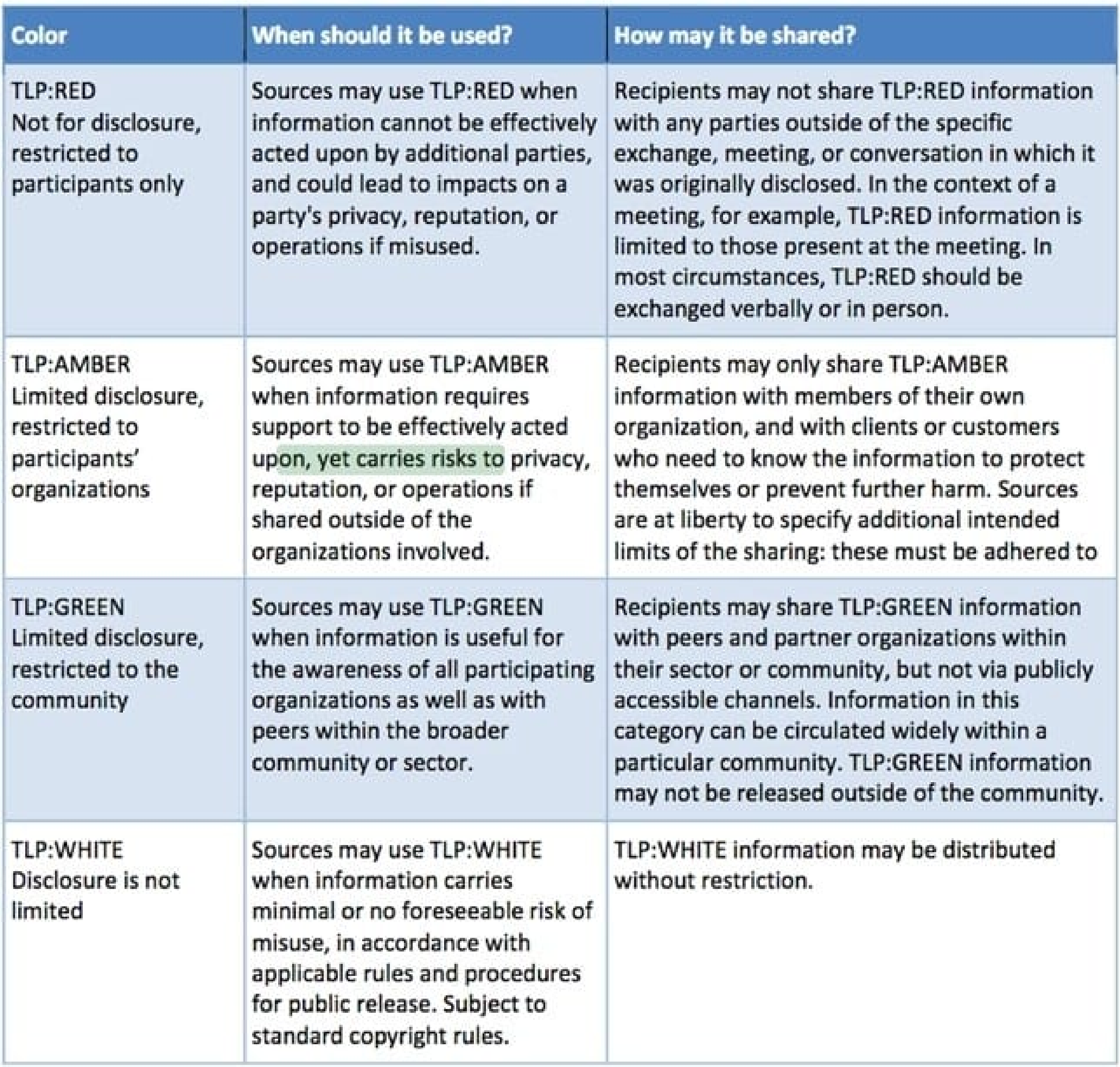
A. TLP:GREEN

B. TLP:AMBER

C. TLP:RED

D. TLP:WHITE

Correct Answer: B



Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to
TLP:GREEN Limited disclosure, restricted to the community	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	TLP:WHITE information may be distributed without restriction.

Table

QUESTION 4

The benefits of improved Security Incident Response are expressed.

A. as desirable outcomes with clear, measurable Key Performance Indicators

B. differently depending upon 3 stages: Process Improvement, Process Design, and Post Go-Live

C. as a series of states with consistent, clear metrics

D. as a value on a scale of 1-10 based on specific outcomes

Correct Answer: C

QUESTION 5

What is the name of the Inbound Action that validates whether an inbound email should be processed as a phishing email for URP v2?

A. User Reporting Phishing (for Forwarded emails)

B. Scan email for threats

C. User Reporting Phishing (for New emails)

D. Create Phishing Email

Correct Answer: A