Mod 1 What you'll learn GESSE's eight security domain Security framework and controls Security audits

Basic security looks Perolect assets and dala Security domain: you will gain underslanding of CISSP's eight security domains Then you'll leaves about primary threats, risks and vulnerabilities to business operations in addition you Il learn national institute of standards and technology Risk" management framework and the steps of risk management unework and Controls Security framework and · Core component and confidentiality integrity and availability (CIA) buse Open aleb Application Decertly Peroject (OWASP) securely principles and girdet.

DATE / /-

Introduction to cybernourely lods: Industry leading securely information and event management (SI & M) lods

'Haw to use SI & M dashbaard as part of their every day work.

Use playbook to reespond to inidents: How Common use of playbooks.

'Use by cybersecerity proffessional use playbooks idenlified threat, risk and vibrerabily.

Later CI SSP's eight security domains
Though risk and velnerability

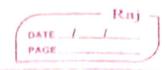
layers of web

NIST Risk Management Framework

Decerity Postere: An organization's ability to manage its defense of critical assets and data, and react to change

Security and risk management (Domain)

Tocused on defining security goals and
objectives, risk mitigation, compilance,
business continuity and legal oregulation.



Rish nitigation. The perocess of having the right procedure and rules in place to quickly reduce the imposed of a risk clike a breach

Bushen Continuity: An organization ability to maintain
their everyday productivity by
establishing suish disaster
secovery plan.

Asset security: Focused on securing digital and physical assets. It's also related to the storage, maintenance retention and destruction of data

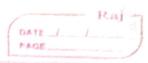
Society arch and eng: Foursel on optimizing data
security by ensuring effective

look, system and perocess

are in place to perotect an

org. assets and data

Shared responsibility: All individual within an org. Take on active role in Lowering risk and maintaining both physical and virtual security



Communication and relevork security: Lowed on managery suring physical network and wireless communication

Edentity and access management: Locused on access and authorization to keep data secure, by making sure users follow established policies to control and manage arsets.

Component: Identification

· Arthentication

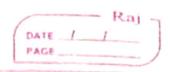
. Anthorystion

· Accountablity

Society Assessment and Testing: Touses on consucting security control lesting Collecting and analyzing data and conducting security dudel audite to monitor for risks threat and veherablity

Lewrely operation: Towned on conducting investigation and implementing preventative measures

Software developmente Security: Focuses or ving secure coding practices



Threals, risks and vulnerableties

Threat: Any circumstance or event that can negatively impact assets Social eng. attack: A manipulation bechnique that exploits human vivor to gain prierate info, access, or valiables

Risks: Anything that can impact the confidentiality integrity or availablity of an asset Low ricks assets : Information that would not have The organizations repetation or ongoing operations, and would not cause

Medium Risk assets: Info that is not available to public and may cause some damage to the org. finances, sup

or organg operation

High Risk assets: Info predected by regulation or laws which it compromised would have a severe negative impact on an organizations finances ongoing operation or reputation

Volnovablety: A weekness that can be exposed exploited by a thereal

Rey impact Russomwave: A malicious attack where threat actors payment to restore access Layers: Sorface web - Dark web · Financial impact · Identity thefit · Repulation RM7 (Risk Management Framework) before. Prepare: Activity that are necessary to many sec and privacy Categorize · Implement · Assess Authorize Monetor

1 Prepare Activity that are necessary to manage secon.

2 Categorize: Used to develop risk management processes and tasks

	PAGE
7	9 1 L 01
3	select: Choose, customize and capture documentation
	Select: Choose, contonize and capture documentation of the control that protect an organiza
4	d. de ti
	implement security and privacy plans for its
	Amplement: security and privacy plans for its
5	Assess Determine 1 + 11/1
	Assess Determine if established control are implemented correctly
	surgerneries Correctly
6	Authorize. Being accomplable los 11.
	and privace sicks that many
	Authorize. Being accountable for the security and privacy risks that may exist in an organization
-	De la Caracteria de la
	Montor: Be aware of how system are opera
	What we Covered
. (TCCP' : II
- 19	brest, risk and vertherability
	IST-RM7
- 11	
79.00	