Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● The event occurred on March 10, 2023, at 8:29:57 a.m. ● *The user belongs to the Legal department and accessed the system using an administrator account.* ● *The IP address associated with the login is 152.207.255.255.*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *The company has not implemented the principle of least privilege, as all employees have access to the administrator account regardless of their role, posing a significant security risk.* ● *Logs and directory records indicate that Robert Taylor Jr, an admin whose contract ended in 2019, accessed payroll systems in 2023 and processed the payment.* ● *This highlights the*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Implement the principle of least privilege to ensure employees only have access to the resources necessary for their roles.* ● *Enforce the separation of duties to minimize the risk of unauthorized actions.* ● *Set user accounts to expire after 30 days for contractors or temporary staff.* ● *Limit contractors' access to essential business resources only.* ● *Enable multi-factor*

		absence of separation of duties within the organization, further exposing the company to potential security breaches.	*authentication (MFA) to enhance account security.*

Accounting exercise

File Edit View Insert Format Data Tools Extensions Help

C22

	A	B	C	D	E	F	G	H	I
1	Event Type: Information								
2	Event Source: AdsmEmployeeService								
3	Event Category: None								
4	Event ID: 1227								
5	Date: 10/03/2023								
6	Time: 8:29:57 AM								
7	User: Legal\Administrator								
8	Computer: Up2-NoGud								
9	IP: 152.207.255.255								
10	Description:								
11	Payroll event added. FAUX_BANK								
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									

Event log ▾   Employee directory ▾

Hugh Chanetsa   **Cybersecurity Portfolio**   **Assets, Threats & Vulnerabilities**

Accounting exercise

File Edit View Insert Format Data Tools Extensions Help

Menus | 100% | $ % .0 .00 123 | Defaul... | — 10 + | B I S A | ▤ | ☰ ↓ ↕ A | 🔗 ⊞ 📊 ▽ ▦

K10 | fx

	A	B	C	D	E	F	G	H	I	J
1	Name	Role	Email	IP address	Status	Authorization	Last access	Start date	End date	
2	Lisa Lawrence	Office manager	l.lawrence@erems.net	118.119.20.150	Full-time	Admin	12:27:19 pm (0 minutes ago)	10/1/2019	N/A	
3	Jesse Pena	Graphic designer	j.pena@erems.net	186.125.232.66	Part-time	Admin	4:55:05 pm (1 day ago)	11/16/2020	N/A	
4	Catherine Martin	Sales associate	catherine_M@erems.net	247.168.184.57	Full-time	Admin	12:17:34 am (10 minutes ago)	10/1/2019	N/A	
5	Jyoti Patil	Account manager	j.patil@erems.net	159.250.146.63	Full-time	Admin	10:03:08 am (2 hours ago)	10/1/2019	N/A	
6	Joanne Phelps	Sales associate	j_phelps123@erems.net	249.57.94.27	Seasonal	Admin	1:24:57 pm (2 years ago)	11/16/2020	1/31/2020	
7	Ariel Olson	Owner	a.olson@erems.net	19.7.235.151	Full-time	Admin	12:24:41 pm (4 minutes ago)	8/1/2019	N/A	
8	Robert Taylor Jr.	Legal attorney	rt.jr@erems.net	152.207.255.255	Contractor	Admin	8:29:57 am (5 days ago)	9/4/2019	12/27/2019	
9	Amanda Pearson	Manufacturer	amandap987@erems.net	101.225.113.171	Contractor	Admin	6:24:19 pm (3 months ago)	8/5/2019	N/A	
10	George Harris	Security analyst	georgeharris@erems.net	70.188.129.105	Full-time	Admin	05:05:22 pm (1 day ago)	1/24/2022	N/A	
11	Lei Chu	Marketing	lei.chu@erems.net	53.49.27.117	Part-time	Admin	3:05:00 pm (2 days ago)	11/16/2020	1/31/2020	
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										

+ ≡ | Event log ▾ | Employee directory ▾

Hugh Chanetsa **Cybersecurity Portfolio** **Assets, Threats & Vulnerabilities**